Gigamon®

GigaVUE Cloud Suite for AWS - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.6

Document Version: 1.0

Last Updated: Friday, April 26, 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
6.6.00	1.0	3/22/2024	The original release of this document with 6.6.00 GA.

Contents

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-FM fabric manager 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 platform 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 Agent) is an agent that is installed in the VM instance. This agent mirrors the selected traffic 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, ZIP and MSI .

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.

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-V.

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 v1.7 can only manage UCT-Vs v1.7. If you have UCT-Vs v1.6 still deployed in the EC2 instances, you must configure both UCT-V Controller v1.6 and v1.7. 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 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 Fabric Components in GigaVUE-FM

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

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

Traffic Acquisition

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

You can acquire traffic using 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 helps you establish connection in between GigaVUE-FM and AWS platform. Once the connection is established, you can use GigaVUE-FM to launch the GigaVUE V Series Nodes, GigaVUE V Series Proxy and UCT-V Controller.

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

Monitoring Session

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

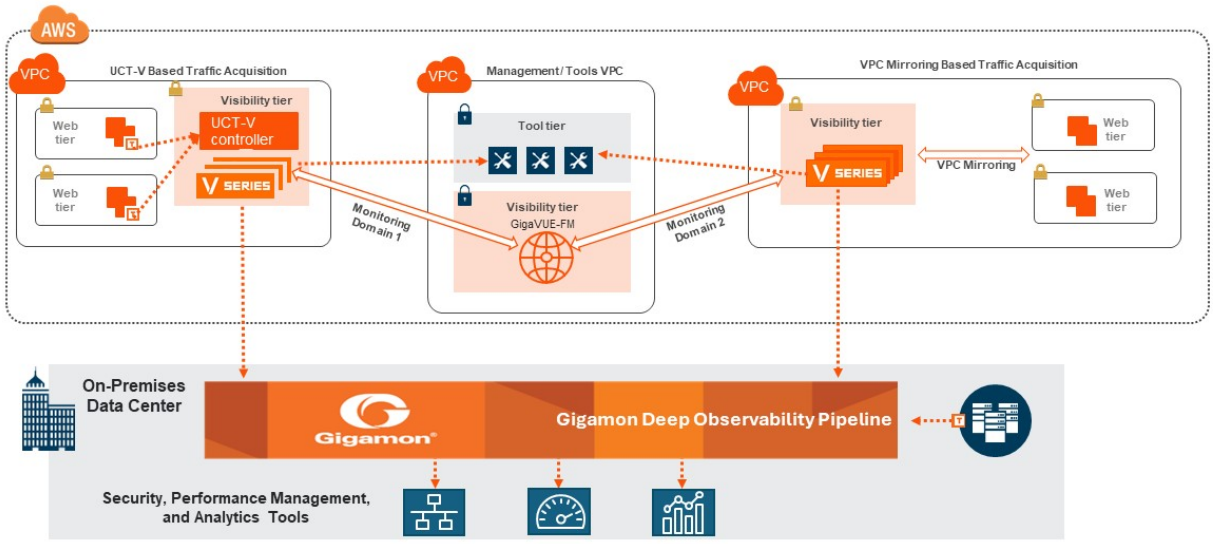
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance to your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions.

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

Third Party Orchestration

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

Architecture



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

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

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

.

Introduction to the Supported Features

GigaVUE Cloud Suite for AWS supports the following features:

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

Precryption™

License: Requires **SecureVUE Plus** license.

Gigamon Precryption™ technology[1] redefines security for virtual, cloud, and containerized applications, delivering 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.

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.

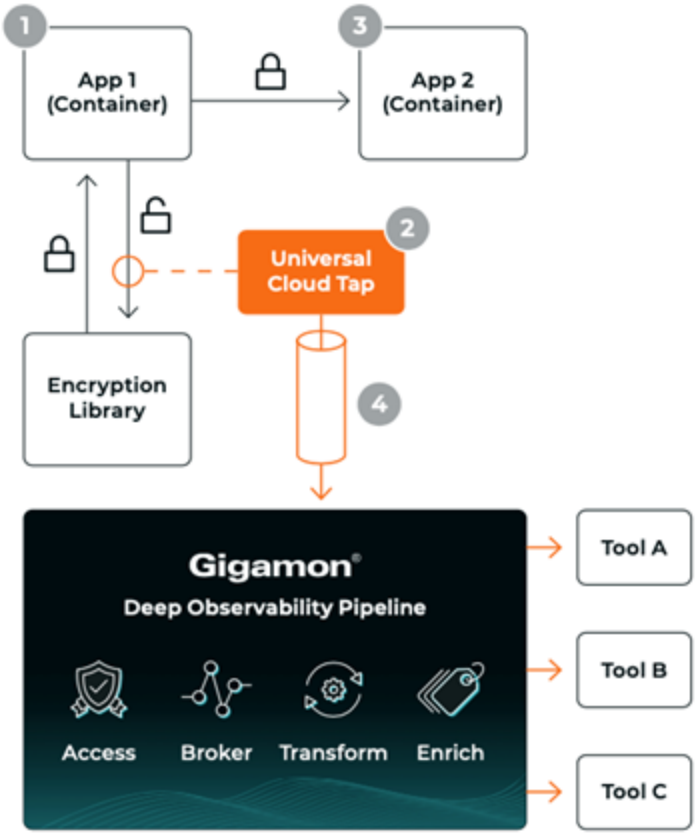
How Gigamon Precryption Technology Works

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

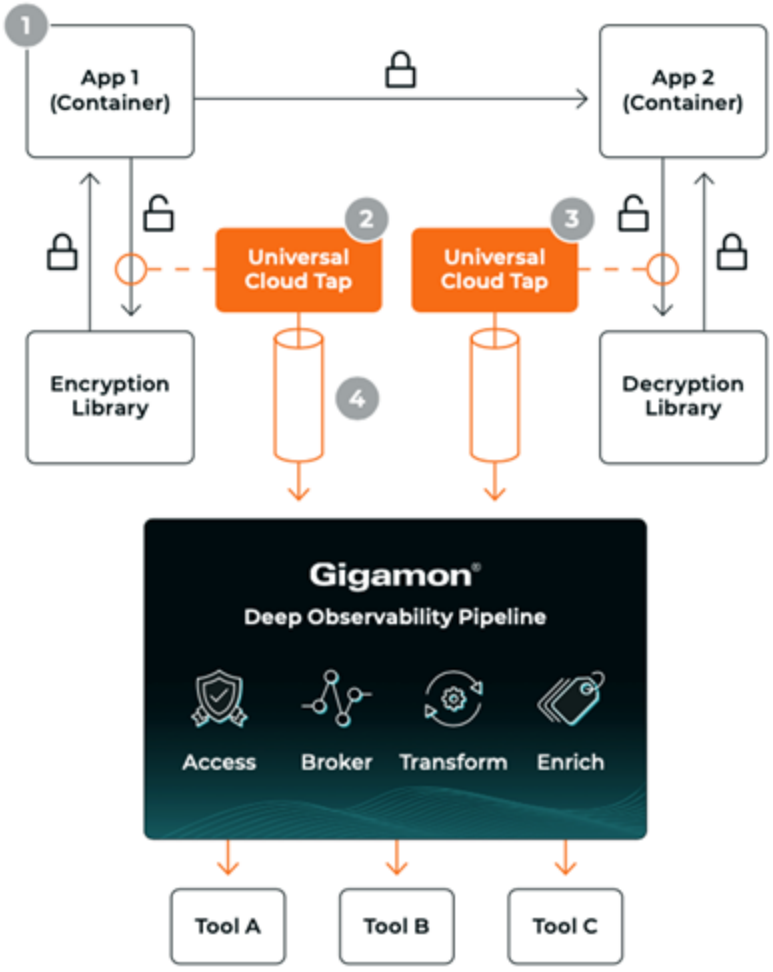
Precryption Technology on Single Node

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.



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

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x
- 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.

Supported Kernel Version

Precryption is supported for Kernel Version 5.4 and above for all Linux and Ubuntu Operating Systems. For the Kernel versions below 5.4, refer to the following table:

Kernel Version	Operating System
4.18.0-193.el8.x86_64	RHEL release 8.2 (Ootpa)
4.18.0-240.el8.x86_64	RHEL release 8.3 (Ootpa)
4.18.0-305.76.1.el8_4.x86_64	RHEL release 8.4 (Ootpa)
4.18.0-348.12.2.el8_5.x86_64	RHEL release 8.5 (Ootpa)
4.18.0-372.9.1.el8.x86_64	RHEL release 8.6 (Ootpa)
4.18.0-423.el8.x86_64	RHEL release 8.7 Beta (Ootpa)
4.18.0-477.15.1.el8_8.x86_64	RHEL release 8.8 (Ootpa)
5.3.0-1024-kvm	ubuntu19.10
4.18.0-305.3.1	Rocky Linux 8.4
4.18.0-348	Rocky Linux 8.5
4.18.0-372.9.1	Rocky Linux 8.6
4.18.0-425.10.1	Rocky Linux 8.7
4.18.0-477.10.1	Rocky Linux 8.8

Kernel Version	Operating System
4.18.0-80.el8.x86_64	centos 8.2
4.18.0-240.1.1.el8_3.x86_64	centos 8.3
4.18.0-305.3.1.el8_4.x86_64	centos 8.4
4.18.0-408.el8.x86_64	centos 8.5

Note

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

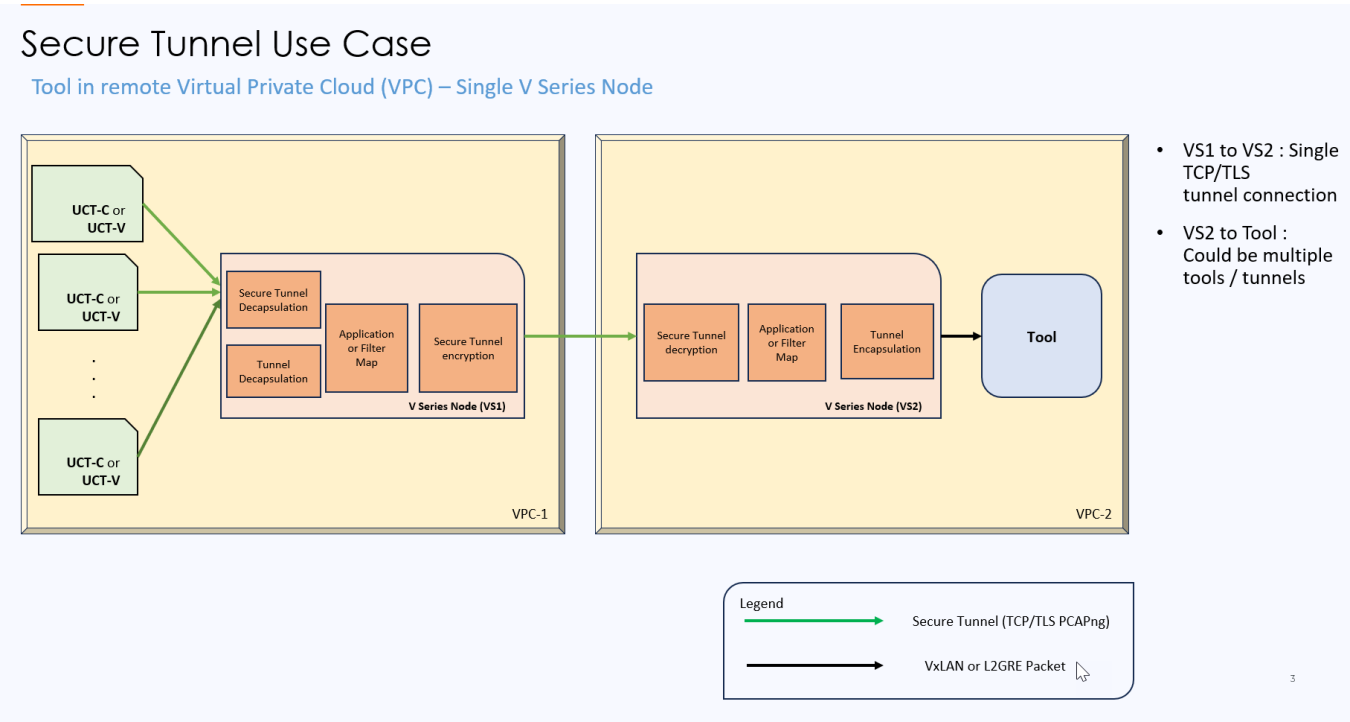
Secure Tunnels

Secure Tunnel 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.



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 Prefiltering Policy Template .

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.

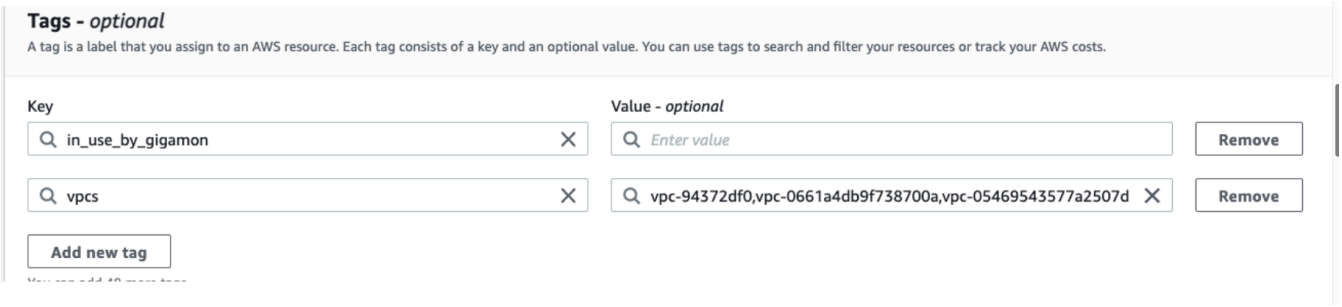
If you want to filter the traffic, then you can create a traffic mirror filter on AWS and add rules to determine the traffic that is mirrored. This traffic mirror filter acts as a pre-filter and pass only the filtered traffic to the GigaVUE V Series Nodes.

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" .



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

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics[1] you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. Refer to Analytics topic in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

Rules and Notes:

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

Virtual Inventory Statistics and Cloud Applications Dashboard

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

To access the dashboards:

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

The following table lists the various virtual dashboards:

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

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	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 options to filter and visualize the data.

Dashboard	Displays	*Visualizations*	Displays
		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 GigaVUE V Series Node. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total 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
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.

Dashboard	Displays	*Visualizations*	Displays
	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		• 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. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session**	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
	• **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. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session**	*Endpoint Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

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

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

Cloud Health Monitoring

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

Customer Orchestrated Source - Use Case

Customer Orchestrated Source is a traffic acquisition method that allows to tunnel traffic directly to the GigaVUE V Series Nodes. In cases where UCT-V or VPC Mirroring cannot be configured due to firewall or other restrictions, you can use this method and tunnel the traffic to GigaVUE V Series Node, where the traffic is processed.

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

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

Licensing 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 GigaVUE 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 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 one 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 expires (and has not been renewed yet), the 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.

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

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

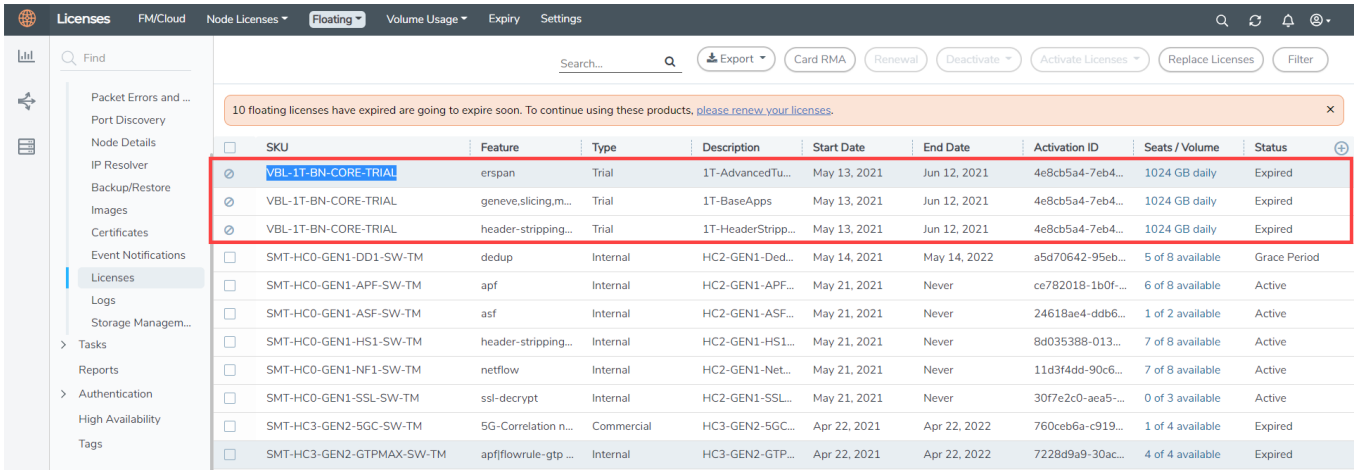
To activate Volume-based licenses:

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).



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.

