



GigaVUE Cloud Suite Deployment Guide - Oracle Cloud Infrastructure

Product Version: 6.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.14	1.0	07/10/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE Cloud Suite Deployment Guide - Oracle Cloud Infrastructure	1
Change Notes	2
Contents	3
Oracle Cloud Infrastructure	5
GigaVUE Fabric Components and Deployment Options	6
Key Concepts	9
Monitoring Domain	10
Monitoring Session	13
Secure Communication between GigaVUE Fabric Components	15
Precryption™	16
Secure Tunneling to GigaVUE V Series Nodes	23
Traffic Acquisition	24
Traffic-Flow-Across-Components	24
Deployment Prerequisites	26
Supported Compute Requirements for OCI	26
Network Requirements	27
Network Firewall Requirements	27
Default Login Credentials	36
Integrate Private CA	36
Adding Certificate Authority	38
SSL Decrypt	38
Deploy Fabric Components using Generic Mode	47
Acquire Traffic using UCT-V	48
Acquire Traffic using Customer Orchestrated Source	68
Configure Secure Tunnel for OCI	89
Precrypted Traffic	89
Mirrored Traffic	89
Prerequisites	89
Notes	90
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node	90
Configure Secure Tunnel between GigaVUE V Series Nodes	91
Viewing Status of Secure Tunnel	94
Configure UCT-V Features	95
Configure Prefiltering	95

Create Precryption Template for UCT-V	97
Configure Precryption in UCT-V	102
Configure Monitoring Session	103
Create a Monitoring Session	104
Create Ingress and Egress Tunnel	107
Create Raw Endpoint	115
Create a New Map	116
Add Applications to Monitoring Session	121
Deploy Monitoring Session	121
Monitor Cloud Health	125
Configuration Health Monitoring	125
View Health Status	125
Traffic Health Monitoring	128
View Monitoring Session Statistics	134
Visualize the Network Topology	134
Administer GigaVUE Cloud Suite for OCI	136
Configure Certificate Settings	136
Interface Mapping	136
Configure Third Party Orchestration Settings	137
About Audit Logs	139
Debuggability and Troubleshooting	141
Sysdumps	141
Additional Sources of Information	144
Documentation	144
Documentation Feedback	147
Contact Technical Support	148
Contact Sales	149
The VÜE Community	149
Glossary	150

Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) delivers a cloud-native visibility and analytics solution. It enables full network observability so you can:

- Migrate workloads to the cloud
- Optimize your existing cloud environment

Gigamon provides clear visibility into network traffic across your environment, helping you eliminate blind spots, reduce security and compliance risk, and resolve performance issues faster.

Traffic Acquisition

OCI captures network traffic from workloads running in OCI.

It uses a simple and efficient process:

- Copies and mirrors traffic through tunnels.
- Sends the traffic to GigaVUE V Series Nodes.
- These nodes filter and process the packets.
- The processed traffic goes to your security and monitoring tools.

Traffic can be acquired in several ways, including:

- Universal Cloud Tap (UCT)
- OCI Traffic Mirroring

Unified Data Visibility

The suite gives you a single, clear view of all data in motion. It works across single, hybrid, and multi-cloud networks.

OCI:

- Collects traffic from any source
- Optimizes it automatically
- Delivers it to any destination

This end-to-end visibility helps your tools analyze raw packet data, application-layer information, and enriched metadata. You can detect threats, improve performance, and make better decisions faster.

Enriched Metadata

GigaVUE Enriched Metadata (GEM) turns raw packet data into actionable insights.

GEM:

- Extracts and enriches metadata
- Sends enriched data to security and analytics tools
- Speeds up threat detection and performance monitoring
- Links platform metadata with real packet data

Key Capabilities

OCI offers powerful features, including

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

GigaVUE Fabric Components and Deployment Options

You can deploy GigaVUE Fabric Components in your OCI cloud environment and configure to support the visibility policies you have defined.

OCI includes the following fabric components:

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

You can use the following approach to deploy GigaVUE Fabric Components:

OCI Orchestrated Fabric Deployment

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

When deploying fabric components through an external orchestration system,

- You can provide the necessary parameters for self-registration with GigaVUE-FM.
- Once registered, GigaVUE-FM serves as the central point for configuring Monitoring Sessions and associated services
- It ensuring unified management and control of the deployed fabric.

Benefits

- Leverage existing orchestration workflows for automated deployment.
- Ensure seamless integration with infrastructure management tools.
- Maintain centralized monitoring and service configuration through GigaVUE-FM.
- Enhances flexibility while maintaining control over network monitoring infrastructure.

Deployment Methods

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

User Driven Fabric Deployment

This method uses a combination of the cloud platform's UI or CLI.

To use the user-driven fabric deployment method:

1. Deploy GigaVUE-FM

Deploy GigaVUE-FM in your OCI environment by using the OCI Console after importing the required custom image.

2. Create a Monitoring Domain

Log in to GigaVUE-FM and create a Monitoring Domain and Connection to define the boundaries for your fabric components.

3. Deploy the fabric components

Use the OCI Console to deploy the following components into the required VCN/subnets within the Monitoring Domain:

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

With these steps, you can efficiently deploy and configure the fabric components in your OCI environment.

Automated Fabric Deployment

When using Infrastructure as Code (IaC) methodology, you can automate the deployment of a fabric component using scripts written in tools such as Terraform, Ansible, or CloudFormation.

To use the automated fabric deployment method,

1. Search for the image in the market place.
2. Deploy GigaVUE-FM

Deploy GigaVUE-FM in your OCI environment using the OCI Console.

NOTE: Deploy GigaVUE-FM before deploying any other fabric component because other components depend on it for registration and management.

3. Create a Monitoring Domain

Log in to GigaVUE-FM and create a Monitoring Domain and Connection to define the boundaries for your fabric components.

4. Deploy the fabric components

Use the OCI Console to deploy the following components into the required VCN/subnets within the Monitoring Domain:

- **UCT-V Controller:** Deploy this if you are using UCT-V to acquire traffic.
- **UCT-V:** Deploy Linux or Windows UCT-V instances, if applicable.
- **GigaVUE V SeriesNodes:** Deploy these for traffic processing.
- **GigaVUE V Series Proxy:** Deploy this if required for your environment.

5. Add additional VNICs for GigaVUE V Series

For GigaVUE V Series, attach the required secondary VNICs after instance launch and reboot the instance so OCI can apply the IP configuration correctly inside the guest OS.

6. Verify registration and health

In GigaVUE-FM, verify that UCT-V Controller, UCT-V, GigaVUE V Series Nodes, V Series Proxy, and GigaVUE-FM appear under the expected Monitoring Domain and Connection, and confirm that their status is Healthy.

With these steps, you can efficiently deploy and configure the fabric components.

Key Concepts

This section provides the key concepts required to understand OCI.

For details, refer to the following section:

- [Monitoring Domain](#)
- [Monitoring Session](#)
- [Precryption](#)
- [Secure Communications](#)
- [Secure Tunnels](#)
- [Traffic Acquisition \(UCT-V\)](#)

Key Concepts	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware	GigaVUE Cloud Suite for Nutanix	GigaVUE Cloud Suite for OCI
Monitoring Domain	✓	✓	✓	✓	✓	✓
Monitoring Session	✓	✓	✓	✓	✓	✓
Precryption	✓	✓	✓	✓	✓	✓
Secure Communications	✓	✓	✓	✓	✓	✓
Secure Tunnels	✓	✓	✓	✓	✓	✓
Traffic Acquisition	✓	✓	✓	✓	✓	✓

Monitoring Domain

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

To clearly define the scope of deployment, OCI follows the concept of Monitoring Domain. This domain establishes a boundary within your Oracle cloud environment where you implement the visibility solution.