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

Direction	Protocol	Port	CIDR	Purpose
GigaVUE-FM				
Inbound	TCP	443	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	TCP	22	Administrator Subnet	Management connection to GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	TCP	443	UCT-V Controller IP	Allows UCT-V Controller to communicate the registration requests to GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE V Series Node to communicate the registration requests to GigaVUE-FM, if GigaVUE V Series Proxy is not used.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM
Inbound	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
Inbound	UDP	2056	GigaVUE V Series Node IP	Receive Application Intelligence, Application Visualization reports from GigaVUE V Series Node.
Outbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE-FM to reach the

Direction	Protocol	Port	CIDR	Purpose
			Address	Pubic Cloud Platform APIs.
UCT-V Controller				
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate with GigaVUE-FM
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to communicate the registration requests from UCT-V.
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V controllers stateful communication with UCT-V Controller
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user initiated management and diagnostics, Specifically when using third party orchestration.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to communicate the registration requests to GigaVUE-FM
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate with UCT-Vs
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM
UCT-V				
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V controllers stateful communication with UCT-V Controller
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
Outbound	• 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	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.

Direction	Protocol	Port	CIDR	Purpose
GigaVUE V Series Proxy (optional)				
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE V Series Node for registration and Heartbeat
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user initiated management and diagnostics, Specifically when using third party orchestration.
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE V Series Node
GigaVUE V Series Node				
Inbound	TCP	8889	• GigaVUE-FM IP • V Series Proxy IP	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	• 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	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user initiated management and diagnostics, Specifically when using third party orchestration.
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound	UDP	2056	GigaVUE-FM IP	Receive Application Intelligence,

Direction	Protocol	Port	CIDR	Purpose
				Application Visualization reports to GigaVUE-FM
Outbound	UDP	2055	Tool IP	Sends NetFlow traffic to external tool.
Outbound	UDP	514	Tool IP	Sends AMI log messages to external tool.
Outbound (optional)	ICMP	• echo request • echo reply	Tool IP	Allows V Series node to health check tunnel destination traffic
Bi-directional	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: admin 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: admin 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: admin 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..
- 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:

- Deployment Options for GigaVUE Cloud Suite for AWS
- Permissions and Privileges
- 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

Deployment Options for GigaVUE Cloud Suite for AWS

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 can be configured to provide visibility for physical and virtual traffic. There are three different ways in which GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components. For information on the prerequisites and work flow refer the following topics:

- Prerequisites
- Deploy GigaVUE Fabric Components using AWS

Deploy GigaVUE Fabric Components using AWS

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

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

Deploy GigaVUE Fabric Components using GigaVUE-FM

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

Traffic Acquisition Method as UCT-V

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

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

Traffic Acquisition Method as VPC Mirroring

Perform the following steps to use VPC mirroring as your traffic acquisition method:

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Create a Monitoring Domain Ensure that the **Use FM to Launch Fabric** toggle button is enabled.	Create a Monitoring Domain
3	Configure GigaVUE Fabric Components **NOTE:** 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.	Configure GigaVUE Fabric Components in GigaVUE-FM
4	Create Monitoring session	Create a Monitoring Session
5	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
6	Deploy Monitoring Session	Deploy Monitoring Session
7	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Tunnel

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

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

Permissions and Privileges

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",
                "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 Subscribe to GigaVUE Products

Subscribe to 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
- UCT-V Controller

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. In the "Pricing model" section, filter the list by checking the box next to "Bring Your Own License"
5. Select the latest version GigaVUE Cloud Suite BYOL version. For more information on Licensing, refer to Licensing GigaVUE Cloud Suite .
6. Click **Continue to Subscribe**. The Terms and Conditions page is displayed.
7. Review the Terms and Conditions and then click **"Accept Terms**".
8. Review the summary and then click "**Continue to Configuration**".
9. In the "**Configure this software**" page, enter the following details for your deployment and click "**Continue to Launch**":
    a. **Fulfillment Option**: <Leave Default>
    b. **Software Version**: <Leave Default>
    c. **Region**: <Select your specific Region>

10. In the Configure this software page, select the following:
    a. **Choose Action**: <Launch from Website>
    b. **EC2 Instance Type**: <select desired size>.
    c. **VPC Settings**: <Indicate your desired VPC>
    d. **Subnet Settings**: <Indicate your desired Subnet>
    e. **Security Group Settings**: <Indicate your security group settings>
    f. **Key Pair**: <Indicate your desired key>
    g. Click Launch.

After subscribing and deploying the GigaVUE-FM, you must change the default username and password. For more information, see 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.

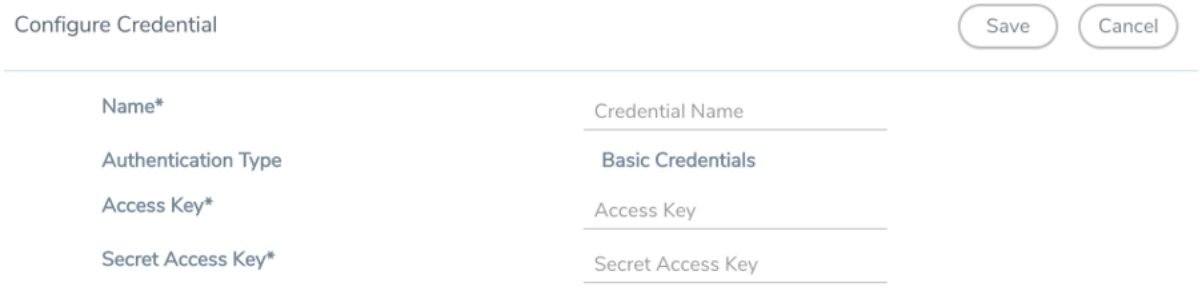
Create AWS Credentials

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.



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 Permissions and Privileges.

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

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:

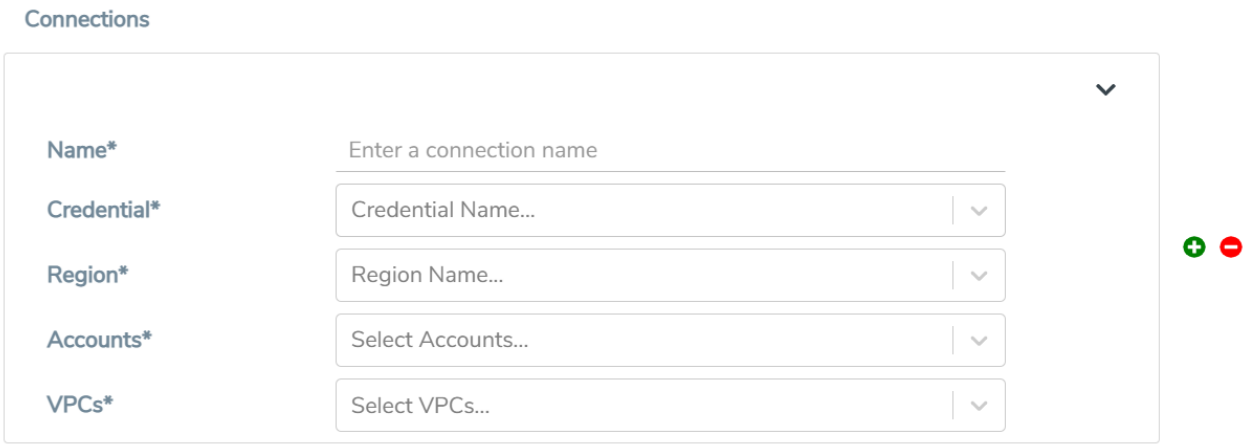
1. Go to **Inventory > VIRTUAL > AWS** , and then click **Monitoring Domain**.
2. On the Monitoring Domain page, click the **New** button. The Monitoring Domain

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 and Privileges 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.

Field	Action
	When using IPv4 tunnels, the maximum MTU value is 8951. The UCT-V tunnel MTU should be 50 bytes less than the agent's destination interface MTU size. When using IPv6 tunnels, the maximum MTU value is 8931. The UCT-V tunnel MTU should be 70 bytes less than the agent's destination interface MTU size.
Use FM to Launch Fabric	Select **Yes** Configure GigaVUE Fabric Components in GigaVUE-FM to or select **No** to Configure GigaVUE Fabric Components in AWS.
Enable IPv6 Preference (This appears only when **Use FM to Launch Fabric** is disabled and Traffic Acquisition Method is UCT-V)	Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.
Connections  **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
- Fabric
- UCT-V

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. • **Edit CA** - You can use this option to edit the existing CA or add a new CA if you haven't added to the selected Monitoring Domain for the Secure Tunnel feature.
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-V

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

The list view shows the following details:

- Monitoring Domain
- IP address
- Registration time
- Last 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. Create a Monitoring Domain.
    a. Select UCT-V as the Traffic Acquisition Method.
3. Configure GigaVUE Fabric Components in GigaVUE-FM
4. Install UCT-V
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 Create Prefiltering Policy Template .

    - 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 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 in GigaVUE-FM
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:

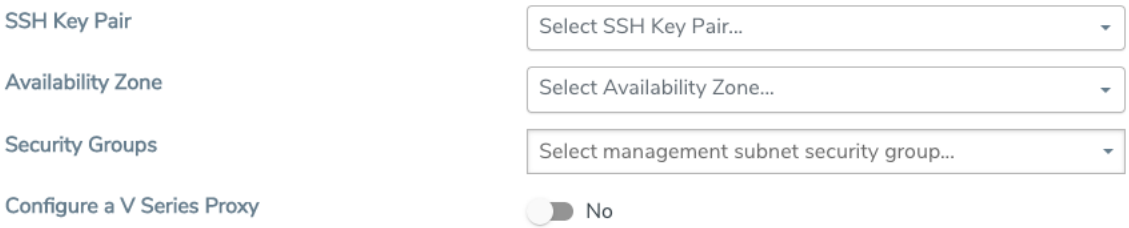
- Configure UCT-V Controller
- Configure GigaVUE V Series Proxy
- Configure GigaVUE V Series Node

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.

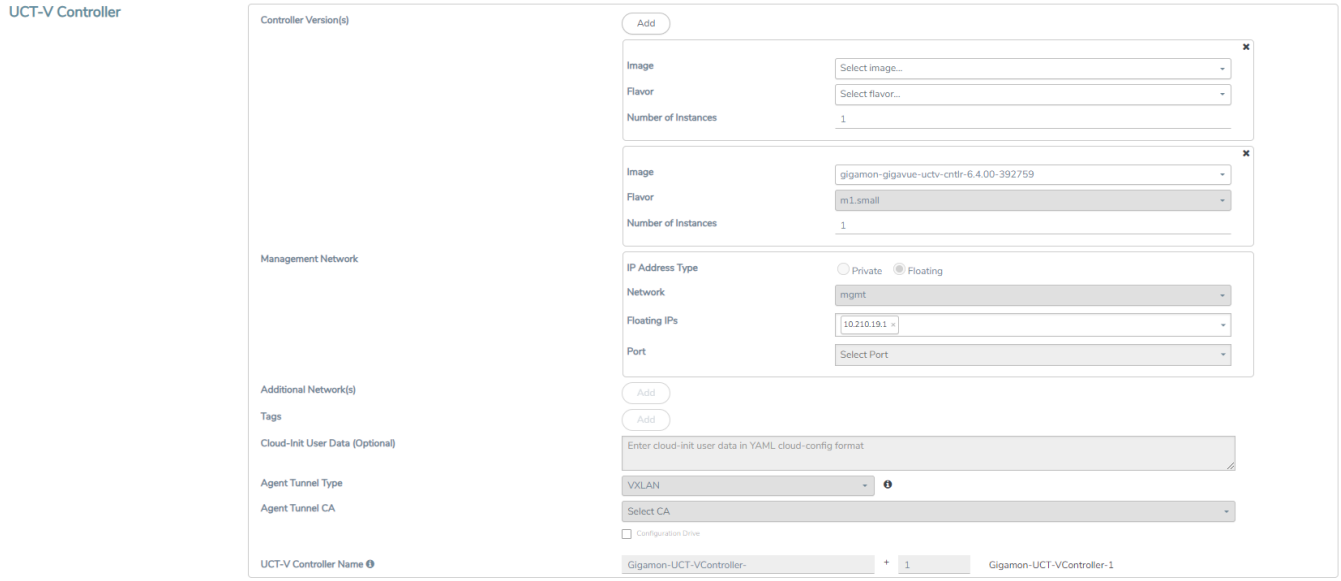
Fields	Description
Security Groups	The security group created for the UCT-V Controller. For more information, refer to Prerequisites.
Prefer IPv6	Enables IPv6 to deploy all the Fabric Controllers, and the tunnel between hypervisor to V Series node using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address. **NOTE:** This option can be enabled only when deploying a new GigaVUE V Series Node. If you wish to enable this option after deploying the GigaVUE V Series Node, then you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.
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.



Configure UCT-V Controller

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



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

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. **NOTE:** Do not configure floating IPv4 for an IPv6-only management /data subnet. Floating IPv4 is not applicable for IPv6-only subnet.
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.
Agent Tunnel	The type of tunnel used for sending the traffic from UCT-Vs to

Fields	Description
Type	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 8951. 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.

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

- Users
- Role
- User Groups

Users

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

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.

To add users perform the following steps:

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

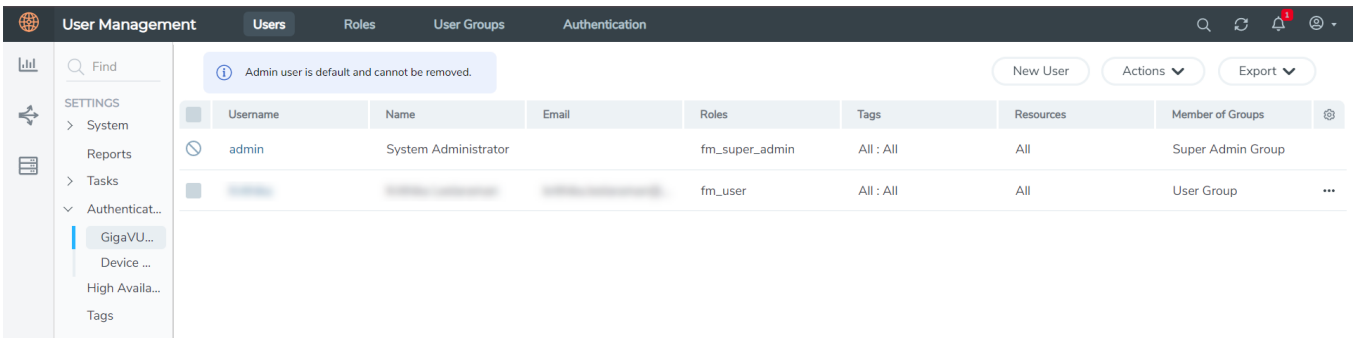


Figure 1 *FM Users Page*

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

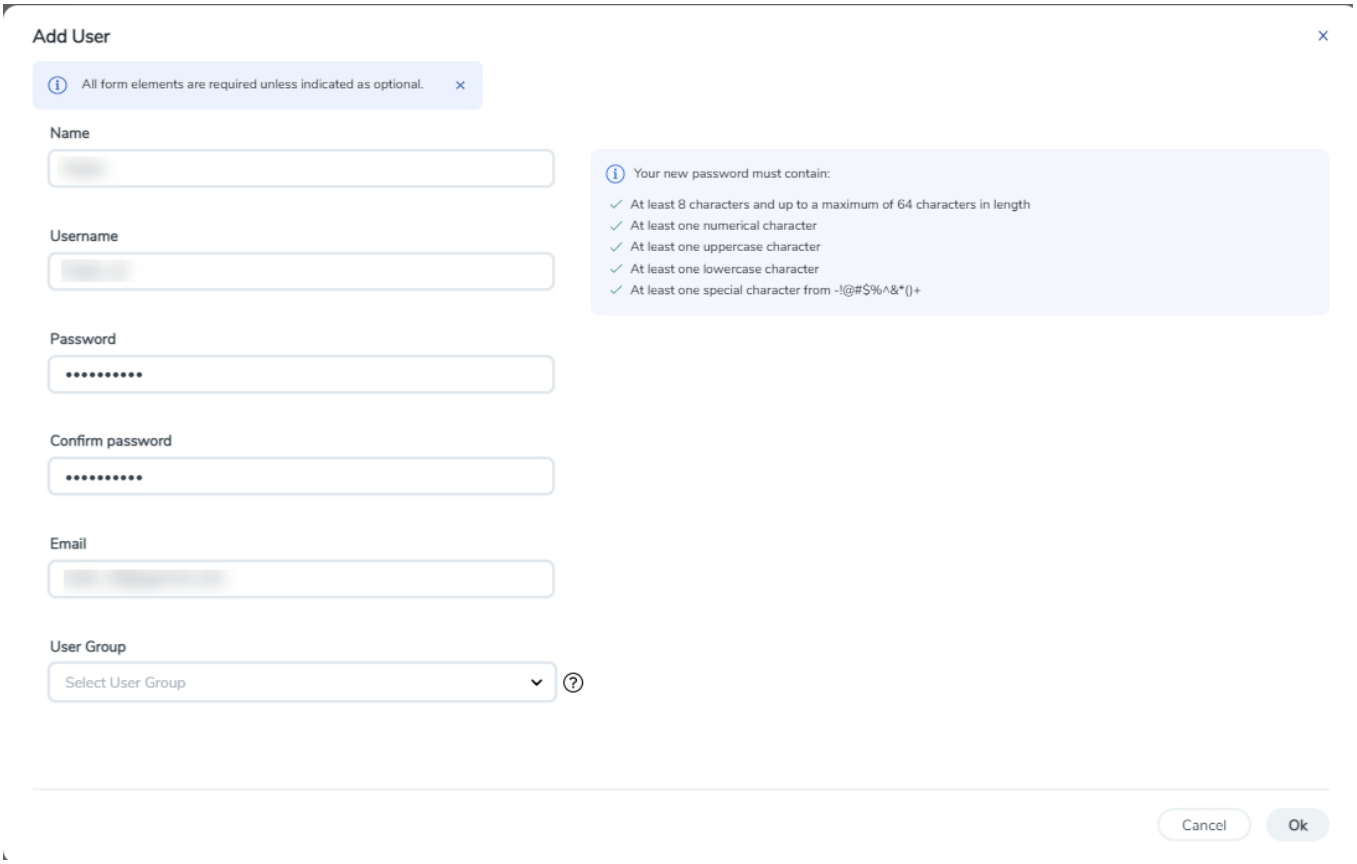


Figure 2 *Create User*

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

- **Name:** Actual name of the user
- **Username**: User name configured in GigaVUE-FM
- **Email**: Email ID of the user
- **Password/Confirm Password**: Password for the user.
- **User Group:** 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.

The username and password created in this section will used in the registration data, used for deploying the fabric components.

Role

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

Create Roles

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

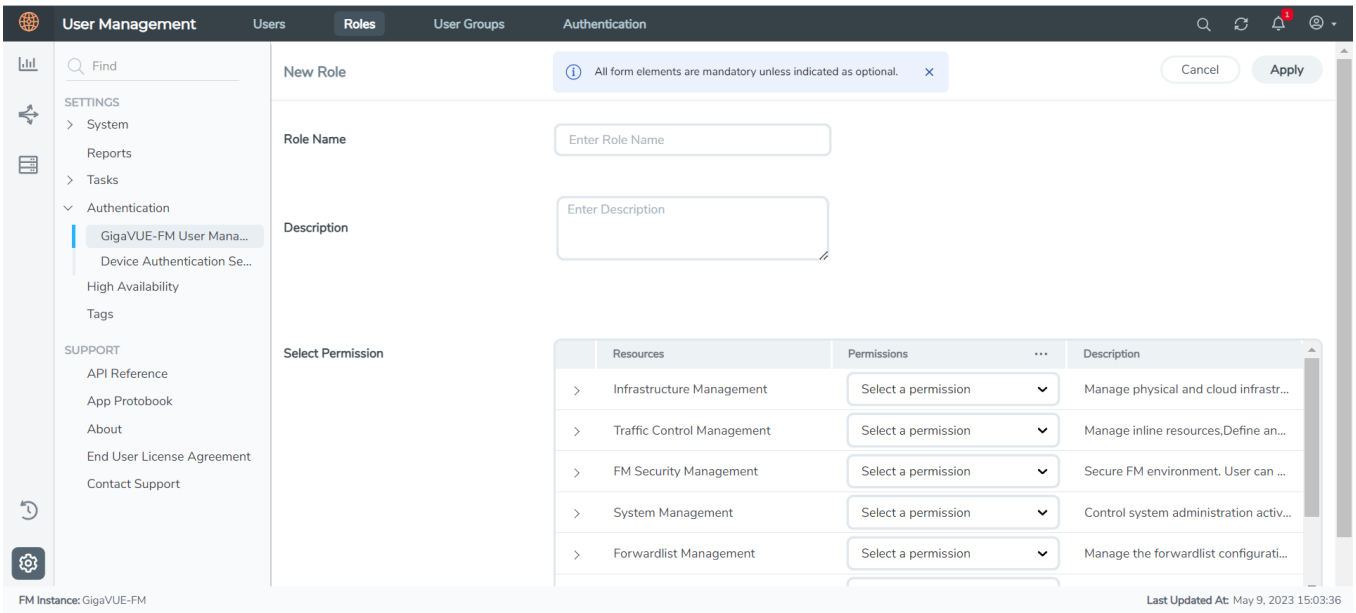
GigaVUE-FM has the following default roles:

- **fm_super_admin** — Allows a user to do everything in GigaVUE-FM 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 GigaVUE-FM 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 GigaVUE-FM 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.

To create a role

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



3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.

- **Select Permission**: For Third Party Orchestration from the **Resources**, select **Write** from the **Permissions** drop-down menu.

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

User Groups

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

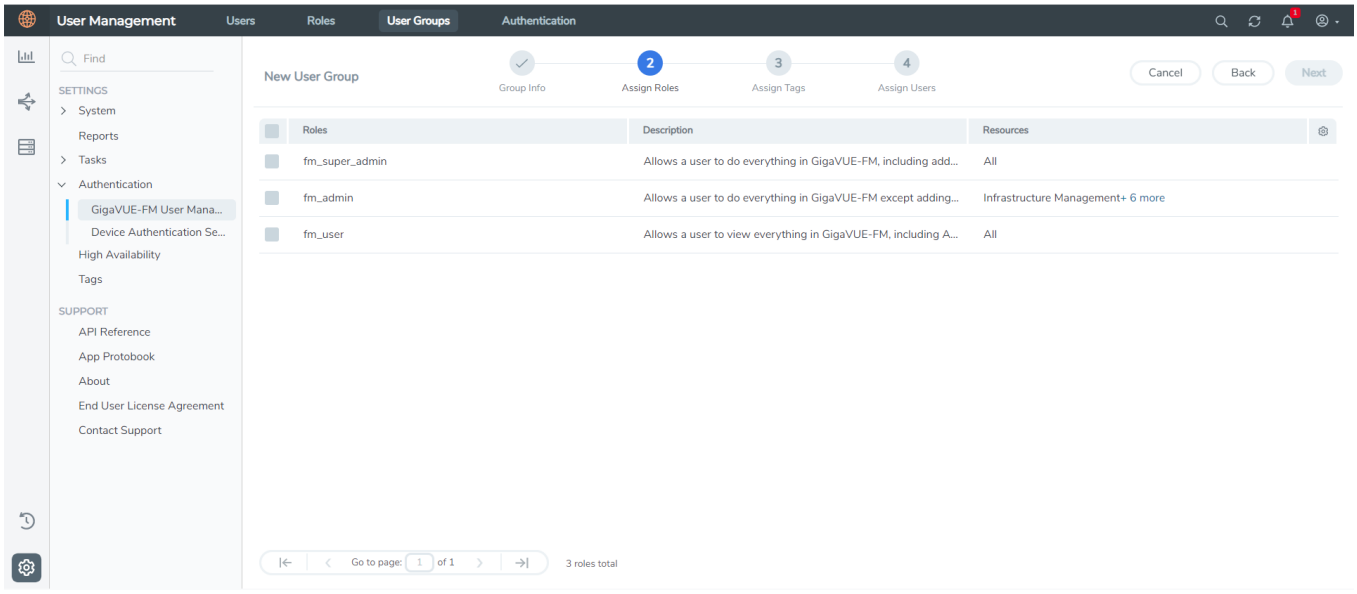
Create User Groups in GigaVUE-FM

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.

To create a custom 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.



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.

Recommended Instance Type

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

Fabric Component	Machine type
GigaVUE V Series Node	c5n.xlarge
UCT-V Controller	T2.micro

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:

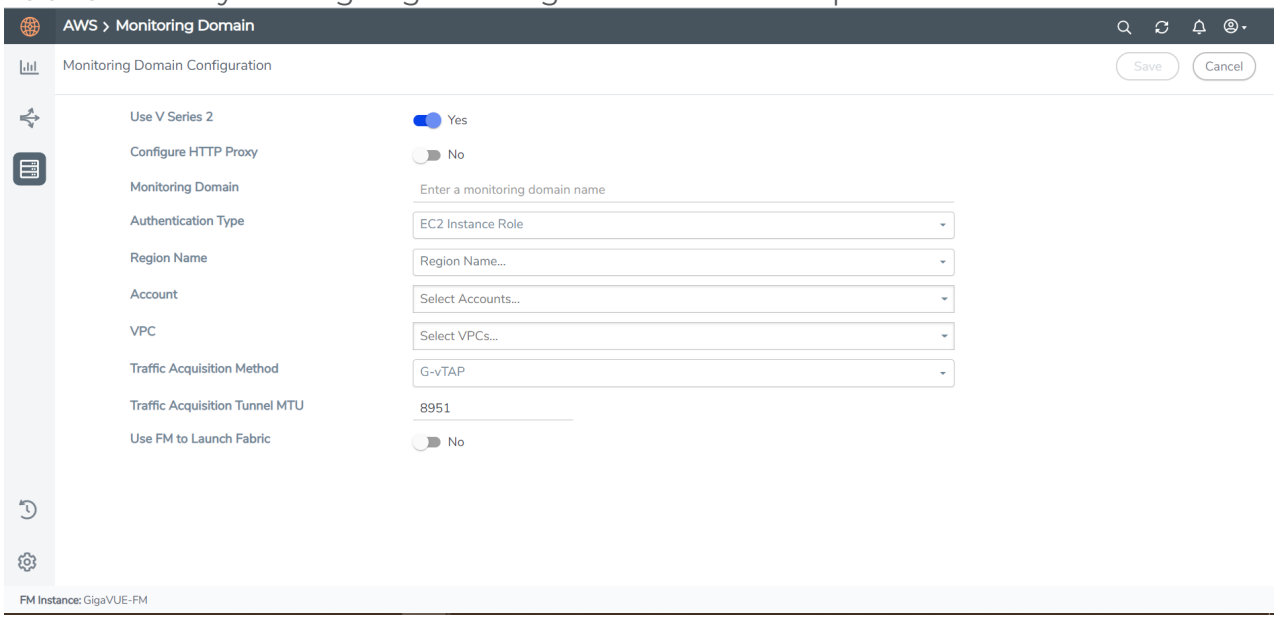
- Configure GigaVUE V Series Nodes and V Series Proxy in AWS
- Configure UCT-V Controller in AWS
- Configure UCT-V in AWS

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.



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:

Field	User Data

User data without custom certificate	`#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`

User data with custom certificate	`#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`

- 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`

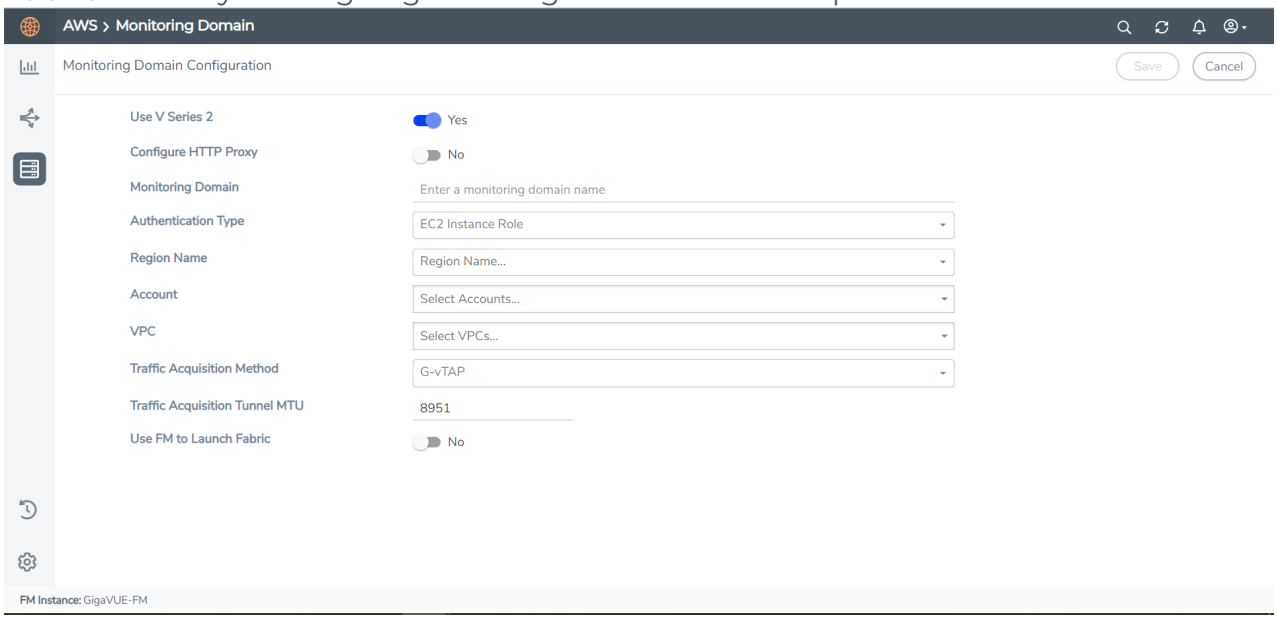
The deployed GigaVUE V Series node or proxy registers with the GigaVUE-FM. After successful registration theGigaVUE V Series node or proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing ,the fabric node status appears as 'Unhealthy'. If more than five heartbeats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

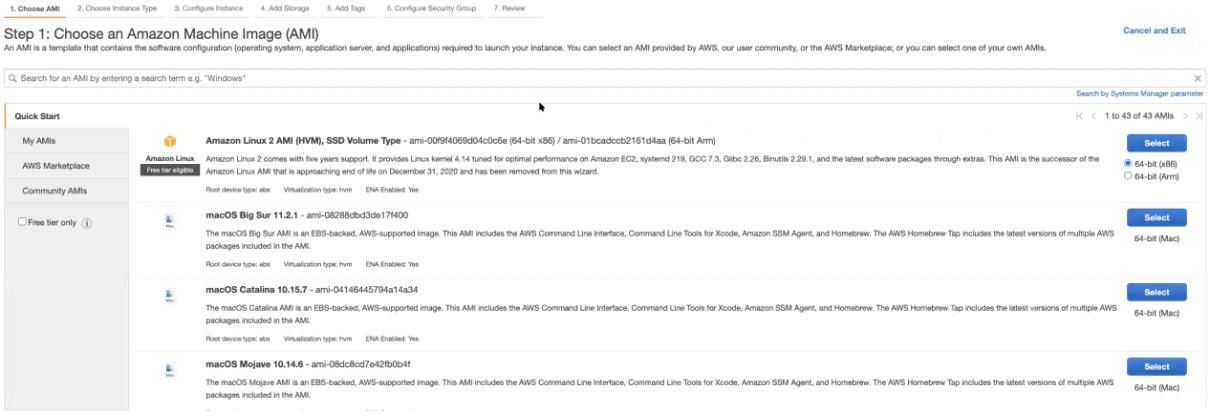


3. In your AWS environment, launch the UCT-V Controller AMI instance using any of the following methods:
   - Register UCT-V Controller using User Data
   - Register UCT-V Controller using a configuration file

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.



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

Field	User Data

User data without custom certificate	`#cloud-config`
	` write_files:`
	` - path: /etc/gigamon-cloud.conf`
	`  owner: root:root`
	`  permissions: '0644'`
	`  content: |`
	`  Registration:`
	`  groupName: <Monitoring Domain Name>`
	`  subGroupName: <VPC Name>`
	`  user: <Username>`
	`  password: <Password>`
	`  remoteIP: <IP address of the GigaVUE-FM>`
	`  sourceIP: <IP address of UCT-V Controller> (Optional Field)`
	`  remotePort: 443`

User data with custom certificate	`#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>`
	`  sourceIP: <IP address of UCT-V Controller> (Optional Field)`
	`  remotePort: 443`

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

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					
	pukhraj-vpc				Connected
		G-vTapController	34.219.250.141	1.7-304	Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	Ok
		Gigamon-VSeriesNode-1	172.30.24.188	2.2.0	Ok

Register UCT-V Controller 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>
    sourceIP: <IP address of UCT-V Controller> (Optional Field)
    remotePort: 443
```

c. Restart the UCT-V Controller service.

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

Assign Static IP address for UCT-V Controller

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

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

```
network:
        version: 2
        renderer: networkd
        ethernets:
                ens3:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens4:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
                ens5:
                        addresses:
                                - <IP address>
                        gateway: <IP address>
```

d. Save the file.
e. Restart theUCT-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. Create a local configuration file and enter the following user data.

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

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

   - If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:
     localInterface:<Interface to which UCT-V Controller is connected>
   - 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, 6.5.00, 6.6.00

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

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

Operating System	Supported Versions	Validated Versions
Ubuntu/Debian	Versions 18-04 and above are supported.	Versions 16.04 and 20.04
CentOS	Versions 7.5 and above.	Versions 7.9 and 8.2
Fedora	Versions 7.5 and above.	Versions 7.5
RHEL	Versions 7.5 and above.	Versions 8.8 and 9.2
Windows Server	Versions 2012 through 2022	Versions 2022
Windows Client	Versions 10 and 11	Versions 10 and 11
Amazon Linux	Versions 1 and 2 (For version 2, package iproute-tc must be installed first)	NA
Rocky OS	Versions 8.4 and above	Versions 8.5 and 8.8

GigaVUE-FM version 6.6 supports UCT-V version 6.6 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 monitoring instance. In the UCT-V configuration, you can configure eth0 as the source and the destination interface, and specify both egress and ingress traffic to be selected for monitoring purpose. The egress and ingress traffic from eth0 is mirrored and sent out using the same interface.

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

Dual ENI Configuration

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

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

Install UCT-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**6.6.00** 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_6.6.00_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**6.6.00** 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_6.6.00_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_**6.6.00**_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_6.6.00_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 **6.6.00** 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
```

   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.
   - User and Password must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