You can create a Monitoring Domain in OCI using:

- OCI accounts
- Regions
- VCNs

OCI interacts only with resources within the specified accounts and VCNs listed in a Monitoring Domain.

Connection

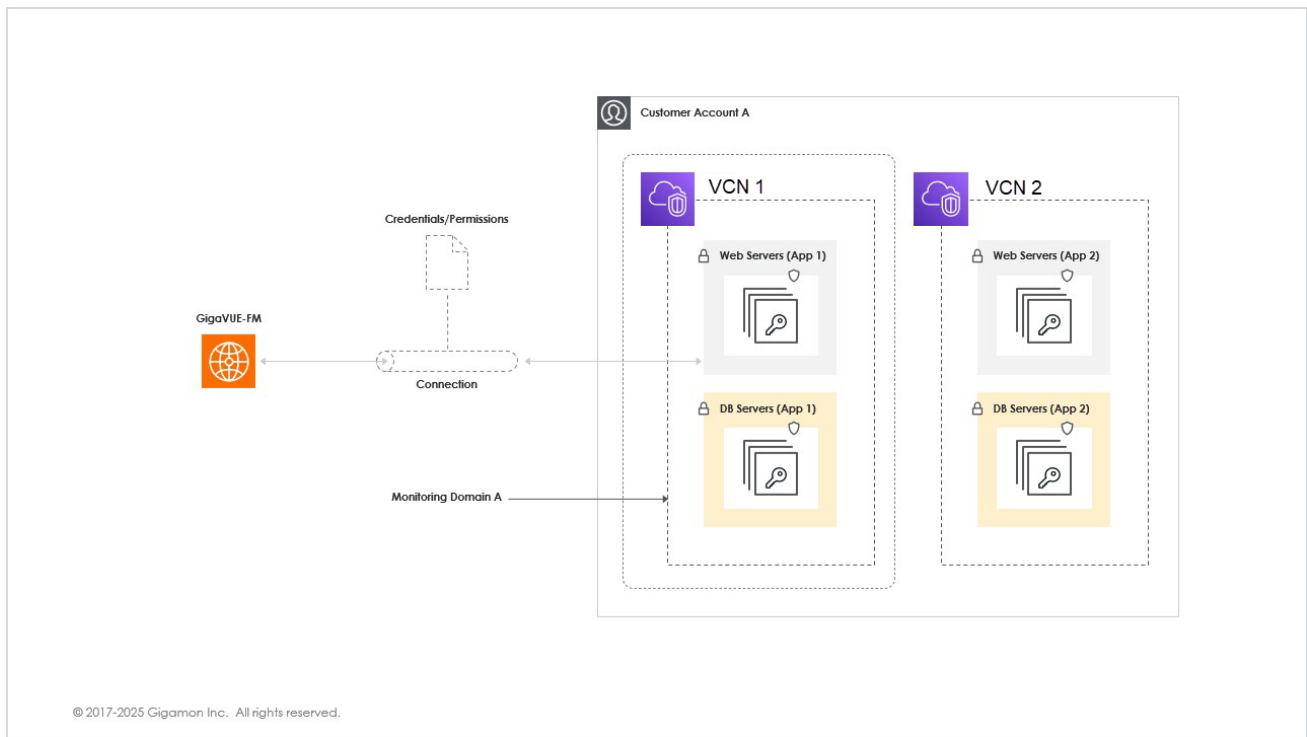
To control access better, OCI uses a Connection.

A connection,

- Includes a set of credentials and permissions that precisely limit what OCI can access.
- Helps you deploy OCI to the appropriate resources with minimal credentials and permissions, enhancing security and control.

Monitoring Domains and Connections work together to provide secure, targeted monitoring. You define what OCI can see and do.

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



In the above diagram:

- You create Monitoring Domain A for VCN 1 in Account A
- You assign a Connection that grants access to only VCN 1
- GigaVUE-FM uses this connection to find and monitor resources like:
 - Workload VMs
 - Subnets
 - Security groups
 - Key pairs

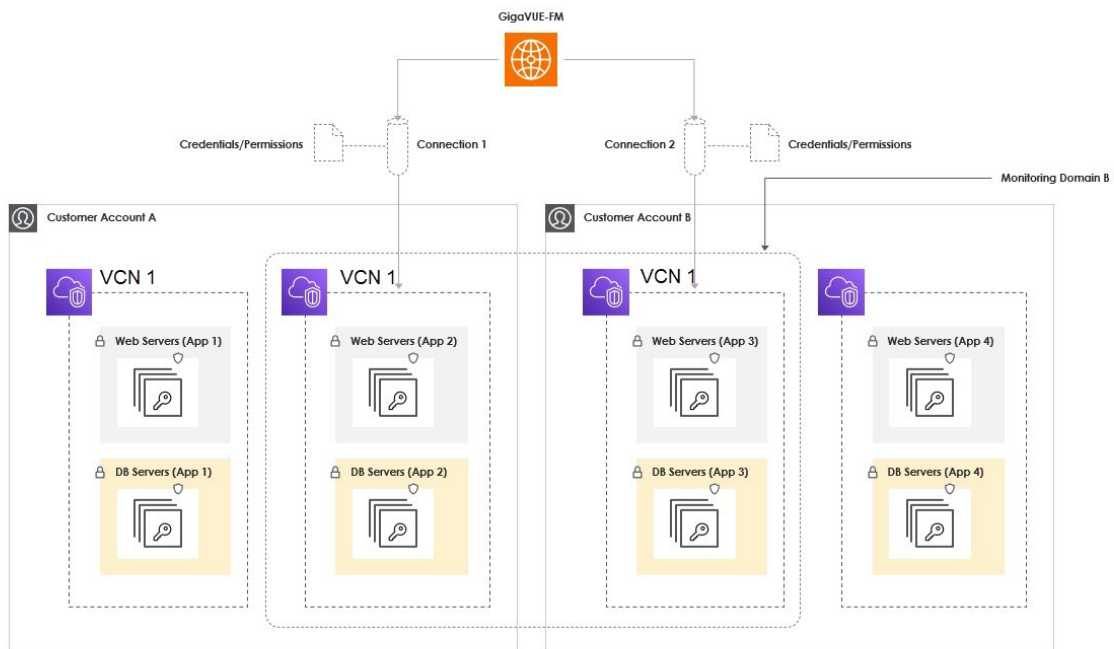
It then deploys GigaVUE components to collect and process traffic. The data is forwarded to your monitoring tools. GigaVUE-FM operates only within VCN 1, following the rules of the Monitoring Domain and its associated connection.

The Monitoring Domain defines a clear boundary within which GigaVUE-FM operates. This ensures both security and performance goals are achieved. In this case, you do not want GigaVUE-FM to access any VCNs other than VCN 1, GigaVUE-FM complies with your intent. It restricts its operations strictly to the boundary defined by the Monitoring

Domain. Additionally, the credentials and permissions you provide through the connection associated with the Monitoring Domain further restrict the actions of GigaVUE-FM.

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

The following diagram illustrates a Monitoring Domain encompassing resources in VCNs in two different OCI accounts:



© 2017-2025 Gigamon Inc. All rights reserved.

In this diagram:

- Monitoring Domain B includes VCN 2 in Account A and VCN 3 in Account B
- You assign Connection 1 to access VCN 2 and Connection 2 to access VCN 3

GigaVUE-FM accesses only VCN 2 and VCN 3. It does not see or touch VCN 1 or VCN 4. The domain and connections define strict access limits.

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

Monitoring Session

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

Workload Selection

You can select target workloads to define the scope of your monitoring:

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

Traffic Acquisition

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

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

Traffic Processing

You can leverage a comprehensive suite of traffic processing features:

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

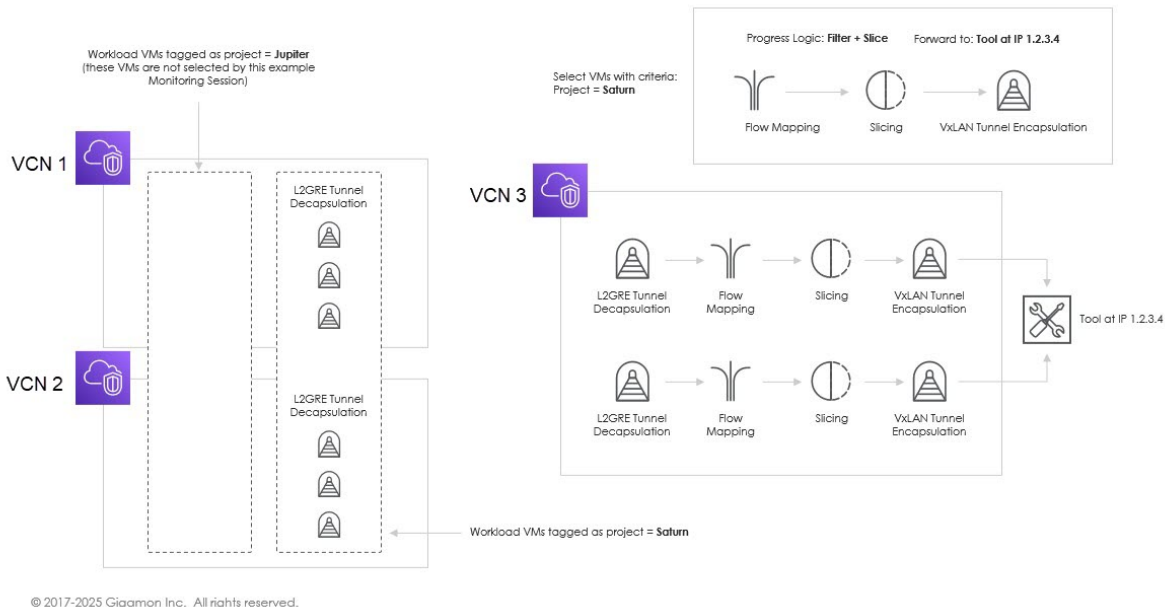
Configuring these elements within a Monitoring Session allows you to create a finely-tuned visibility policy that aligns perfectly with your specific monitoring objectives in OCI environments.

After you define a Monitoring Session, GigaVUE-FM

- Automatically configures the required traffic acquisition points
- Processes the traffic.
- Sends the captured traffic to GigaVUE V Series Nodes.
- Forwards the process data to to your analysis tools.

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

Example: Visibility Policy Defined as Monitoring Session A



The above diagram display an example to monitor VMs tagged with project = "Saturn". For this, you

- Define a Monitoring Session with this tag filter
- Choose UCT-V to acquire traffic
- Apply packet slicing in the V Series Nodes
- Forward traffic to your analysis tool at IP 1.2.3.4

When deployed, GigaVUE-FM:

- Discovers all matching VMs in your Monitoring Domain
- Configures UCT-V on these VMs
- Starts forwarding sliced packets to your tool

If new Saturn-tagged VMs are launched, GigaVUE-FM detects them automatically. It applies the same monitoring policy without manual action.

Benefits

- Focus monitoring on only the workloads you need
- Control how traffic is captured and processed

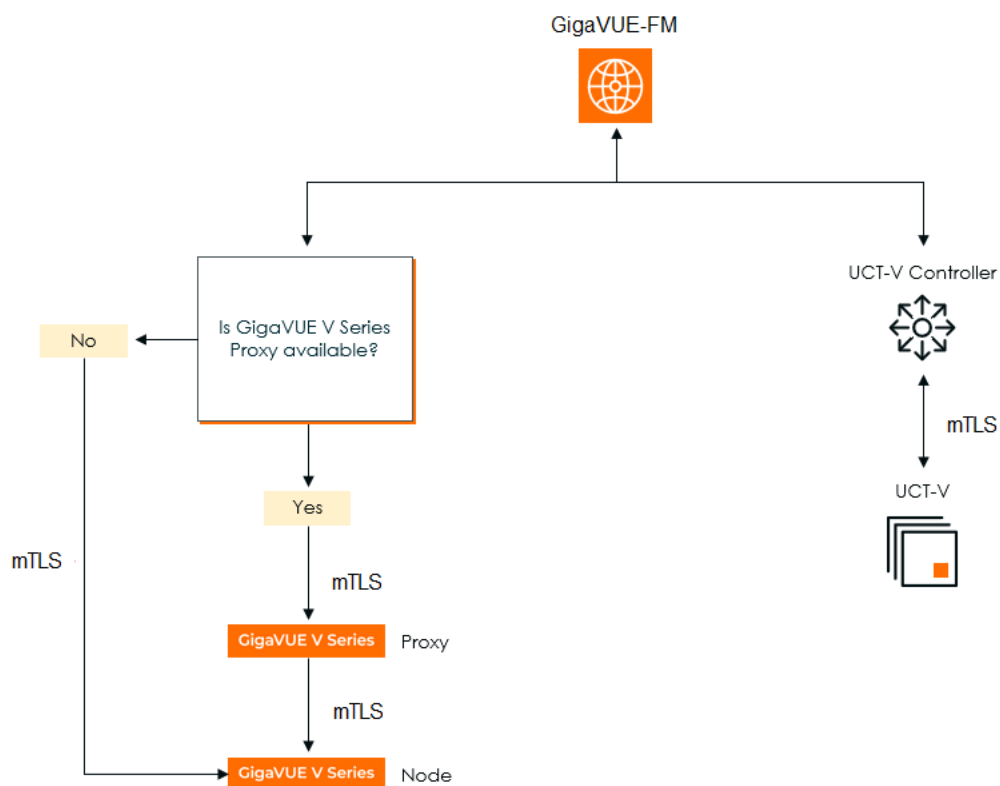
- Automatically update monitoring as your environment changes

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

Secure Communication between GigaVUE Fabric Components

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

How it Works!



In this setup:

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

- If a GigaVUE V Series is available, GigaVUE-FM first connects to the GigaVUE V Series Proxy and establishes an mTLS connection with the GigaVUE V Series Node.
- GigaVUE-FM also initiates an mTLS connection to the UCT-V Controller, establishing an mTLS connection with UCT-V.

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

GigaVUE-FM acts as the PKI

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

Bring Your Own CA

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

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

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

Rules and Notes

- If a public IP is revoked in public cloud platforms, you can issue a new certificate to remove the old IP.
- This feature is optional.
- Ensure NTP (Network Time Protocol) runs if GigaVUE-FM and components are on different hosts.
- Applying a certificate may temporarily cause a component to show as Down, but it recovers automatically.

Precription™

License: Precription requires a **SecureVUE Plus** license.

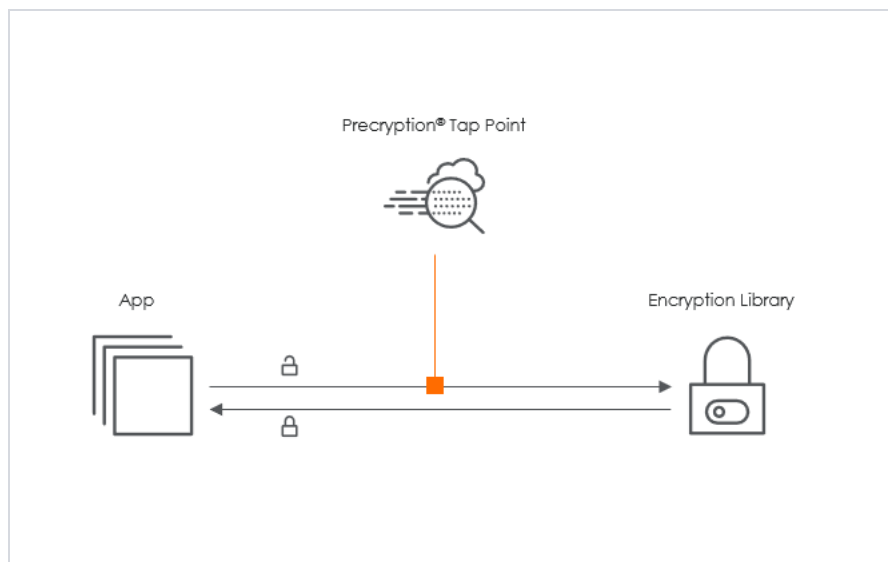
Gigamon Precryption™ technology¹ provides you clear-text visibility into encrypted network traffic without the need for traditional decryption. It works across virtual, cloud, and container environments, helping you get the full security stack without added complexity

In this section:

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

How Gigamon Precryption Technology Works

Precryption technology leverages built-in Linux functionality to copy communications between the application and the encryption library, such as OpenSSL.