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

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

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 **6.6.00** 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
```

   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.
   - User and Password must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

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

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

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

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

Upgrade UCT-V

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

- Before upgrading UCT-V, ensure that the UCT-V is in the **ON** state on the **UCT-V** page.
- 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.

1. Uninstall the existing UCT-V. Refer to Uninstall UCT-V for more detailed information on how to uninstall UCT-V.
2. Install the latest version or the new UCT-V. Refer to the following topics for more detailed information on how to install a new UCT-V:
   - Linux UCT-V Installation
   - Windows UCT-V Installation
3. Restart the UCT-V service.
   - Linux platform:
     ```
     $ sudo service uctv restart
     ```
   - Windows platform: Restart from the Task Manager.

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

Notes

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

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

To configure a secure tunnel in UCT-V, you must configure one end of the tunnel to the UCT-V and the other end to GigaVUE V Series node. You must configure the CA certificates in UCT-V and the private keys and SSL certificates in GigaVUE V Series node. Refer to the following steps for configuration:

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>1.</td><td>Upload a Custom Authority Certificate (CA)</td><td>)You must upload a Custom Certificate to UCT-V Controller for establishing a connection with the GigaVUE V Series node.

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

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

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. To add SSL Key, follow the steps in the section Upload SSL Keys.</td></tr>
</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. **NOTE:** When GigaVUE V Series is upgraded or deployed to 6.5, all the existing monitoring sessions will be redeployed, and individual TLS TEPs are created for each agent.
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 Inventory > Resources > Security > CA List.
2. Click Add, to add a new Certificate Authority. The Add Certificate Authority page appears.
3. Enter or select the following information.
<table><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 Save.
5. Click Deploy All.

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:
1. In the Edit Monitoring Session page, click Options. The Monitoring Session option page appears.
2. Enable the Secure Tunnel 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>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>6</td><td>Create an Egress tunnel from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.</td><td>You must create a tunnel for traffic to flow out from GigaVUE V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Configure Monitoring Session to know about monitoring session.

To create the egress tunnel, follow these steps:
1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr><tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr></table></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>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel</td></tr>
<tr><td>Traffic Direction</td><td>Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:
MTU- The default value is 1500.
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.
DSCP - Enter the Differentiated Services Code Point (DSCP) value.
Flow Label - Enter the Flow Label value.
Source L4 Port- Enter the Souce L4 Port value
Destination L4 Port - Enter the Destination L4 Port value.
Flow Label
Cipher- Only SHA 256 is supported.
TLS Version - Select TLS Version1.3.
Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments.
SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.
Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments.</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>
4. Click Save.
</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</td><td>You must create a ingress tunnel for traffic to flow in from GigaVUE V Series Node with tunnel type as TLS-PCAPNG</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td>TLS-PCAPNG while creating the monitoring session for GigaVUE node 2.</td><td>while creating the monitoring session. Refer to Configure Monitoring Session to know about monitoring session.

To create the ingress tunnel, follow these steps:
1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<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.
NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</td></tr>
<tr><td>Traffic Direction</td><td>Choose in (Decapsulation) for creating an ingress tunnel that receives traffic from 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. IPv4 and IPv6 are 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>
4. Click Save.</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.

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.

To enable prefiltering, refer to Monitoring Session Options

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

A monitoring session defines how traffic should be processed and send to the tunnel endpoints.

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.

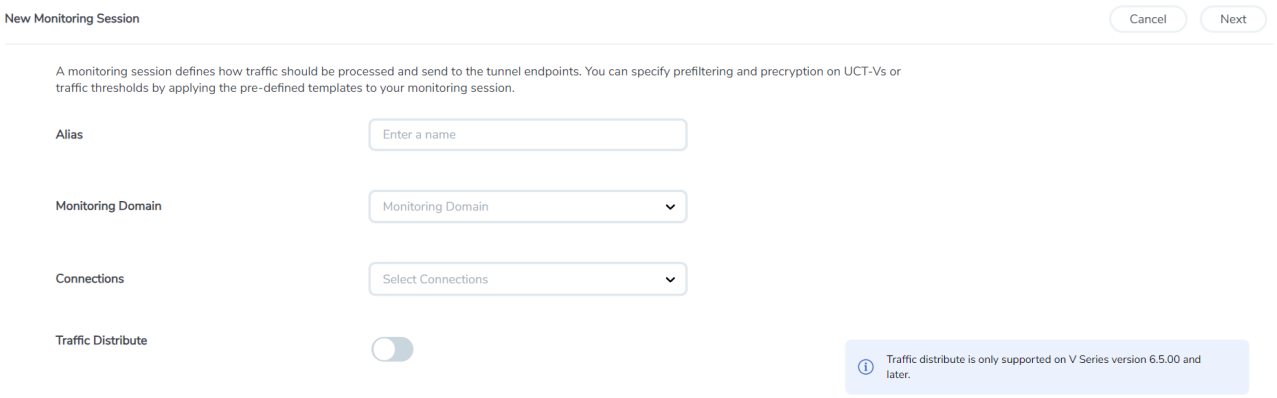
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance to your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions.

For the connections without UCT-Vs, there are no targets that are automatically selected. You can use Customer Orchestrated Source in the monitoring session to accept a tunnel from anywhere.

You can create multiple monitoring sessions per monitoring domain.

To create a new monitoring session:

1. Go to **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.
Traffic Distribute	Enabling the "Traffic Distribute" option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.

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

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

Button	Description
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
Delete	Deletes the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Deploy	Deploys the selected monitoring session.
Undeploy	Undeploys the selected monitoring session.
Apply Threshold	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates, and how to apply threshold templates.
Apply Policy	You can use this button to enable precyption, prefiltering, or Secure Tunnel. Refer to Enable Prefiltering and Precryption 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, Secure Tunnel, User Defined Applications, here. You can also create prefiltering and threshold template and apply it to the monitoring session. Refer to Monitoring Session Options for more detailed information.
Show Targets	Use to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
Dashboard	The dashboard displays the statistics for all the applications, end points and the maps available in the monitoring session.

Button	Description
Ok / Cancel	**Ok:** Use to save the configurations in the monitoring session when the monitoring session is in undeployed state. **Cancel**: After the monitoring session is deployed, if you have made any changes and wish to remove them, use this option.
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 more detailed information.

Monitoring Session Options

Prefiltering, Precyption, Secure tunnel, User-defined applications, and Thresholds can be enabled for the monitoring session from the **Options** page.

To navigate to **Options** page, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. In the Edit Monitoring Session page, click **Options**. The **Options** page appears.

You can perform the following actions in the Options page:

- Enable Prefiltering
- Enable Precryption and Secure Tunnels
- Enable User Defined Applications
- Create Threshold

Enable Prefiltering

To enable Prefiltering, follow the steps given below:

1. In the **Monitoring Session Options** page, Click **Mirroring** tab.
2. Enable the **Mirroring** toggle button.
3. Enable the **Secure Tunnel** button if you wish to use Secure Tunnels. For more information about Secure Tunnel, refer to Secure Tunnels.

4. 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.
5. 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 and Secure Tunnels