Key Highlights

¹**Disclaimer:** The Precryption feature allows you to capture decrypted traffic from both virtual machine (VM) and container-based environments. After capturing the traffic using (via UCT-C or UCT-V), you can send to the V Series product for further processing. You can choose to secure this traffic using encrypted tunnels between the capture point and the V Series. This option helps protect sensitive data during transit. If you don't enable encrypted tunnels, the captured (decrypted) traffic remains in plain text while moving between the source and the V Series—introducing potential exposure risks. Please note that the feature behavior and security options may change over time. Stay informed about updates to ensure you use the latest protections. By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

- Captures network traffic in plain text, either before the system encrypts it or after it decrypts it.
- Does not change how encryption or transmission works.
- Avoids proxies, retransmissions, and “break-and-inspect” steps. Instead, it sends the plaintext copy to the Gigamon Deep Observability Pipeline, where tools can optimize, transform, and forward the traffic as needed.
- Runs on GigaVUE® Universal Cloud Tap (UCT) and supports hybrid and multi-cloud environments, including on-prem and virtual platforms.
- Runs independently of your applications, so you don’t need to change your 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.

Precryption helps you:

- Improve visibility for East-West traffic into virtual, cloud, and container platforms
- Delivers unobscured visibility into all encryption types, including TLS 1.3, without managing and maintaining decryption keys.
- Manages compliance with IT organizations, keeps communications private, architects a Zero Trust foundation, and boosts security-tool effectiveness by a factor of 5x or more.

Key Features

The following are the key features of this technology:

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

- Integration with Gigamon Deep Observability Pipeline for the full suite of optimization, transformation, and brokering capabilities.

Key Benefits

The following are the key benefits of this technology:

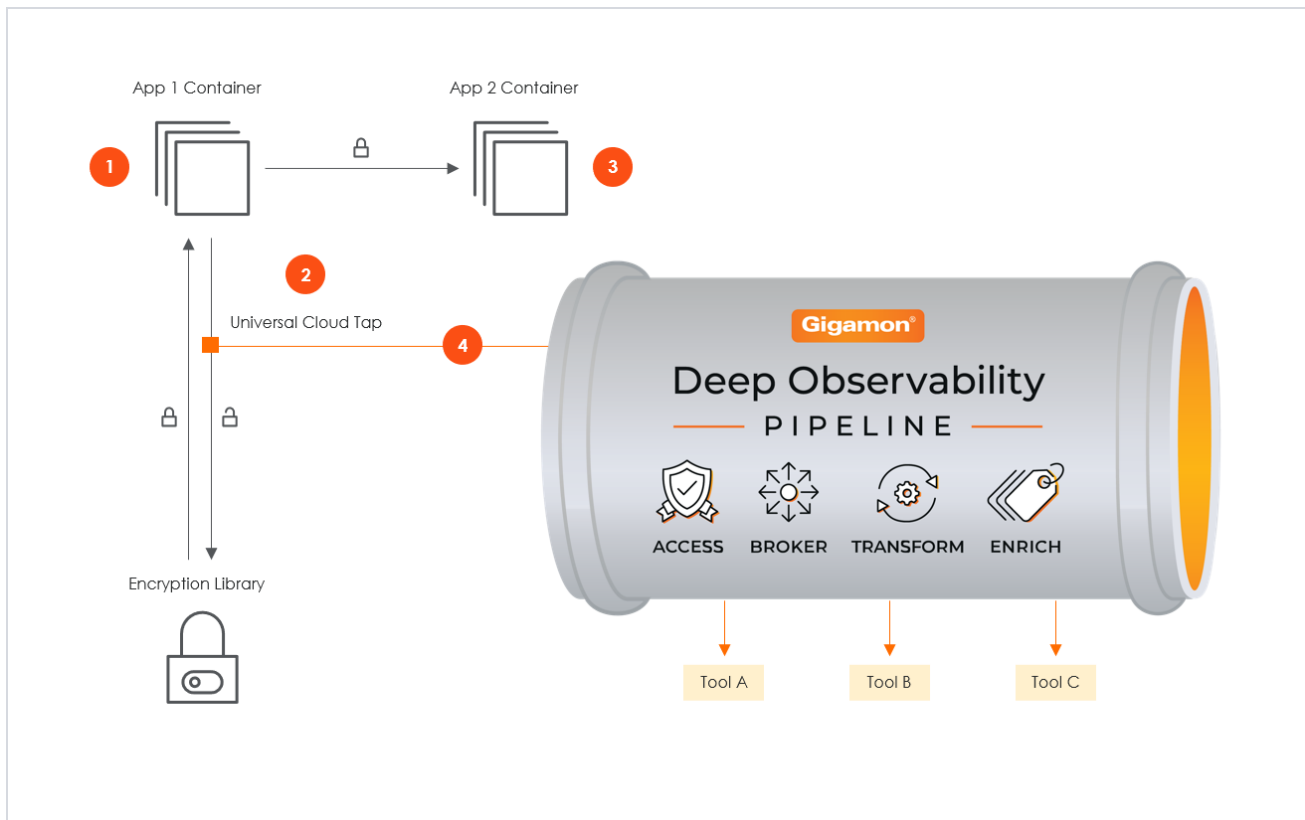
- Eliminates blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitors application communications with an independent approach that enhances development team velocity.
- Extends security tools' visibility to all communications,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

How Gigamon Precryption Technology Works

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

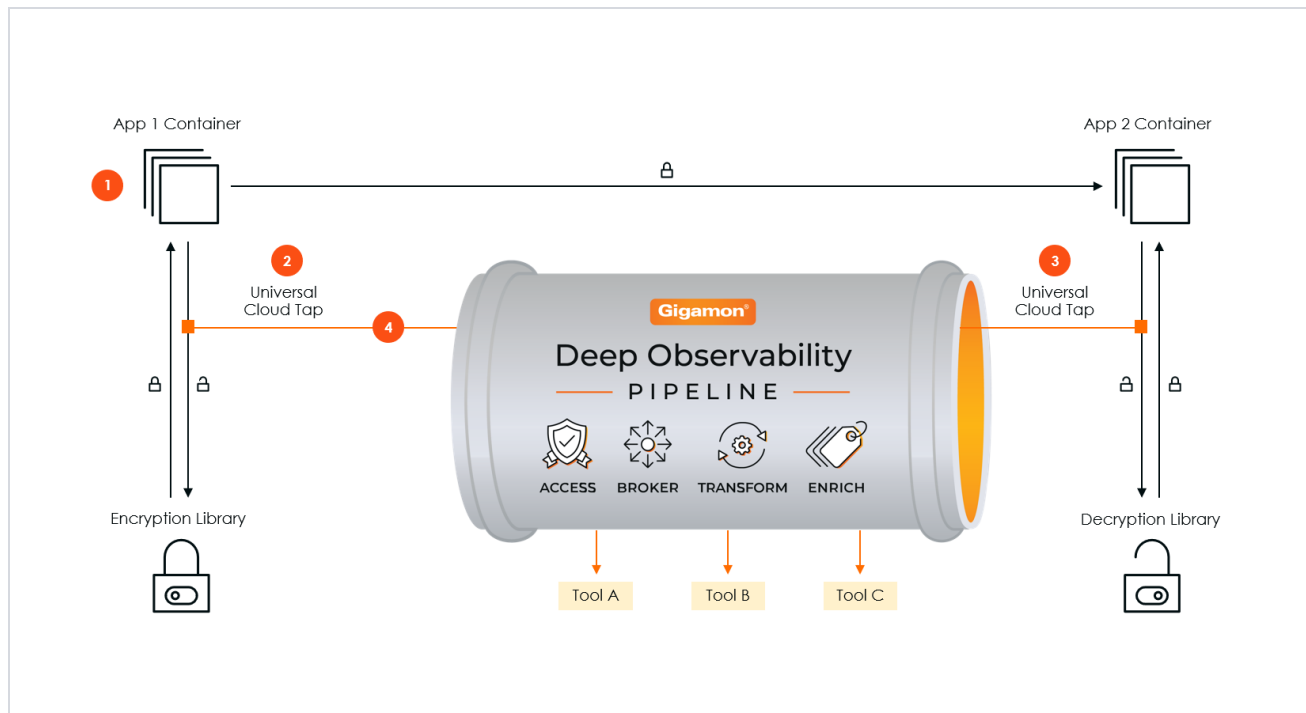
- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)

Precryption Technology on Single Node



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

Preryption Technology on Multi-Node



1. An application uses an encryption library, such as OpenSSL, to encrypt a message.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Preryption technology, gets a copy of this message before it is encrypted on the network
3. Optionally, GigaVUE UCT enabled with Preryption can also acquire a copy of the message from the server end after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline.
5. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Container environments: Preryption™ is supported on the following container platforms that support UCT-C:

Platform Type	Platform
Public Cloud	• EKS • AKS • GKE • OKE
Private Cloud	• OpenShift • Native Kubernetes (VMware)

Prerequisites

Points to Note

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x.
- For UCT-C, worker pods should always have libssl installed to ensure that UCT-C Tap can tap the Precryption packets from the worker pods whenever libssl calls are made from the worker pods.
- For GigaVUE-FM, add port 5671 in the security group to capture the statistics.
- In security group settings on the UCT-V Controller, enable Port 9900 to receive the statistics information from UCT-V.
- For UCT-C, add port 42042 and port 5671 to the security group.
- Precryption works only on Linux systems running Kernel version 4.18 or later.

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

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

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

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

Note

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

Secure Tunneling to GigaVUE V Series Nodes

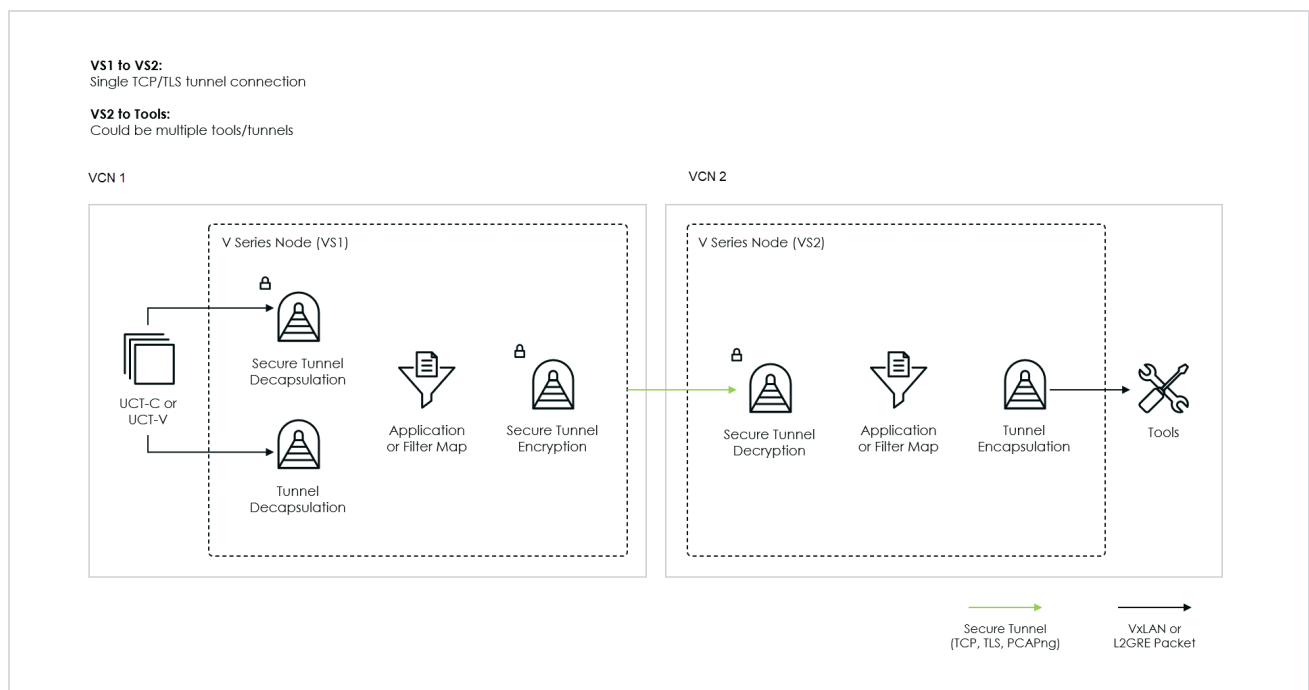
Secure Tunnel transfers the cloud captured packets from one GigaVUE V Series Node to another.

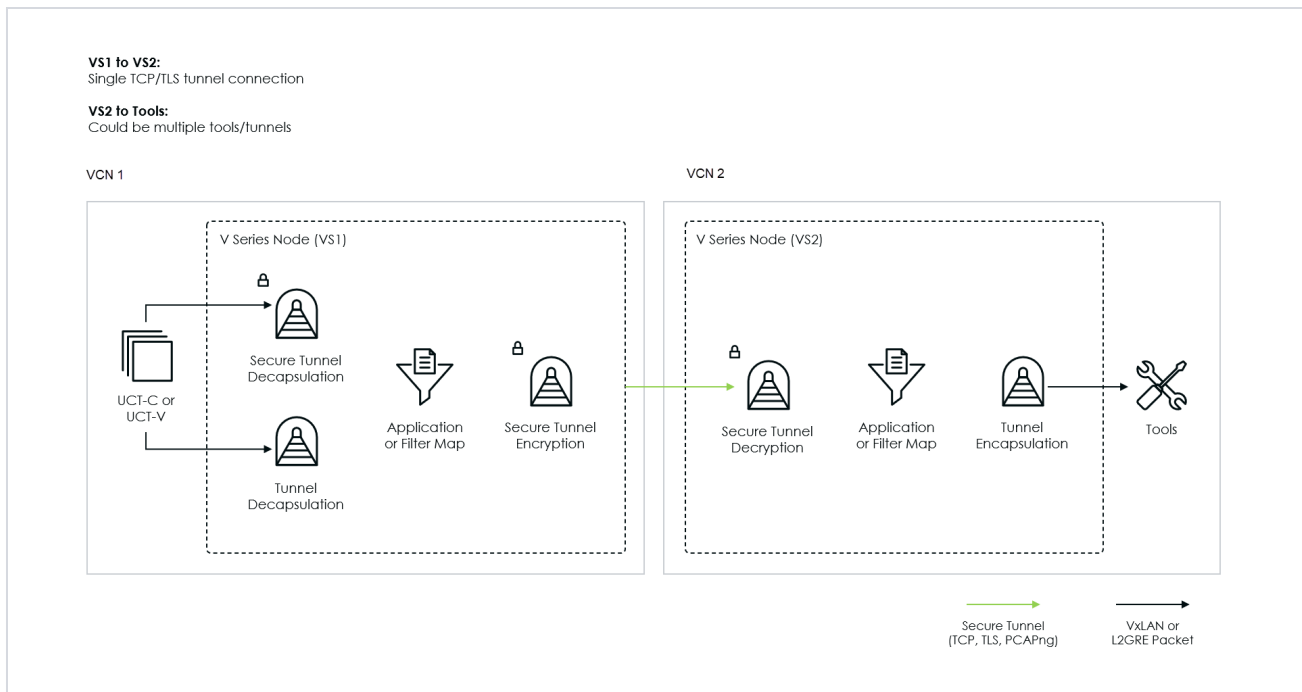
When sending traffic between two V Series Nodes, the source node captures and encapsulates the packets in PCAPng format. It then sends them to the destination V Series Node that decapsulates and processes the traffic based on your configuration.