To enable Precryption, follow the steps given below:

1. In the **Monitoring Session Options** page, Click **Precryption** tab.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic for more details on Precryption.
3. Enable the **Secure Tunnel** button if you wish to use Secure Tunnels. For more information about Secure Tunnel, refer to Secure Tunnels.

Enable User Defined Applications

To enable user defined application, follow the steps given below:

1. In the **Monitoring Session Options** page, Click **User-Defined Apps** tab.
2. Enable the **User-defined Applications** toggle button. Refer to User Defined Application for more detailed information User Defined Applications and how to configure it.

Create Threshold

To create threshold, follow the steps given below:

1. In the **Monitoring Session Options** page, Click **Threshold** tab.
2. Refer toTraffic Health Monitoring topic for more detailed information on how to create threshold template and apply the templates to the monitoring session.

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**.

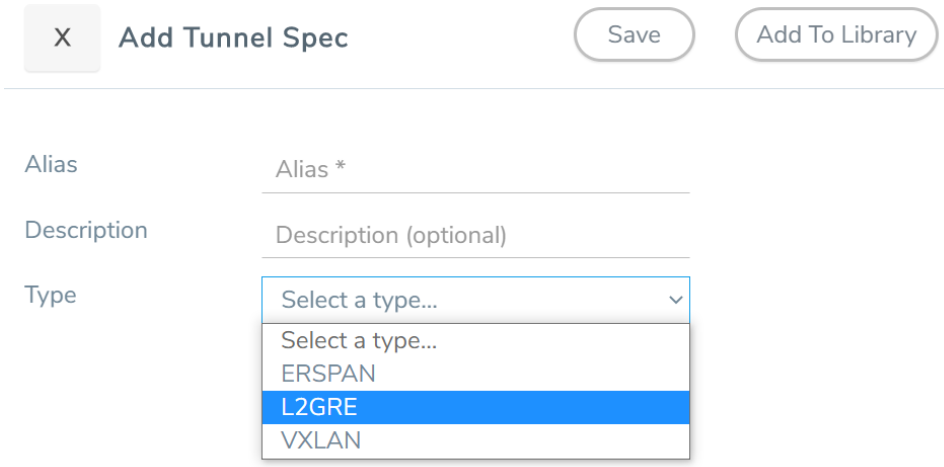
Create Ingress and Egress Tunnels

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, UDP, or ERSPAN tunnel.

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

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, TLS-PCAPNG, UDP, 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,

Field	Description	
		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
	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.		

Field	Description	
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.
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. Select IPv4 or IPv6.
	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.
Out	**Remote Tunnel IP**	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Configure Physical Tunnel	Configure the Physical Tunnel from your GigaVUE V Series monitoring session for an Ingress Tunnel. Save your changes before moving towards the Physical Tunnels configuration page.

Field	Description	
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) 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.
UDP:		

Field	Description	
Out	**L4 Destination IP Address**	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. Refer to Application Metadata Exporter for more detailed information on what AMX application is and how to configure it.
	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.

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.

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

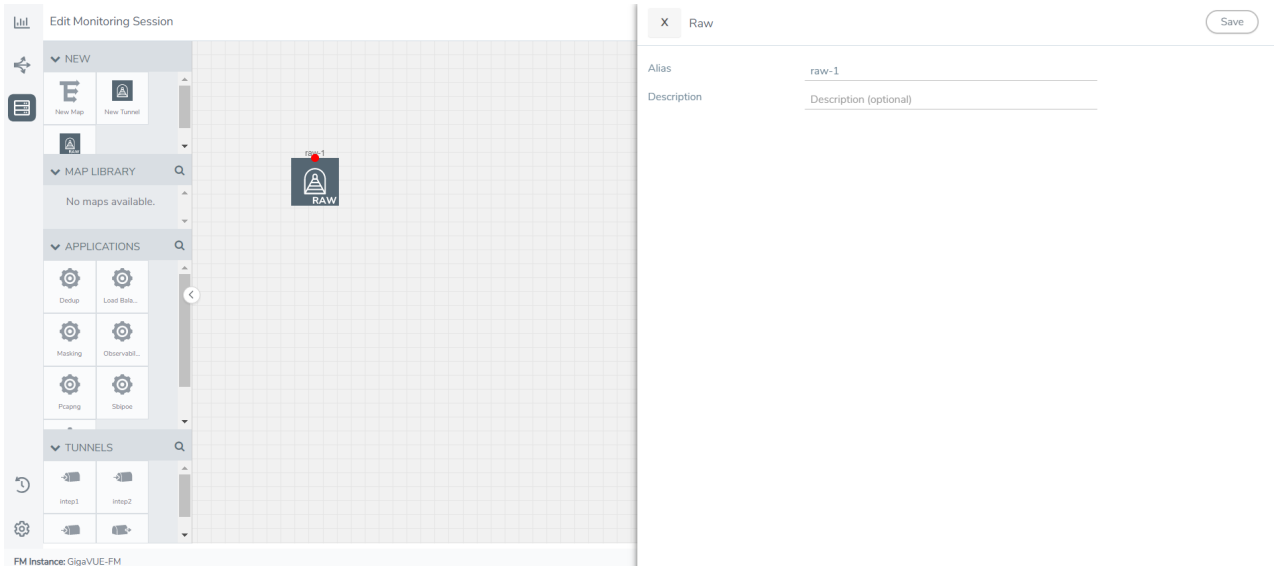
After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When 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**.



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:

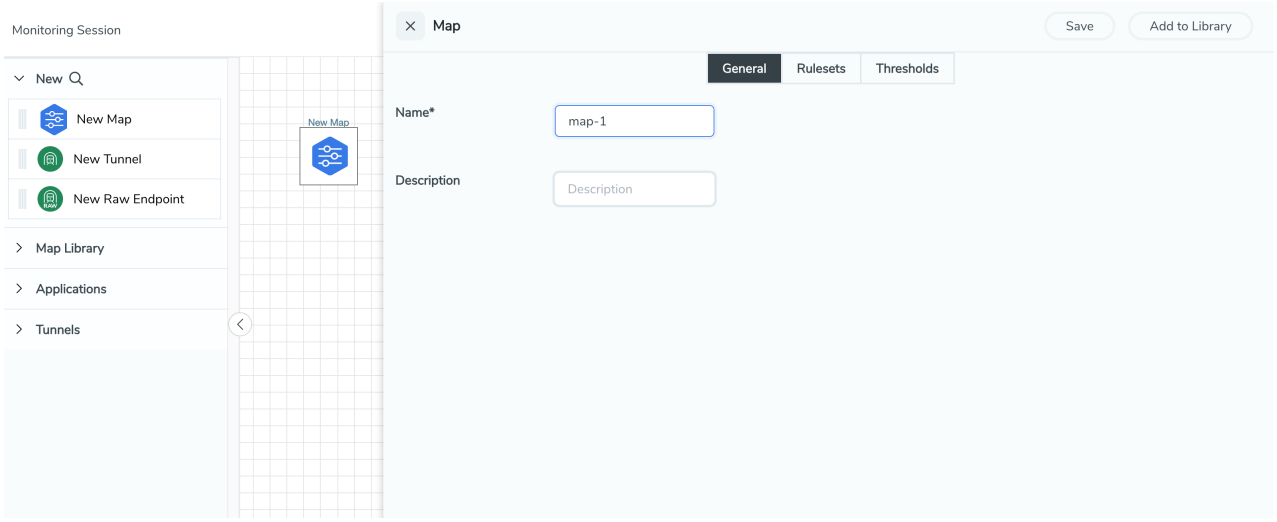
Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and

	the (egress or ingress) direction of tapping the network traffic.
Priority	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.



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. 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.

Map Library

To reuse a map,

1. In the Monitoring Session page, Click **Actions > Edit**. The Edit Monitoring Session page opens.
2. Click the map you wish to save as a template. Click **Details**. The Application quick view appears.
3. Click **Add to Library**. Save the map using one of the following ways:

4. Select an existing group from the **Select Group** list or create a **New Group** with a name.
5. Enter a description in the **Description** field, and click **Save**.

The Map is saved to the **Map Library** in the Edit Monitoring Session Canvas page. This map can be used from any of the monitoring session. To reuse the map, drag and drop the saved map from the Map Library.

Add Applications to Monitoring Session

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

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

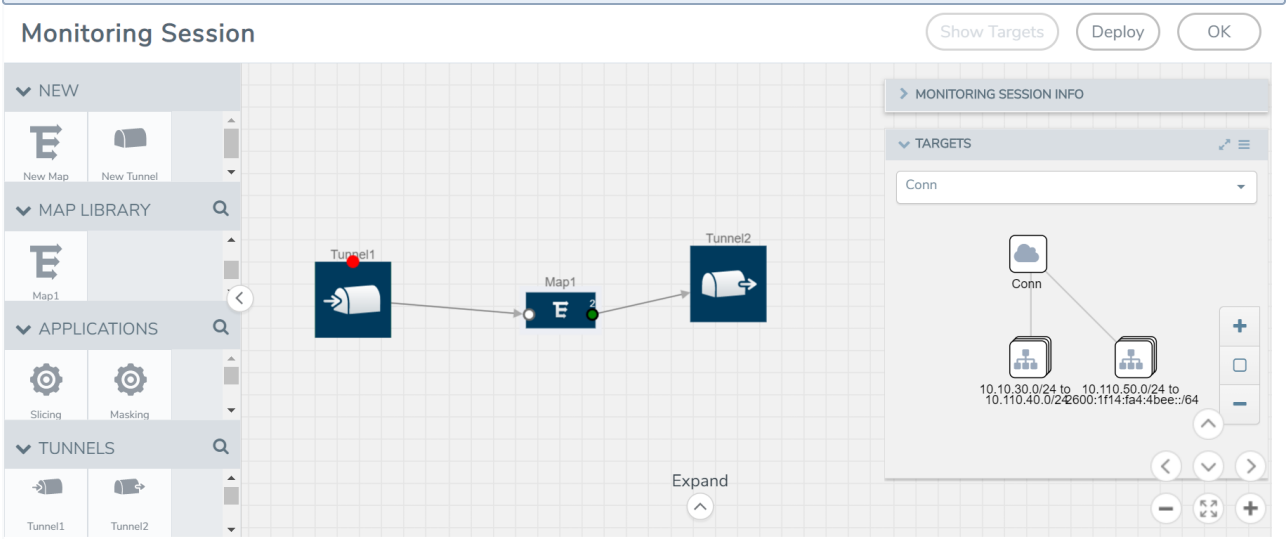
For more detailed information on how to configure these application, refer to *GigaVUE V Series Applications Guide*.

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.

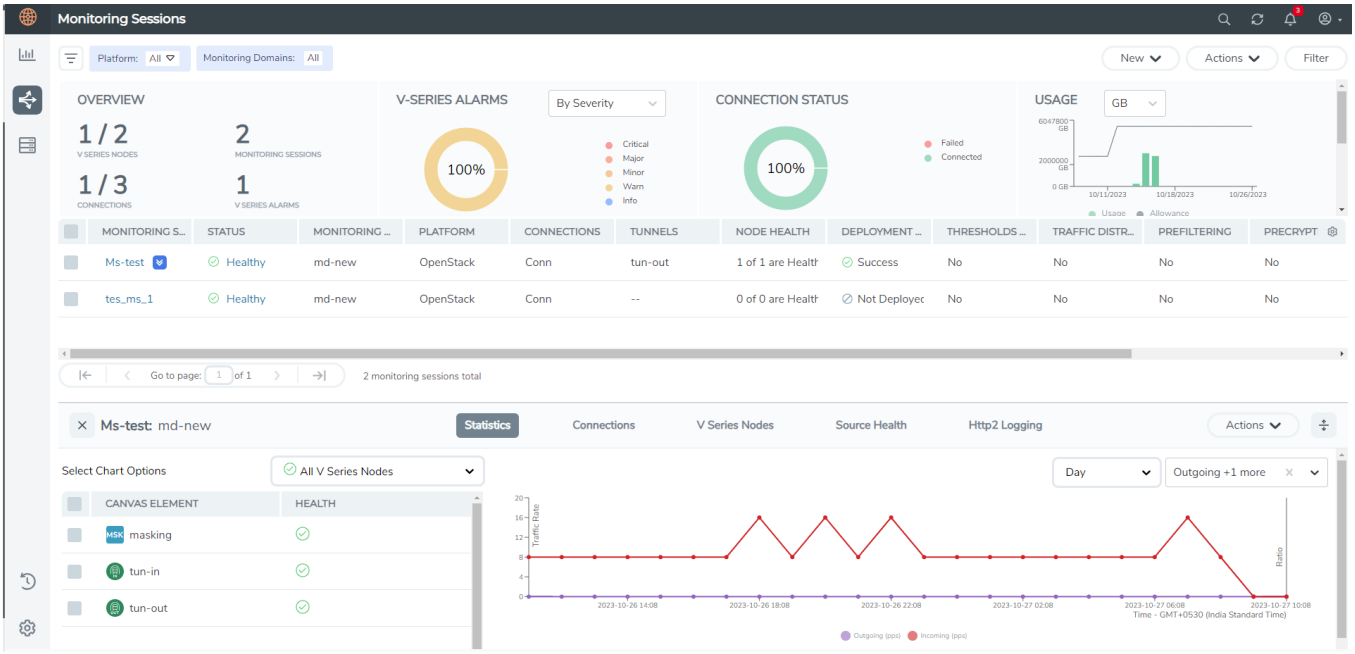
The Monitoring Session page also has the following options under the **Actions** button:

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 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.

On the Monitoring Sessions page, click the name of the monitoring session, and then click **View**. A split window appears displaying the **Statistics**, **Connections**, **V Series Nodes**, **Source Health** and **Http2 Logging** of the monitoring session as shown:



To know more about the statistics of the session, click **Statistics**.

You can view the statistics by applying different filters as per the requirements of analysing the data. GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- You can view the **Statistics** in full screen. To view in full screen, click the **Actions** drop-down list at the right corner of the window, and select **Full Screen**. **Statistics** appear in full screen.
- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can select the options from the drop-down list box.
- You can filter the traffic and view the statistics based on factors such as **Incoming**, **Outgoing**, **Ratio (Out/In), Incoming Packets**, **Outgoing Packets**, **Ratio (Out/In) Packets**. You can select the options from the drop-down list box.
- 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** from the drop-down list 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.

- You can view the statistics of the elements involved in the monitoring session. To view the statistics, click on the **Select Chart Options** page and select the elements associated with the session.
- Directly on the graph, you can click on **Incoming(Mbps)**, **Outgoing (Mbps)**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.

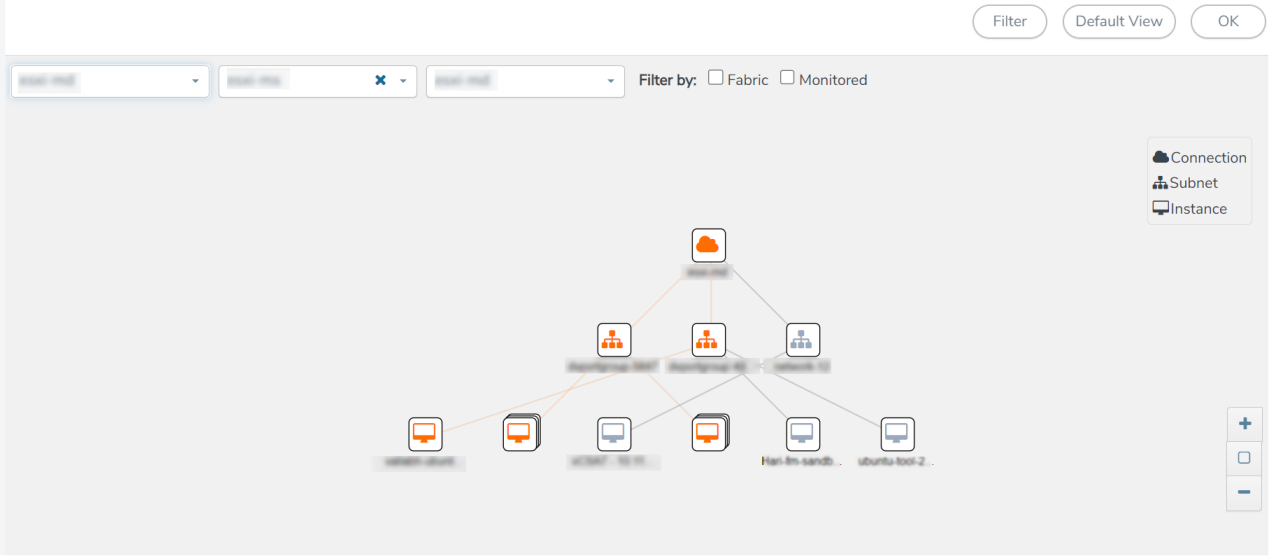
Visualize the Network Topology

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.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, Application Intelligence solution can be configured from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for virtual environment from the **Application Intelligence** page. The following operations can only be performed using the existing Application Intelligence Session:

- View Details
- Delete

- Forced Delete

It is highly recommended to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM will migrate all your virtual Application Intelligence sessions and their connections seamlessly. All sessions will be rolled back to their original states if the migration fails.

Points to Note:

- You must have **fm_admin** role in GigaVUE-FM to perform this migration. Refer to Configure Role-Based Access and Set Permissions for more detailed information how to create Users and assign Roles to the user.
- If any of the existing Application Intelligence Session is in PENDING or SUSPENDED, then the migration will not be triggered. Resolve the issue and start the migration process.
- If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration, then the migration will not be triggered. Resolve the issue and start the migration process.
- If an existing Monitoring Session has a same name as the Application Intelligence Session, then the migration will not be triggered. Change the existing Monitoring Session name to continue with the migration process.
- If any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set, you cannot continue with the migration. In the Monitoring Session either only Pass All or Advanced Rules as Drop is supported in the fifth Rule Set. Please delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for migrating the Application Intelligence Session in these scenarios.

To migrate your existing Application Intelligence Session to Monitoring Session Page, follow the steps given below:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**. You cannot create a new Application Intelligence Session from this page.
2. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
3. Review the message and click **Migrate.**
4. The **Confirm Migration** dialog box appears. The list Application Intelligence Session that will be migrated appears here.
5. Review the message and click **Migrate**.

6. GigaVUE-FM checks for the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
7. Click on the **Go to Monitoring Session Page** button to view the Application Intelligence Session that are migrated to the monitoring session page.

All the virtual Application Intelligence Sessions in the Application Intelligence page is migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