How Does it Work!

- The source V Series forwards packets to the destination V series for further analysis.
- The destination node applies processing features such as de-duplication, application intelligence, or load balancing.
- The built-in load balancer distributes traffic across multiple V Series Nodes.
- If the load balancer sends packets to another node, it can re-encapsulate them and send them over another secure tunnel.

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





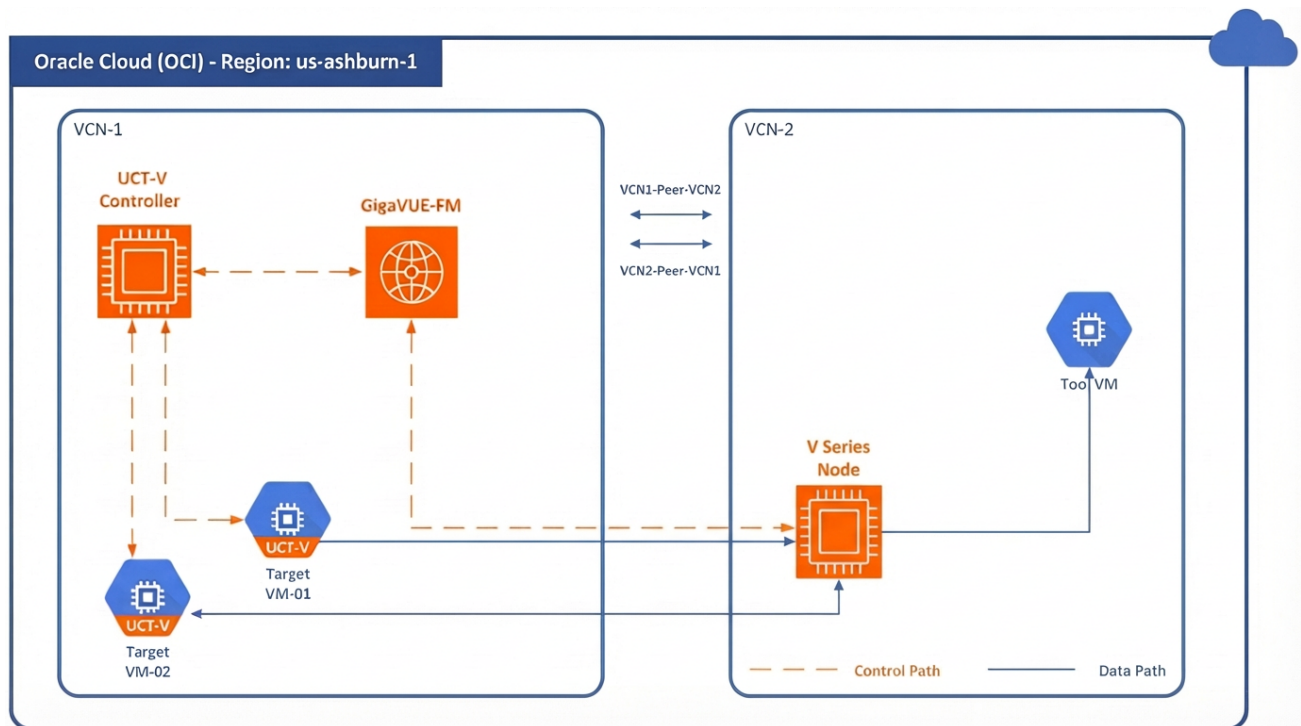
Traffic Acquisition

You can acquire traffic from multiple virtual machines and container pod instances using UCT-V

The acquired traffic is forwarded to the GigaVUE V Series Node to conduct core intelligence and additional GigaSMART processing.

Traffic-Flow-Across-Components

GigaVUE Cloud Suite for OCI mirrors traffic from workload VMs in VCN-1, sends the mirrored packets to a GigaVUE V Series Node in VCN-2, and then forwards optimized traffic to a tool VM for analysis. Production application traffic remains in the normal data path, while visibility traffic follows a separate, parallel path through the visibility fabric.



Traffic Flow Across Components

1. **Workload VMs generate production traffic**

Applications on Target VM-01 and Target VM-02 in VCN-1 generate production traffic on their primary network interfaces. This traffic continues to flow to its destinations without modification.

2. **UCT-V on each target VM mirrors selected traffic**

A UCT-V agent runs on each target VM in VCN-1. UCT-V inspects packets on the VM interfaces and mirrors only the traffic that matches the configured monitoring policies, reducing the amount of data sent for analysis.

3. **UCT-V encapsulates mirrored traffic and sends it to the V Series Node**

UCT-V encapsulates mirrored packets in a tunnel (such as VXLAN or L2GRE) and sets the GigaVUE V Series Node in VCN-2 as the remote tunnel endpoint. The encapsulated traffic leaves the target VMs and traverses the OCI network across the peering between VCN-1 and VCN-2.

4. **The GigaVUE V Series Node decapsulates and processes the traffic**

The V Series Node in VCN-2 receives the tunneled traffic from all UCT-V agents, decapsulates the packets, and applies monitoring-session logic such as filtering, slicing, and other GigaSMART processing to create tool-ready traffic.

5. The V Series Node forwards optimized traffic to the tool VM

After processing, the V Series Node forwards the optimized traffic to the tool VM in VCN-2, using the configured egress method (for example, direct IP, VXLAN, or ERSPAN). The tool VM then analyzes the received traffic for security, performance, or compliance monitoring.

Deployment Prerequisites

Before you deploy the fabric components in OCI, ensure that the following prerequisites are met:

- Deploy GigaVUE-FM first and note its IP address or FQDN.
- Create the required VCNs, subnets, routing rules, and security rules.
- Create the Monitoring Domain and Connection in GigaVUE-FM.
- Generate the registration token in GigaVUE-FM.
- Ensure that the required ports are open between GigaVUE-FM, UCT-V Controller, UCT-V, GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-C components, as applicable.
- For GigaVUE V Series deployments, plan for a minimum of two VNICs and reboot the instance after you attach the secondary VNICs.

With these prerequisites in place, you can deploy and configure the fabric components in your OCI environment.

Supported Compute Requirements for OCI

In OCI, flavors set the vCPU, memory, and storage requirements for an image. Gigamon recommends that you create a flavor on your choice that matches or exceeds the supported requirements listed in the following table.

Fabric Component	Recommended OCI shape(s)	Minimum OCPUs	Minimum RAM	Networking	Notes
GigaVUE-FM	VM.Standard3.Flex	2	16 GB	1 VNIC (mgmt)	GigaVUE-FM requires Native virtualization on import.
GigaVUE V Series Node	VM.Standard.E6.Flex (recommended) / VM.Optimized3.Flex (optional)	4	32 GB	2 VNICs (mgmt + data)	Attach secondary VNIC post-launch and reboot.
GigaVUE V Series Proxy	VM.Standard3.Flex	1	4 GB	1 VNIC (mgmt)	Register proxy with GigaVUE-FM

					and node with proxy if using proxy.
UCT-V Controller	VM.Standard3.Flex	2	8 GB	1 VNIC (mgmt)	Enable Basic Authentication for versions 6.9 and lower.
UCT-V	VM.Standard3.Flex	1	4 GB	1 VNIC (mgmt)	Register via Controller(s).

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

The instance size of the GigaVUE V Series Node is configured and packaged as part of the qcow2 image file.

Network Requirements

The following table lists the recommended requirements to setup the network topology.

Network	Purpose
Management	Identify the subnets that GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data	Identify the subnets that receives the mirrored tunnel traffic from the monitored instances. In data network, if a tool subnet is selected then the V Series node egress traffic on to the destinations or tools.

NOTE: If you are using IPv6 in the tenant network, then it is recommended to use SLAAC or stateless DHCPv6 for dynamic address assignment.

Network Firewall Requirements

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

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

GigaVUE FM

The following table specifies the inbound and outbound communication parameters—protocols, ports, and CIDRs—required for GigaVUE-FM to support secure access, registration, certificate exchange, and control-plane communication with associated components.

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

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

				Controller.
Outbound	TCP	80	GigaVUE V Series Node	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Node.
Outbound	TCP	80	GigaVUE V Series Proxy	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Proxy.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.

UCT-V Controller

The following table defines the network communication parameters—protocols, ports, and CIDRs—required for UCT-V Controller to interact with GigaVUE-FM and UCT-V components, supporting registration, diagnostics, certificate exchange, and control-plane operations including third-party orchestration..

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

for Third Party Orchestration)				to GigaVUE-FM using REST API.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound (This is the port used for Third Party Orchestration)	TCP	9600	GigaVUE-FM IP	Allows GigaVUE-FM to receive certificate requests from the UCT-V Controller.
Outbound	TCP	9902	UCT-V Subnet	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs for UCT-Vs with version greater than 6.10.00.
Outbound	TCP	8301	UCT-V Subnet	Allows ACME validation flow from UCT-V Controller to UCT-V.

UCT-V

The following table outlines UCT-V Controller's network communication requirements with GigaVUE-FM, detailing essential ports, protocols, and CIDRs for registration, diagnostics, certificate exchange, and orchestration traffic.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller.
Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V to receive the ACME challenge requests from the UCT-V Controller.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node.
Outbound	TCP	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V

				Controller.
Outbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	8300	UCT-V Controller IP	Allows UCT-V to receive ACME validation flow from UCT-V Controller.

GigaVUE V Series Node

The following table outlines GigaVUE V Series Node's network communication requirements, detailing protocols, ports, and CIDRs necessary for tunneling, management, diagnostics, and secure data transfer across connected components

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	UDP (VXLAN)	VXLAN (default 4789)	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive VXLAN tunnel traffic to UCT-V.
Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE tunnel traffic to UCT-V.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from UDPGRE Tunnel.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Node to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	80	GigaVUE V Series Proxy IP	Allows UCT-V to receive the ACME challenge requests from the GigaVUE V Series Proxy.

Inbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	UCT-V subnet	Allows to securely transfer the traffic to GigaVUE V Series Nodes.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence and Application Visualization reports to GigaVUE-FM.
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	- echo request - echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.

Giga VUE V Series Proxy(Optional)

The following table defines GigaVUE V Series Proxy's network communication parameters, listing essential protocols, ports, and CIDRs for registration, certificate exchange, diagnostics, and control-plane traffic with GigaVUE-FM and V Series Nodes.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Proxy to receive the ACME challenge requests from the GigaVUE-FM.
Inbound	TCP	8300	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive certificate requests from GigaVUE V Series Node for the configured params and provides the certificate using those parameters.
Inbound	TCP	8892	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and management plane traffic with GigaVUE V Series Node.

UCT-C Controller - deployed in Kubernetes worker mode

The following table outlines UCT-C Controller's network communication parameters in Kubernetes worker mode, specifying TCP ports and CIDRs required for management, statistics exchange, and secure connectivity with GigaVUE-FM.

UCT-C Controller deployed inside Kubernetes worker node				
Direction	Protocol	Port	Source CIDR	Purpose

Inbound	TCP	8443 (configurable)	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-C Controller.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	Any IP address	Allows UCT-C Controller to send statistics to GigaVUE-FM.
Outbound	TCP	443	GigaVUE-FM IP	Allows UCT-C Controller to communicate with GigaVUE-FM.

Ports for Backward Compatibility

Ensure to open these ports for backward compatibility when GigaVUE-FM is running version 6.10 or later, and the fabric components are on (n-1) or (n-2) versions.

UCT-V Controller

The following table specifies the communication parameters required for third-party orchestration, detailing the TCP ports and CIDRs used by UCT-V Controller to manage registration and control-plane traffic with UCT-V components.

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

GigaVUE V Series Node

The following table specifies the outbound communication requirement for GigaVUE V Series Node, detailing the protocol, port, and source CIDR used to send registration and heartbeat messages to the GigaVUE V Series Proxy during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Outbound	TCP	8891	GigaVUE V	Allows GigaVUE V Series Node to

(This is the port used for Third Party Orchestration)			Series Proxy IP	send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.
---	--	--	-----------------	--

GigaVUE V Series Proxy(Optional)

The following table specifies the optional inbound communication parameter for GigaVUE V Series Proxy, detailing the protocol, port, and source CIDR required to receive security parameter requests from GigaVUE V Series Node during third-party orchestration.

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

Default Login Credentials

Using the default credentials, you can log in to the GigaVUE V Series Node and GigaVUE V Series Proxy.

Product	Login credentials
GigaVUE V Series Node	Using ssh, you can log in to the GigaVUE V Series Node. The default username and password are: - Username: gigamon - Password: Gigamon123!
GigaVUE V Series proxy	Using ssh, you can log in to the GigaVUE V Series proxy. The default username and password are: - Username: gigamon - Password: Gigamon123!

Integrate Private CA

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

Rules and Notes

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

To integrate private CA

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

Generate CSR

To create an intermediate CA certificate:

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

The CSR is downloaded successfully.

Upload CA Certificate

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

To upload the signed CA certificate to GigaVUE-FM:

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

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

Adding Certificate Authority

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

The CA Certificate chain List page allows you to add the root CA for the devices.

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

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

SSL Decrypt

License: For information on licensing, refer to the *Volume Based License (VBL)* section of respective GigaVUE Cloud Suite Deployment Guide.

SSL Decrypt application delivers decrypted traffic to out-of-band tools that can then detect threats entering the network. Secure Socket Layer (SSL) is a cryptographic protocol that adds security to TCP/IP communications such as Web browsing and email. The protocol allows the transmission of secure data between a server and client who both have the keys to decode the transmission and the certificates to verify trust between them.

SSL encryption secures traffic between a client and a server, such as a Web server. SSL decryption uses keys to decode the traffic between the client and server.

SSL and Transport Layer Security (TLS) protocols consist of a set of messages exchanged between a client and server to set up and tear down the SSL connection between them. To set up the connection, the client and server use the Public Key Infrastructure (PKI) to exchange the bulk encryption keys needed for data transfer.

IMPORTANT: To use SSL Decrypt application in GigaVUE-FM 6.3.00, install new GigaVUE-FM 6.3.00 image. Refer to *GigaVUE-FM Installation and Upgrade Guide* for step-by-step instructions on how to install GigaVUE-FM. SSL Decrypt application does not work if you upgrade from any previous GigaVUE-FM version to GigaVUE-FM 6.3.00.