After migrating Application Intelligence session to Monitoring Session page, you must consider the following things:

1. If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow the steps given below.
   a. Enable Secure Tunnels in the **Options** page. Refer to Enable Prefiltering, Precryption, and Secure Tunnel topic more detailed information on how to enable secure tunnel for a monitoring Session.
   b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The monitoring session is undeployed.
   c. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.
   d. Add the Application Intelligence applications.
   e. Modify the Number of Flows as per the below table:

Cloud Platform	Instance Size	Maximum Number of Flows (Considers Secure Tunnels Configuration also)
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	Large (c5n.2xlarge)	300k
	Medium (t3a.xlarge)	100k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

NOTE: Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

   f. Click **Deploy**. Refer to Application Intelligence topic for more detailed information on how to deploy the Application Intelligence applications.

2. When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating theApplication Intelligence Session to the Monitoring Session and redeploying the monitoring session, a momentary loss in the statistical data of the Application Visualization application will be seen while redeploying the monitoring session.

3. After migrating the Application Intelligence Session to monitoring session, if you wish to make any configuration changes, then the GigaVUE V Series Node version must be greater than or equal to 6.3.00.

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

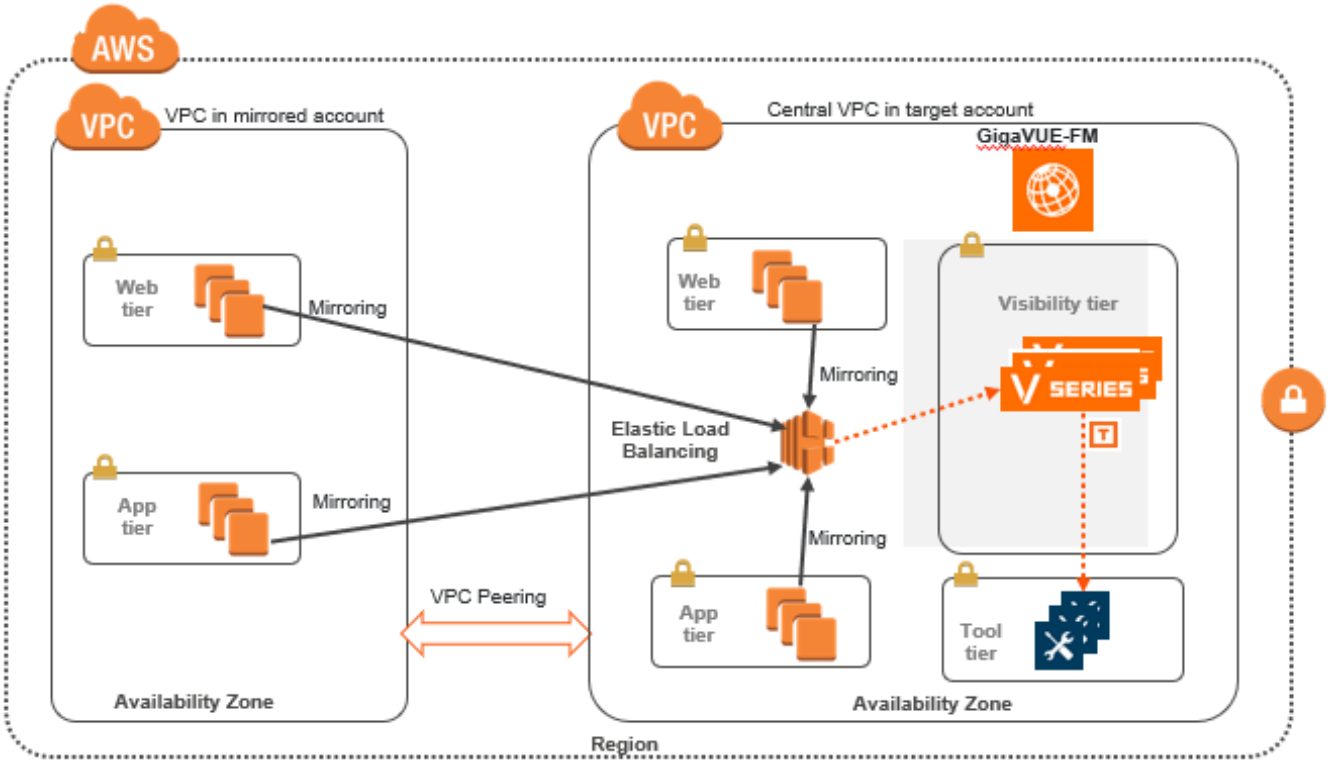
AWS Network Load Balancer on GigaVUE Cloud Suite

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 an External Load Balancer in AWS
- Deploy GigaVUE V Series Solution Elastic 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 an External 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 an external load balancer in AWS:

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

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

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

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

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

   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.

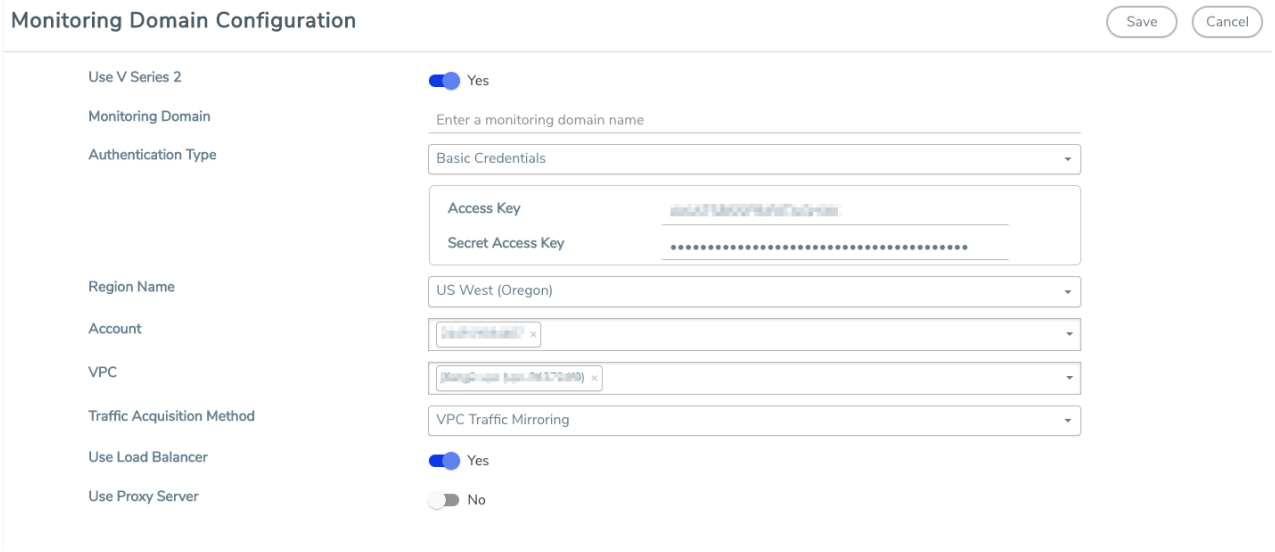
   NOTE: For detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in the AWS EC2 Auto Scaling document.

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

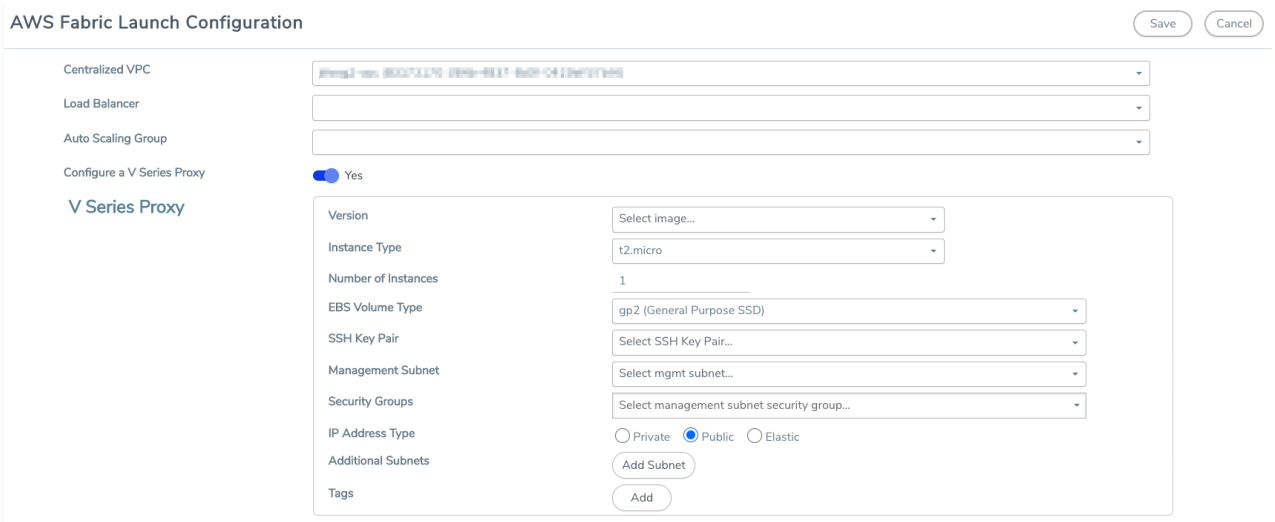
Deploy GigaVUE V Series Solution Elastic Load Balancing

To deploy GigaVUE V Series solution across the AWS accounts with Elastic 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.



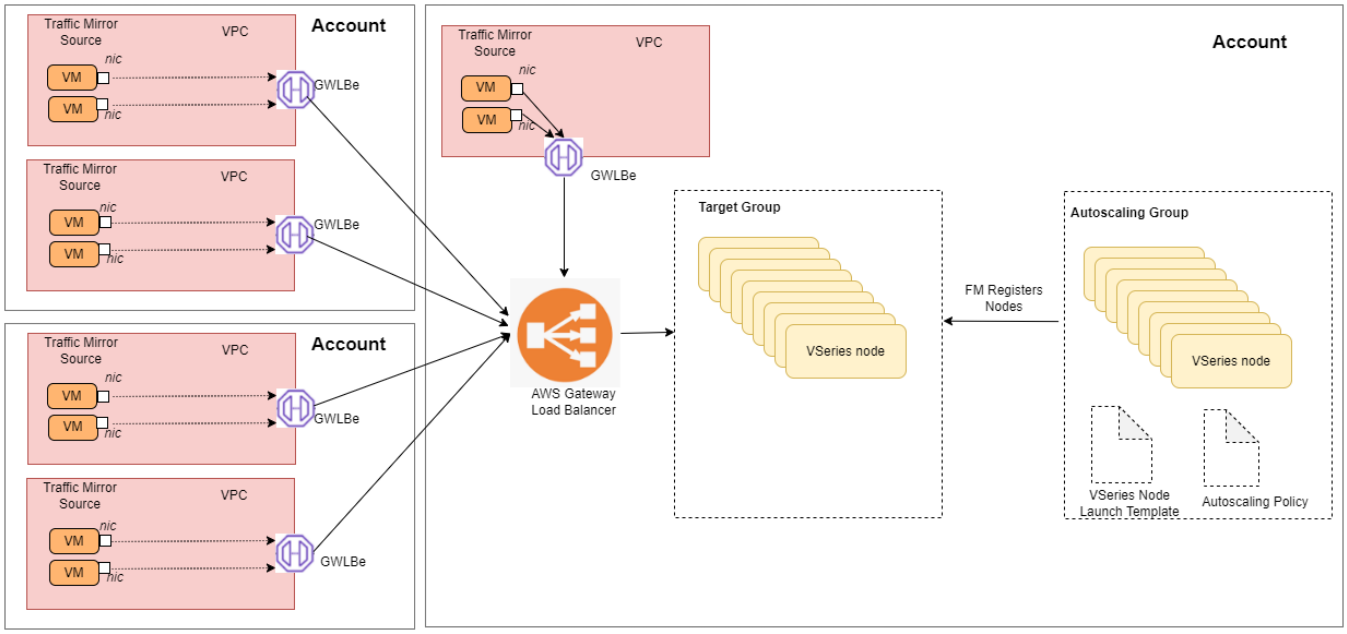
4. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
   - Select the Load Balancer configured in AWS
   - Select the Auto Scaling Group configured in AWS

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

Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS

The gateway load balancer (GWLB) uses the gateway load balancer end points to distribute the traffic across the end points. It is a VPC endpoint that provides connectivity in between virtual machines. With GWLB Endpoint as a target, mirrored traffic can be forwarded from any subnet. You can monitor network traffic across multiple VPCs and accounts, with centralized traffic inspection in a single VPC across their entire organization.

Architecture



In the architecture, you can see the deployment of GigaVUE Cloud Suite for AWS environments that have GWLB implementation for the security appliances, such as firewalls. In such deployments, the applications and your appliances are in different VPCs. The workload VPC is configured with the Gateway load balancer endpoint while the service VPC is configured with the Gateway load balancer. Gigamon deployed VPC has the solution components, such as GigaVUE-FM, GigaVUE V Series Nodes, and the OOB tools which consume the mirrored and decapsulated data.

Configure a Gateway Load Balancer in AWS

Prerequisites

- Create or update Security Group policies 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 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.
- For more information on AWS recommended design for Gateway Load Balancer implementation with inline services, such as firewall. see Getting started with Gateway Load Balancers - Elastic Load Balancing (amazon.com)
- You must create a VPC endpoint and endpoint service. For more information, see Create endpoint service
- Create a routing table. For more information, see Amazon documentation.

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.

Rules and Notes

- To avoid packet fragmentation, you should change the option Precryption-path-mtu in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.
- Protocol version IPv4 and IPv6 are supported.

- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must be 6.6.00 or above.

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.
Traffic Distribute	Enabling the "Traffic Distribute" option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.

4. Click **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Click **Options** button. The Monitoring Session Options appears.
6. Click **Precryption** tab.
7. Enable **Precryption**.
8. 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 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.

To know more, refer to Precryption™.

Check for Required IAM Permissions

GigaVUE-FM allows you to validate whether policy attached to the FM using "EC2 Instance Role" or "Access Credential" has the required IAM permissions and notifies the users about the missing permissions.

The following are the pre-requisite that are required to deploy GigaVUE Cloud Suite. You can validate them by clicking the **Check Permissions** button on the Create Monitoring Domain page and Create Fabric Launch page. The GigaVUE-FM displays the minimum required IAM permissions.

- IAM permissions - Checks whether the minimum required permissions are granted for the instance where the GigaVUE-FM is deployed.
- Access to public cloud end points - Checks for access to the AWS cloud end point APIs.
- Subscription to the Gigamon Cloud Suite - Before deploying the solution, you must subscribe to the GigaVUE Cloud Suite components from the AWS marketplace. It checks whether the required components are subscribed in the marketplace.
- Security group rules - Checks whether the required ports are configured in the security group. For more information on the security groups, see Security Group

  Note: Security group rules validation does not validate prefix List and user groups. For a successful validation, the ports and CIDR range should be updated in the Security Group.

After you press the **Check Permissions** button, GigaVUE-FM will verify the minimum required permissions. Any missing permissions will be highlighted in a dialog box. You can use the the displayed IAM Policy JSON as a reference and update the policy that is attached to the GigaVUE-FM.

You can view the permission status reports from Settings--> View Permissions. The reports are purged once in every 30 days.

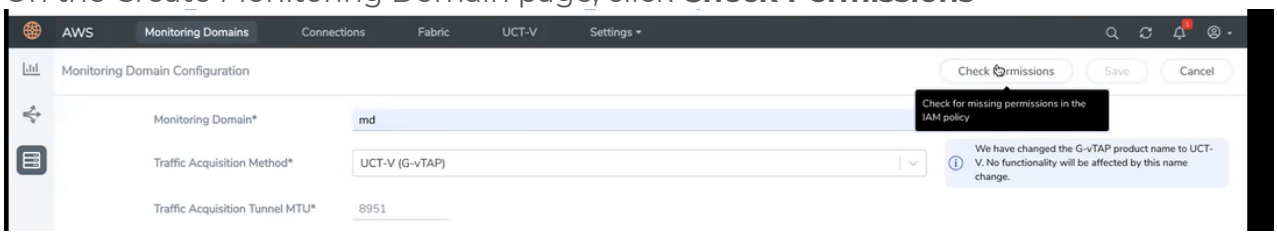
You can check permissions while configuring the following :

1. Monitoring Domain
2. GigaVUE Fabric components in GigaVUE-FM
3. VPC Mirroring

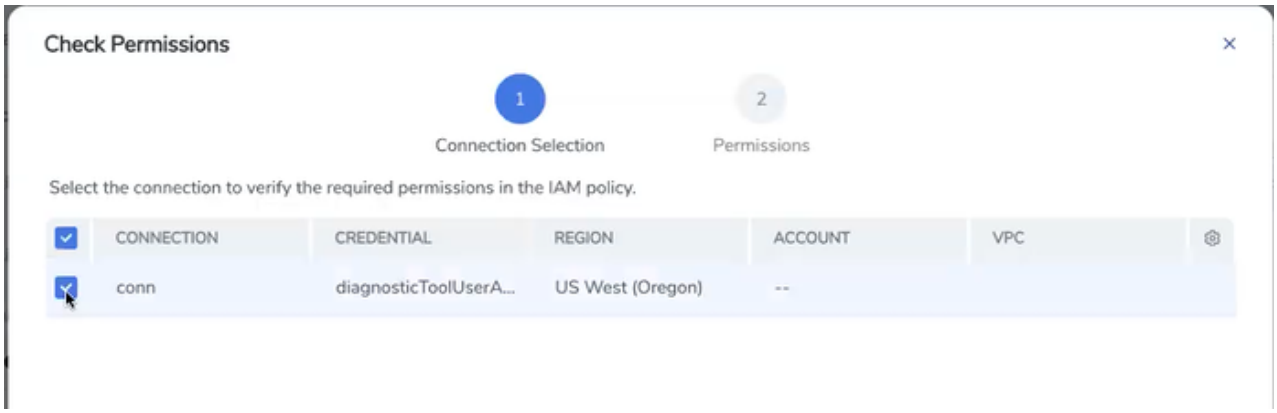
Check Permissions while configuring a Monitoring Domain

To check the permissions while creating a monitoring domain, do the following:

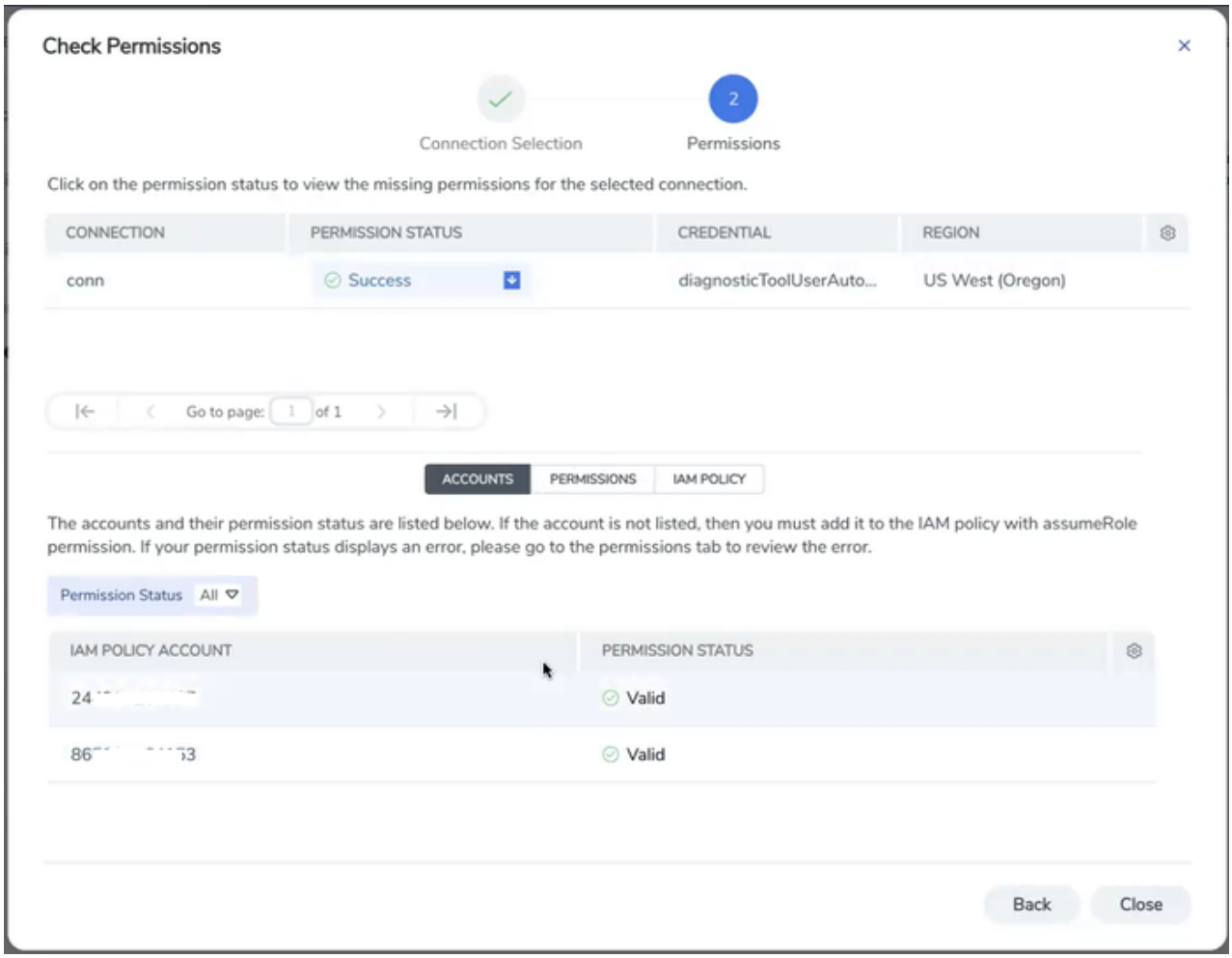
1. On the Create Monitoring Domain page, click **Check Permissions**



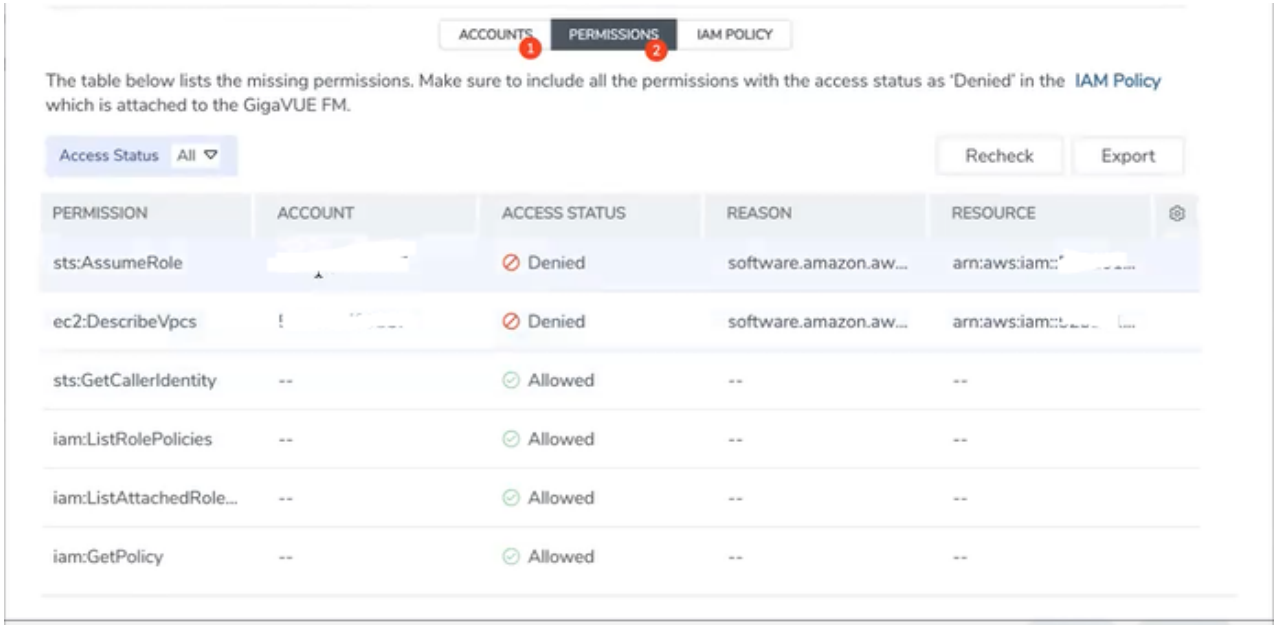
2. Select the connection and then click **Next.**



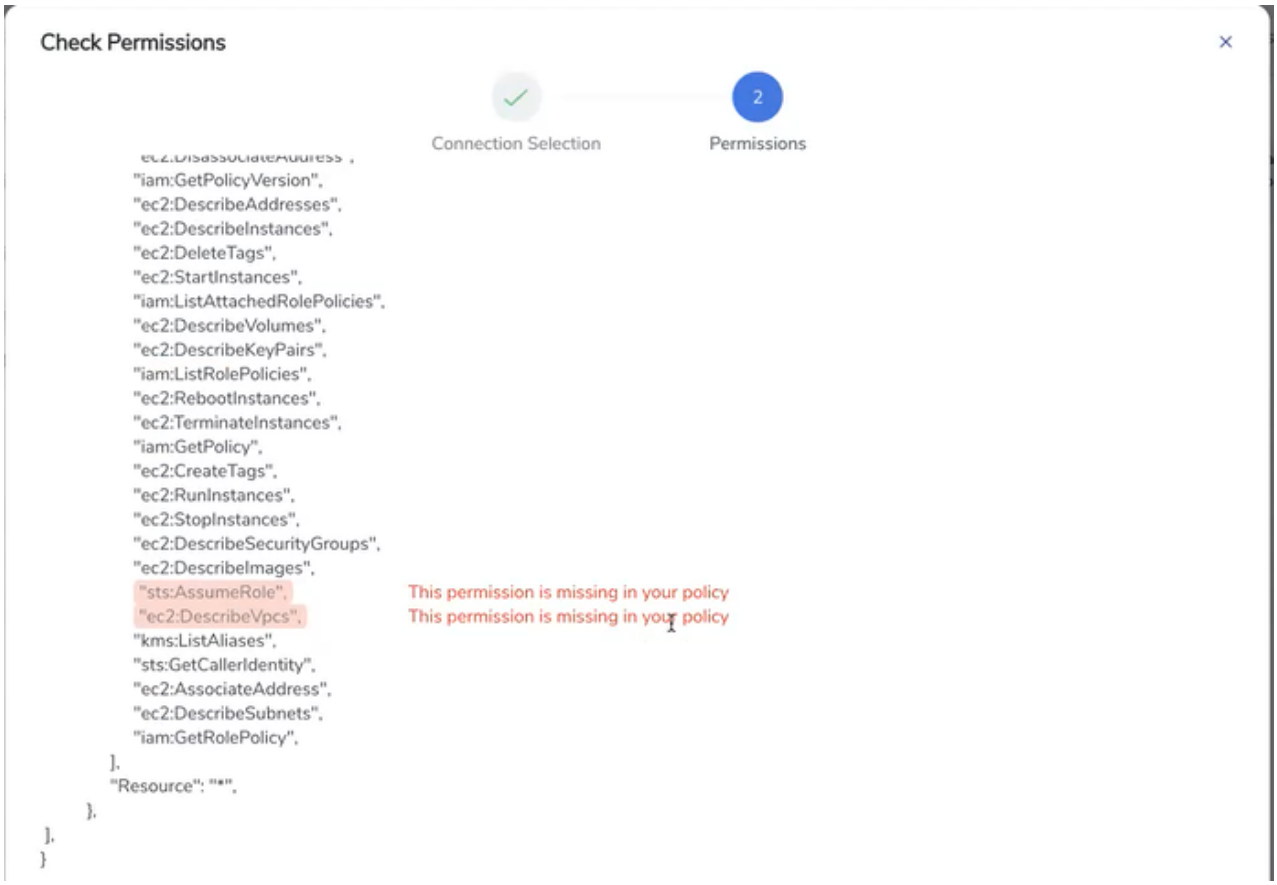
3. The accounts and the permissions status are listed under Accounts tab. Review the accounts that has an error in the permission status.



4. The permissions tab lists the permissions required to run GigaVUE Cloud Suite. Make sure to include all these permissions in the IAM policy with Access Status as 'Denied'.



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



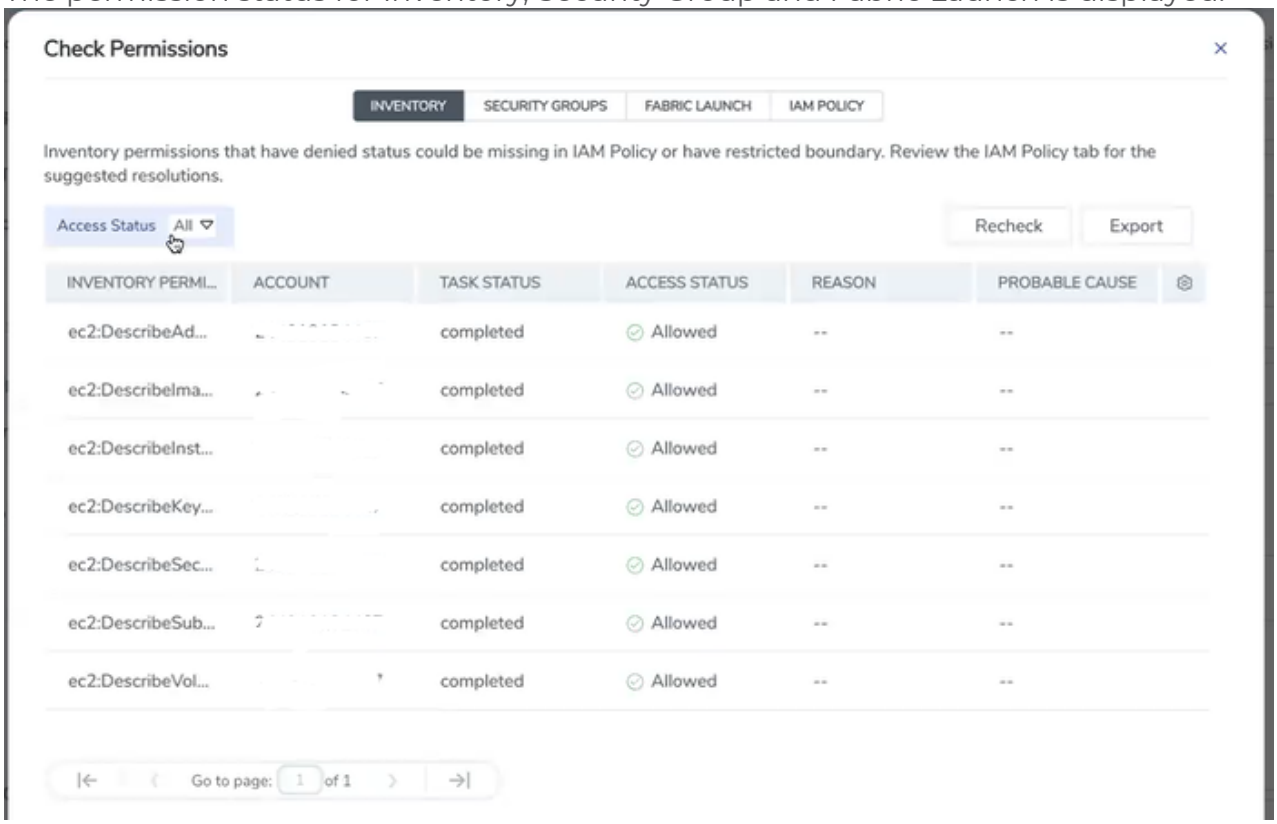
When you click Copy or Download, the entire JSON will be copied or downloaded.

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

Check Permissions while configuring GigaVUE Fabric components in GigaVUE-FM

To check for permissions from the AWS Fabric Launch page, do the following:

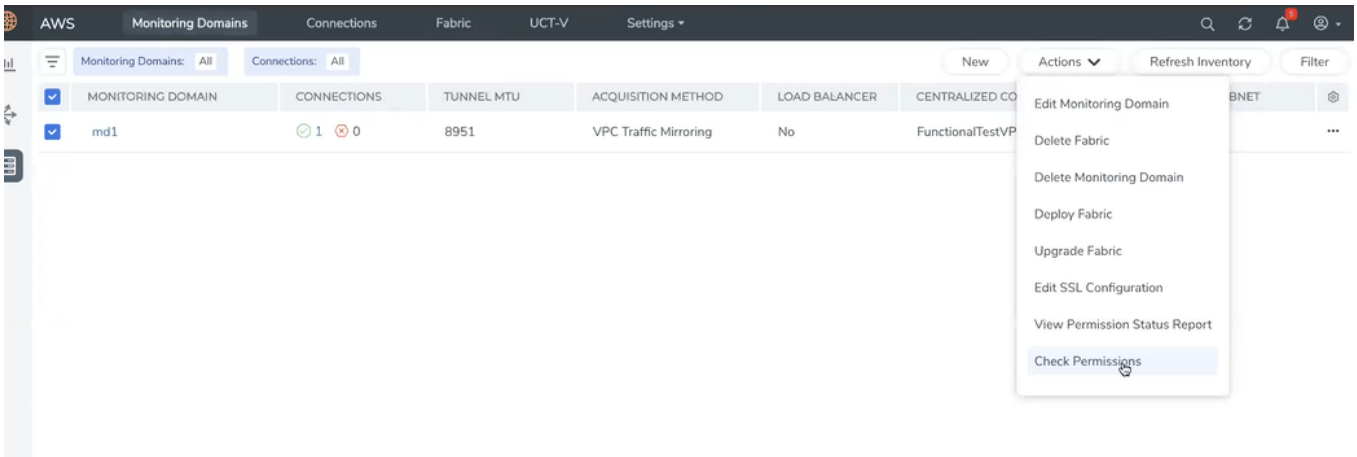
1. In the AWS Fabric Launch page, click **Check Permissions**
2. The permission status for Inventory, Security Group and Fabric Launch is displayed.



Note: Populating permissions status for Fabric launch takes a longer duration.

Check Permissions to acquire traffic using VPC mirroring

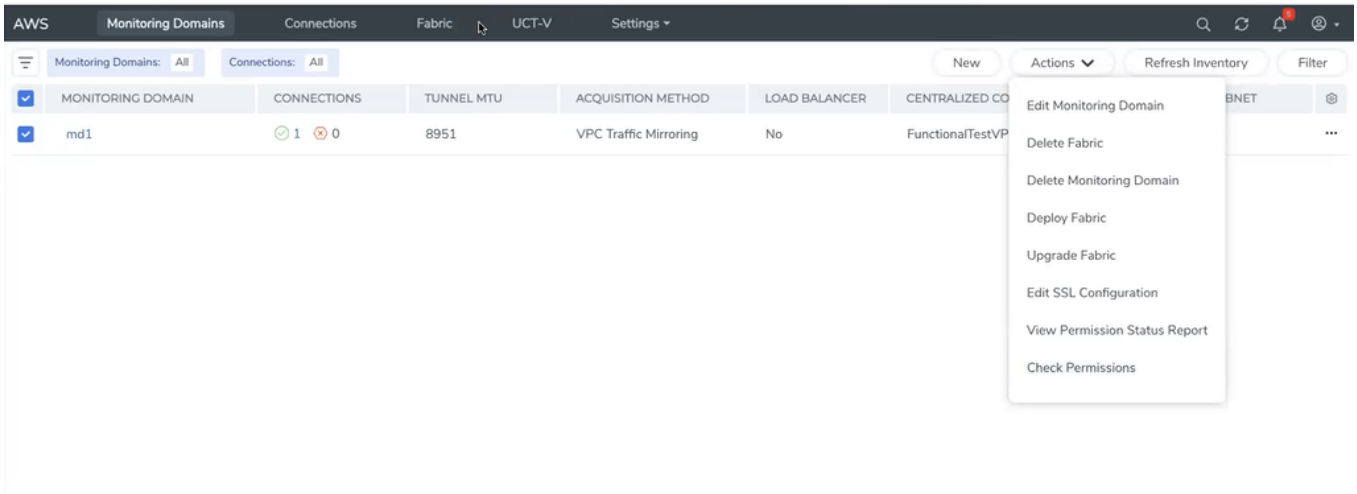
To check permissions to acquire traffic using VPC mirroring, navigate to the Monitoring Domain page, select the Monitoring Domain, click **Actions**, and then click **Check Permissions.**



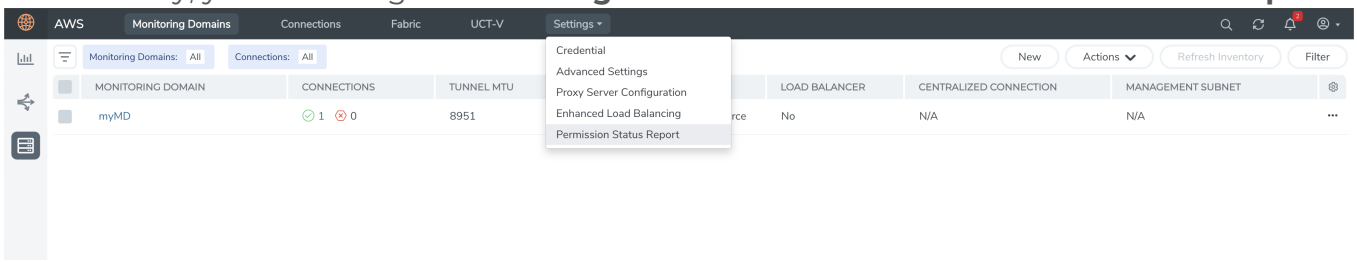
View permission status reports

Permission status reports consists previously ran Check permissions reports. They are auto purged once in 30 days. You can change the purge interval from the **advanced settings** page.

To view the reports, click **Actions** and then click View **Permission Status Report**.



Alternatively, you can navigate to **Settings** and then click **View Permission Status Report**



Upgrade GigaVUE-FM in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed in AWS.

Refer to the following sections for details:

- Upgrade GigaVUE-FM using Snapshot in AWS
- Upgrade from UI. For more information on upgrading from UI, refer to the Upgrade from UI topic in GigaVUE-FM Installation and Upgrade Guide.

At a Glance

To upgrade the GigaVUE-FM instance successfully, you must perform the following steps:

Step 1: Stop the existing version of the GigaVUE-FM instance.

Step 2: Create a snapshot of the second disk (dev/sdb) of the FM instance.

Step 3: Make a note of the snapshot ID.

Step 4: Launch the latest version of the GigaVUE-FM instance. While launching the latest version, enter the snapshot ID of the old version of the GigaVUE-FM instance in **Add Storage** > **Add New Volume**.

Step 5: Complete the launch.

Step 6: Verify if the data from the previous GigaVUE-FM instance is restored in the new instance.

Step 7: Terminate the old FM instance.

Stop GigaVUE Cloud Suite FM Instance

Before upgrading the GigaVUE-FM instance, the existing version of the GigaVUE-FM instance must be stopped.

NOTE: Do not terminate the GigaVUE-FM instance.

To stop the GigaVUE-FM instance:

1. Login to the AWS account and select **Services > EC2**.
2. In the left navigation pane, select **Instances**.
3. In the search field, enter the name of the existing GigaVUE-FM instance and select the Instance ID.

NOTE: If the instance ID is the password for logging in to the existing GigaVUE-FM, make note of this instance ID. This instance ID will be used as the password for logging in to the upgraded GigaVUE-FM as well. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

4. Go to **Instance State** > **Stop**.

Create Snapshot of the GigaVUE-FM Instance

You must create a snapshot of the volume of the existing version (dev/sdb) of the GigaVUE-FM instance. Snapshots capture data that are written to your Amazon EBS volume at the time the snapshot is taken. This excludes any data that are cached by any applications or the operating system.

To create a snapshot:

1. Select the GigaVUE-FM instance and click the **Description** tab.
2. Click **Storage** and locate Block Devices.
3. Click the **/dev/sdb** link. The Block Device dialog box is displayed with the volume ID link.
4. In the Block Device dialog box, click the volume ID link. The Volumes page is displayed.
5. Click **Actions** and select **Create Snapshot.**
6. Enter the description and tags.
7. Click **Create**.

NOTE: Make a note of the snapshot ID. This snapshot ID will be used to find the snapshot and add the volume while upgrading the GigaVUE-FM instance.

Upgrade GigaVUE-FM Instance

While upgrading the GigaVUE-FM instance, the Amazon EBS volume must be restored with the data from the snapshot that is created in Create Snapshot of the GigaVUE-FM Instance.

To upgrade the GigaVUE-FM instance:

1. Select **Services > EC2**.
2. Click **Launch Instance** and go to **AWS Marketplace** or **Community AMIs**.
3. Search for **Gigamon**, locate the latest version of the GigaVUE-FM AMI, and click **Select**.
4. Choose the Instance Type. The recommended instance type is **m4.xlarge**.
5. Click **Next: Configure Instance Details.**
6. Select the **Key pair(login)**
7. Enter the following information.
   - **Network**— Select the VPC where you want to launch the AMI.
   - **Subnet**— Select the management subnet that the instance will use after launch. (Required)
   - **Auto-assign Public IP**— Select **Enable**.
   - **Security group:** Select the security group
8. Click **Configure storage** and then click **Advanced**.
9. Select **Volume 2** and then select the Snapshot that you created in Create Snapshot of the GigaVUE-FM Instance.
10. Click **Advance Details** and then select **IAM Instance Profile**.
11. Click **Launch Instances**.
12. It will take several minutes for the instance to initialize. After the initialization is completed, verify the instance through the Web interface as follows:
    a. Find the instance and expand the page in the **Descriptions** tab to view the instance information, if necessary.
    b. Copy the Public IP address and paste the value into a new browser window or tab.
    c. Copy the Instance ID of the previous version of the GigaVUE-FM. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

NOTE: Do not have multiple versions of GigaVUE-FM instances monitoring the same AWS connection.

Launch the new version of the GigaVUE-FM instance. Verify if the data from the previous GigaVUE-FM instance is restored in the new instance. Once the data is verified, terminate the old version of the GigaVUE-FM instance.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes. For more detailed information about UCT-V, UCT-V Controller, GigaVUE V Series Proxy and Node Version refer GigaVUE-FM Version Compatibility Matrix.

Refer to the following topic for more information:

- Prerequisite
- Upgrade UCT-V Controller
- Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes, you must upgrade GigaVUE-FM to software version 5.13 or above.

Upgrade UCT-V Controller

NOTE: UCT-V Controllers cannot be upgraded. Only a new version that is compatible with the UCT-V's version can be added or removed in the **AWS Fabric Launch Configuration** page.

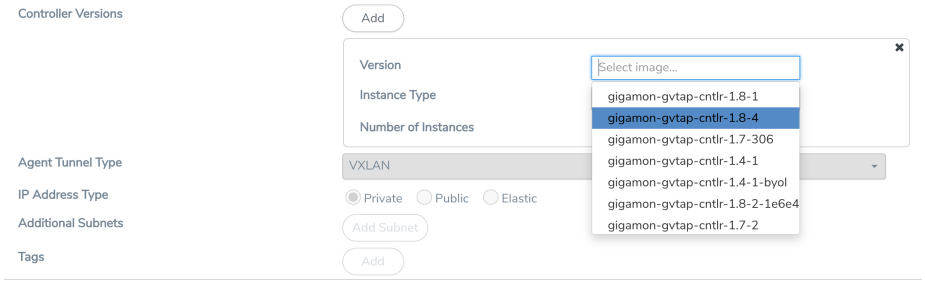
To change the UCT-V Controller version follow the steps given below:

To change UCT-V Controller version between different major versions

NOTE: You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 1.8-x if your existing version is 1.7-x.

a. Under **Controller Versions**, click **Add**.
b. From the **Version** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
c. From the **Instance Type** drop-down list, select a size for the UCT-V Controller.

d. In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.



You cannot change the IP Address Type and the Additional Subnets details, provided at the time of UCT-V Controller configuration.

After installing the new version of UCT-V Controller, follow the steps given below:

1. Install UCT-V with the version same as the UCT-V Controller.
2. Delete the UCT-V Controller with older version.

To change UCT-V Controller version with in the same major version

This is only applicable if you wish to change your UCT-V Controller version from one minor version to another within the same major version. For example, from 1.8-2 to 1.8-3.

a. From the **Version** drop-down list, select a UCT-V Controller image with in the same major version.
b. Specify the **Number of Instances**. The minimum number you can specify is 1.
c. Select the **Subnet** from the drop-down.

- You cannot modify the rest of the fields.
- After installing the new version of UCT-V Controller with the same version.

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes at a time.

There are two ways to upgrade the GigaVUE V Series Proxy and Nodes. You can:

- Launch and replace the complete set of nodes and proxy at a time.

  For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and Nodes are deleted from the VPC.

  NOTES:

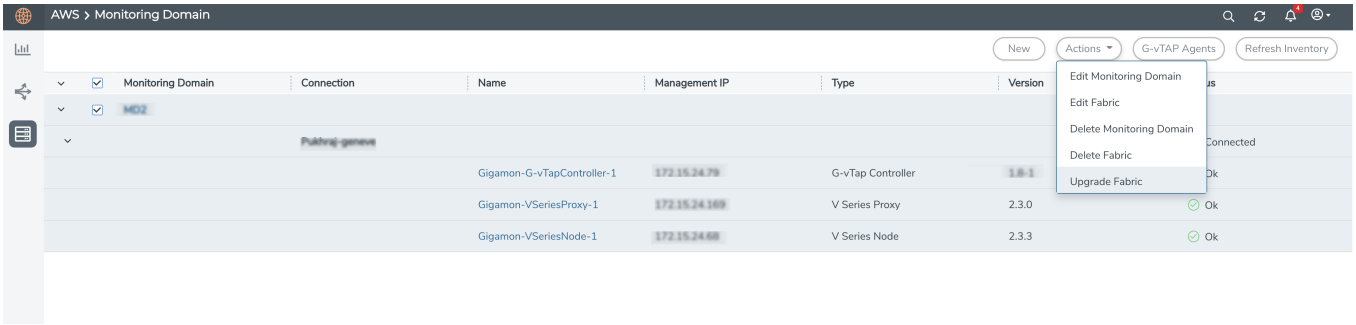
- When the new version of nodes and proxy are launched, the old version is not deleted by GigaVUE-FM until the new version of node and proxy is launched and the status is changed to **Ok**. Make sure that the instance type of the node and proxy selected during the configuration can accommodate the total number of new and old fabric nodes present in the VPC. If the instance type cannot support so many Virtual Machines, you can choose to upgrade the fabric nodes in multiple batches.
- If there is an error while upgrading the complete set of proxy and nodes present in the VPC, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
- Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of free addresses are available in the respective subnets. Otherwise, the upgrade will fail.
- Do not configure floating IPv4 for an IPv6-only management /data subnet. Floating IPv4 is not applicable for IPv6-only subnet.

- Launch and replace the nodes and proxy in multiple batches.

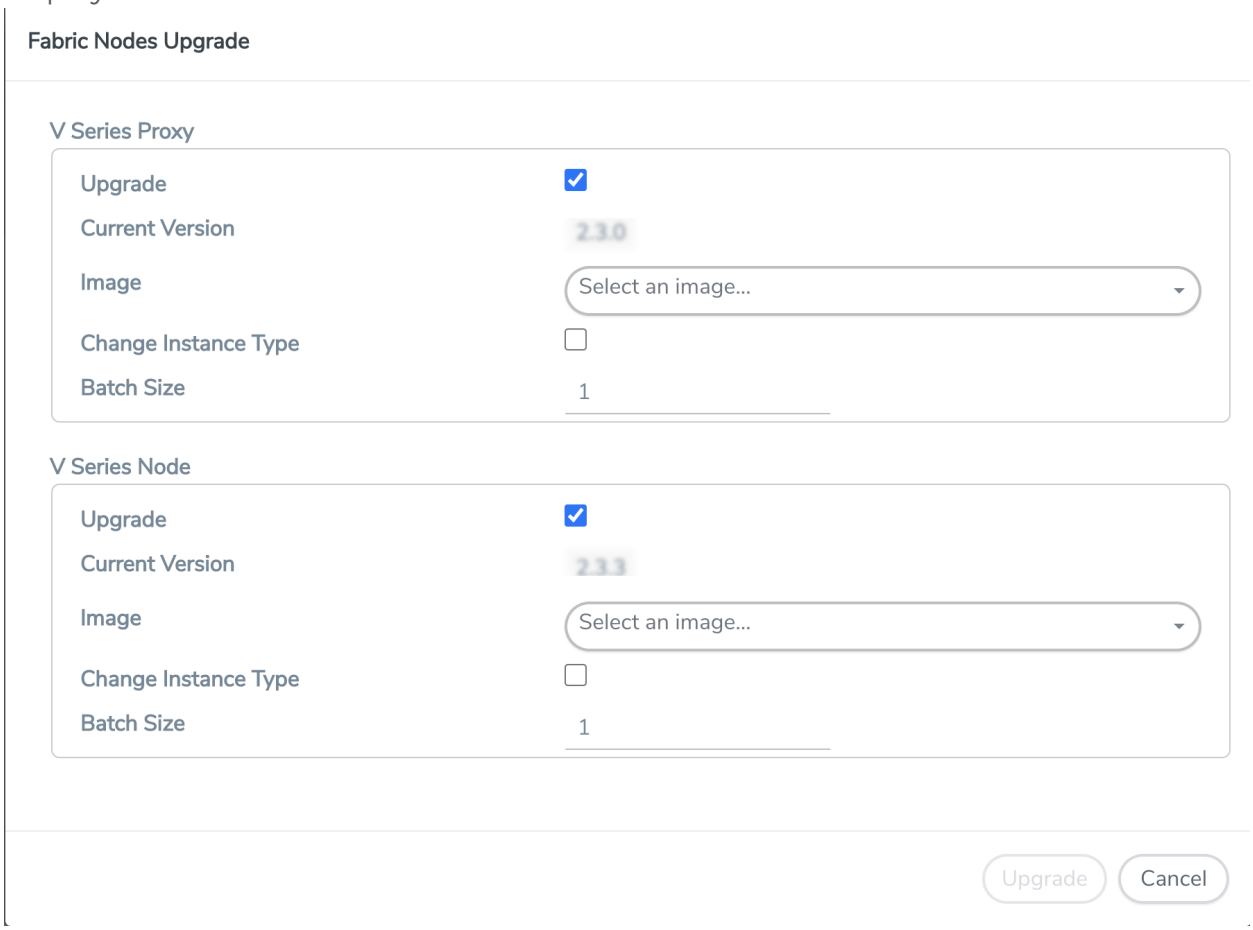
  For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes:

1. Go to **Inventory > VIRTUAL > AWS** , and then click **Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The Fabric Nodes Upgrade page is displayed.



4. To upgrade the GigaVUE V Series Nodes/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy/Nodes.
6. Select the **Change Instance Type** checkbox to change the instance type of the nodes/proxy, only if required.
7. To upgrade the GigaVUE V Series Nodes/Proxy, specify the batch size in the **Batch Size** box.

   For example, if there are 7 GigaVUE V Series Nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series Nodes in each batch. In the last batch, the remaining 1 V Series Node is launched.
8. Click **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V Series Proxy and Nodes upgrading in your AWS environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. In the V Series Proxy page, click the link under Progress to view the upgrade status.

Once the nodes are upgraded successfully, the monitoring session is re-deployed automatically.

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 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
- Third Party Orchestration

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:

- Supported Resources and Metrics
- Create Threshold Template
- Apply Threshold Template

- Edit Threshold Template
- Clear Thresholds

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.

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
RawEnd Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
Map	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Slicing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
HeaderStripping	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
TunnelEncapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Template

To create threshold templates:

1. There are two ways to navigate to the Threshold Template page, they are:
   a. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
   b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a monitoring session, click **Actions > Edit**. In the Edit Monitoring Session page, click **Options > Threshold**.
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.
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

View Health Status

You can view the health status of the monitoring session on the Monitoring Session details page. The health status of the monitoring session is healthy only if both the configuration health and traffic health are healthy.

View Health Status of an Application

To view the health status of an application across an entire monitoring session:

1. After creating a Monitoring Session, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a monitoring session, click **Actions > Edit**. The Edit Monitoring Session Page appears.
2. Click on the application for which you wish to see the health status and select **Details**. The quick view page appears.
3. Click on the **HEALTH STATUS** tab.

This displays the configuration health and traffic health of the application and also the thresholds applied to that particular application.

NOTE: The secure tunnel status is refreshed for every 5 minutes, and the GigaVUE-FM does not display UCT-V secure tunnel status that is older than 7 minutes. If the secure tunnel in the UCT-V is removed, it takes up to 7 minutes to reset the status on the GigaVUE-FM.

View Health Status for Individual GigaVUE V Series Nodes

You can also view the health status of the view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Statistics** tab.
3. Select the GigaVUE V Series Node from the **All V Series Nodes** drop-down menu.

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 the name of the monitoring session and click **View**.
2. Select the **Statistics** tab.
3. Select the GigaVUE V Series Node from the **All V Series Nodes** drop-down menu.
4. The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

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**.

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.
Reboot threshold limit for UCT-V Controller down	Specifies the number of times GigaVUE-FM tries to reach UCT-V Controller, when the UCT-V Controller moves to down state. GigaVUE-FM retries every 60 seconds.

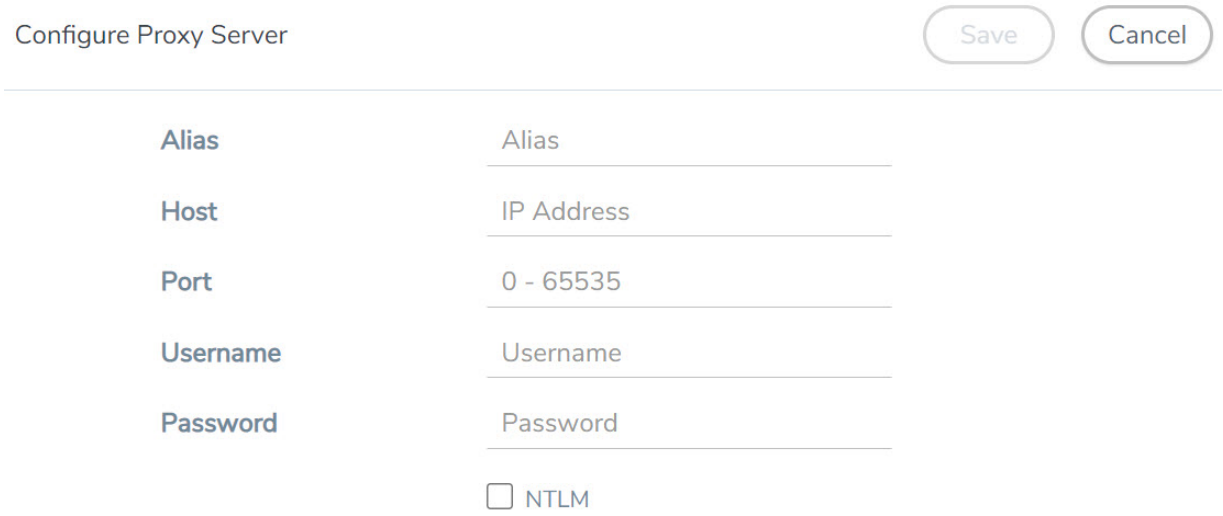
Configure Proxy Server

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

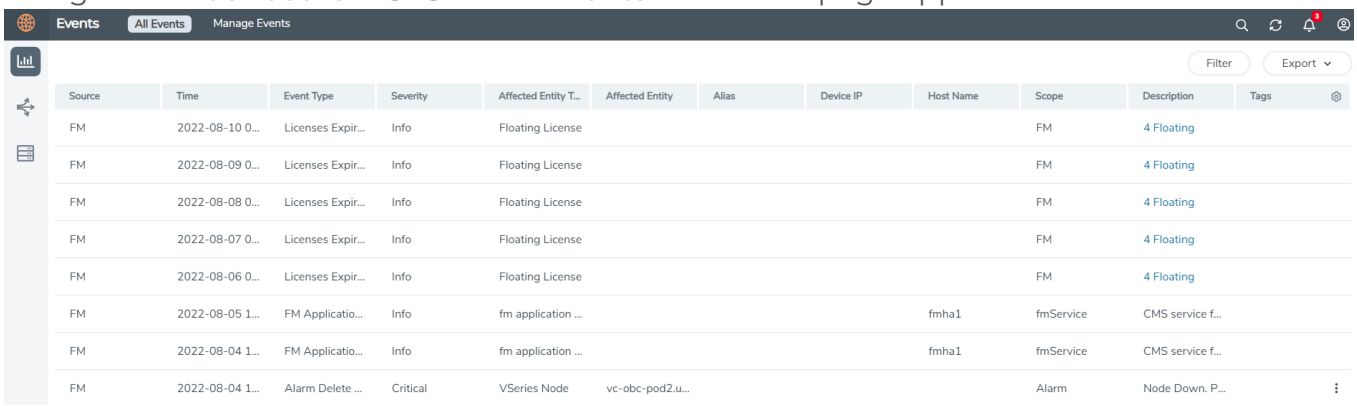
The Events page displays all the events occurring in the virtual fabric component, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- Cloud provider License Expiry
- UCT-V Inventory Update Completed
- Cloud provider Connection Status Changed

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. An example of alarm could be your cloud provider license expiry.

The alarms and events broadly fall into the following categories: Critical, Major, Minor, or info.

Navigate to **Dashboard > SYSTEM > Events**. The Event page appears.



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 GigaVUE-FM fabric manager. ▪ IP address - is the address of the GigaVUE HC Series node that detected the event. For a node to be able to send notifications to the GigaVUE-FM fabric manager, the SNMP_TRAP must be configured with the GigaVUE-FM 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.

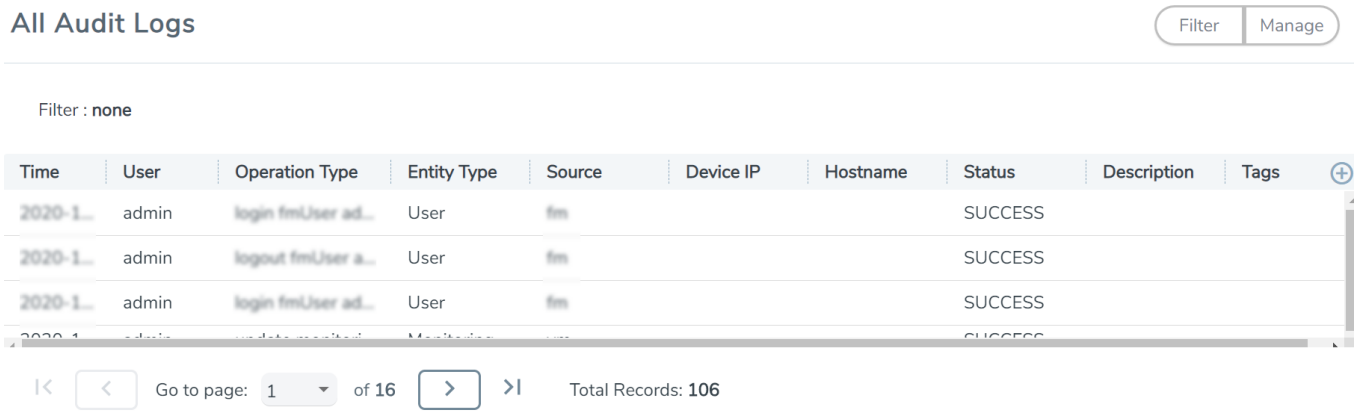
To filter the alarms and event:

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.



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 GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

NOTE: Ensure that the GigaVUE-FM time is set correctly to ensure accuracy of the trending data that is captured.

Filtering the audit logs allows you to display specific type of logs. You can filter based on any of the following:

- **When**: display logs that occurred within a specified time range.
- **Who**: display logs related a specific user or users.
- **What**: display logs for one or more operations, such as Create, Read, Update, and so on.
- **Where**: display logs for GigaVUE-FM or devices.
- **Result**: display logs for success or failure.

To filter the audit logs, do the following:

1. Click **Filter**. The quick view for Audit Log Filters displays.
2. Specify any or all of the following:
   - **Start Date** and **End Date** to display logs within a specific time range.
   - **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
   - **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
   - **Where** narrows the logs to particular of system that the log is related to, either GigaVUE-FM or device. Select **All Systems** apply both GigaVUE-FM and device to the filter criteria.
   - **Result** narrows the logs related to failures or successes. Select All Results to apply both success and failure to the filter criteria.
3. Click **OK** to apply the selected filters to the Audit Logs page.

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 6.6 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
6.6.00	v6.6.00	v6.6.00	v6.6.00	v6.6.00	v6.6.00
6.5.00	v6.5.00	v6.5.00	v6.5.00	v6.5.00	v6.5.00
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

GigaVUE-FM	G-vTAP Agent Version	Next GenerationG-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series Nodes
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
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 6.6 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-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide

GigaVUE Cloud Suite 6.6 Hardware and Software Guides
GigaVUE-TA100 Hardware Installation Guide
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 Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE 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 (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

GigaVUE Cloud Suite 6.6 Hardware and Software Guides
Universal Cloud Tap - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon.
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "6.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 6.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	**Document Title**	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	**Describe the issue**	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? **Be as specific as possible.**	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings**  **> Support > Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)