Keep in mind the following when using SSL Decrypt application:

1. On updating the keys, service, or key maps which are already used in a monitoring session, the monitoring session is dynamically updated, and you need not re-deploy the monitoring session. You can also see if the updated keys, services, or key maps were successfully updated to the monitoring session and the respective GigaVUE V Series Nodes on the **All Events** page. Refer to [Overview of Events](#) section in the *GigaVUE Administration Guide* for detailed information on Events.
2. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the key will be removed from the Key Map. If that key is the only available entry in the Key Map, then it will not be removed.
3. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session that is not deployed, then the key will be removed from the Key Map and if that key is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.
4. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the service will be removed from the Key Map. If that service is the only available entry in the Key Map, then it will not be removed.
5. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is not deployed, then the service will be removed from the Key Map and if that service is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.
6. In VMware NSX-T platform, the throughput of SSL Decrypt application is improved to 480 Mbps.

Refer to the following topics for more detailed information:

- [Supported Protocols, Algorithms, and Ciphers for SSL Decrypt](#)
- [Configure SSL Decrypt](#)

Supported Protocols, Algorithms, and Ciphers for SSL Decrypt

The supported protocols are as follows:

- SSL 3.0
- TLS 1.0
- TLS 1.1

- TLS 1.2

The supported authentication (Au) is as follows:

- RSA

The supported key exchange (Kx) is as follows:

- RSA

The supported encryption algorithms (Enc) are as follows:

- NULL
- RC4
- DES
- 3DES
- AES (including GCM mode)
- CAMELLIA
- SEED
- IDEA

The supported compression algorithm is as follows:

- NULL

The supported digest algorithms are as follows:

- MD5
- SHA1
- SHA2

The supported key sizes are 128, 256, 512, 1024, 2048, and 4096.

The supported TLS extensions are as follows:

- Extended Master Secret, RFC 7627
- Encrypt-then-MAC, RFC 7366

The following table lists the supported ciphers:

Table 1: Supported Ciphers for SSL Decrypt

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_NULL_MD5	RSA	RSA	NULL	0	MD5
TLS_RSA_WITH_NULL_SHA	RSA	RSA	NULL	0	SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_RC4_128_MD5	RSA	RSA	RC4_128	128	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RSA	RC4_128	128	SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
TLS_RSA_WITH_IDEA_CBC_SHA	RSA	RSA	IDEA_CBC	128	SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
TLS_RSA_WITH_DES_CBC_SHA	RSA	RSA	DES_CBC	56	SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	168	SHA
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	128	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES_256_CBC	256	SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	CAMELLIA_128_CBC	128	SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	CAMELLIA_256_CBC	256	SHA
TLS_RSA_WITH_SEED_CBC_SHA	RSA	RSA	SEED_CBC	128	SHA
TLS_RSA_WITH_NULL_SHA256	RSA	RSA	NULL	0	SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES_128_CBC	128	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES_256_CBC	256	SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES_128_GCM	128	SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES_256_GCM	256	SHA384

All algorithms used for SSL Decrypt application are FIPS 140-3 compliant.

All key URLs must point to an RSA private key stored in the PEM or PKCS12 format, as follows:

- <http://keyserver.domain.com/path/keyfile.pem>
- <https://keyserver.domain.com/path/keyfile.pem>
- <ftp://keyserver.domain.com/path/keyfile.pem>
- <tftp://keyserver.domain.com/path/keyfile.pem>
- [scp://username\[:password\]@keyserver.domain.com/path/keyfile.pem](scp://username[:password]@keyserver.domain.com/path/keyfile.pem)

The supported applications are as follows:

- HTTPS
- FTPS
- SMTP, IMAP, and POP3 with StartTLS

Configure SSL Decrypt

To configure SSL Decrypt Application using GigaVUE-FM follow the steps given below:

- [Upload SSL Key Pairs](#)
- [Create SSL Service](#)
- [Key Mapping](#)
- [SSL Key Pair Store](#)
- [Add SSL Decrypt to Monitoring Session](#)

Upload SSL Key Pairs

To upload an SSL private key, do the following:

1. Go to **Inventory > Resources > Security > SSL Keys**.
2. Click **Add**. The **Create SSL Key Pair** page appears.
3. Enter the following details:

Field	Description
Key Alias	Enter a name for the key.
Comment	Enter a description
Key Type	Select the either of the key type:
PEM	
PassPhrase (optional)	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Pair Store in which the Key is stored.
Private key	Enter the Private Key using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
Certificate	Enter the Certificate using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
PKCS12	
PassPhrase	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Pair Store in which the Key is stored.

4. Click **Save**.

NOTE: SSL Decrypt application does not support HSM.

The following actions can also be performed from the SSL Key Pairs Page:

Field	Description
Edit	To edit a SSL Key pair, select the key from the list in the SSL Key Pairs page and click the Edit button.
Delete	To delete a SSL Key pair, select the key from the list in the SSL Key pairs page and click the Delete button.
Delete all	Use this button to delete all the SSL Key pairs in the SSL Key pairs page.
View certificate	To view the certificate associated with the particular SSL Key Pair, select the key from the list in the SSL Key Pairs page and click the View Certificate button.

Create SSL Service

After uploading a private key, you can add a service. A service maps to a physical server, such as an HTTP server. One server can run multiple services. A service is a combination of an IP address and a server port number.

Prerequisite

Before creating a service, upload a private key as described in [Upload SSL Key Pairs](#)

To create a SSL service, do the following:

1. Go to **Inventory > Resources > Security > SSL Service**. The SSL Services page appears.
2. Click **Add**. The **Create SSL Service** page appears.
3. On the Create SSL Service page, enter the following details:

Field	Description
Alias	Enter a name for the SSL Service.
Default Service	Enable this to use default service.
Server IP Address	Enter the IP address of the server in which the service runs.
Server Port	Enter the port number of the server.

4. Click **Save**.

The following actions can also be performed from the SSL Service Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the Edit button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the Delete button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

Key Mapping

After adding the SSL Service, now you map the private key with the service using Key Mapping.

To map a key with the service, follow the steps given below,

1. Go to **Inventory > Resources > Security > SSL Key Mapping**. The SSL Key Pair Mapping page appears.
2. Click **Add**.

3. Enter the Key Mapping Alias.
4. Select the SSL Service and Key Alias from the drop-down.
5. Click **Save**.

The following actions can also be performed from the SSL Key Pairs Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the Edit button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the Delete button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

SSL Key Pair Store

SSL Key Pair Store is a repository, that allows you to save all the key under a single location. You can create multiple key stores and in each key store you can store multiple keys.

1. Go to **Inventory > Resources > Security > SSL Key Store**. The SSL Key Pair Store page appears.
2. Click **Add**.
3. Enter the **Key Store Alias** and **Comment**.
4. Click **Save**.

The following actions can also be performed from the SSL Key Pair Store Page:

Field	Description
Edit	To edit a SSL Key pair Store, select the Key Store from the list in the SSL Key Pair Store page and click the Edit button.
Delete	To delete a SSL Key Pair Store, select the SSL Key Pair Store from the list in the SSL Key Pair Store page and click the Delete button.
Delete all	Use this button to delete all the SSL Key Pair Store in the SSL Key Pair Store page.

Add SSL Decrypt to Monitoring Session

After mapping your keys with service, to add GigaSMART applications to GigaVUE V Series Node, follow the steps given below,

1. Drag and drop **SSL Decrypt** from APPLICATIONS to the graphical workspace.
2. Click the SSL Decrypt application and select **Details**.



X application

Save

Application	SSL Decrypt
Alias	ssl-decrypt
Enable	☒
Key Map	▼
In Port ⓘ	0
Out Port ⓘ	0
Session Timeout (sec)	300
Pending Session Timeout (sec)	60
Tcp Syn Timeout (sec)	20
Decrypt Fail Action	☐ Pass ☒ Drop
Key Cache Timeout (sec)	10800
Ticket Cache Timeout (sec)	10800
Non-ssl Traffic	☐ Pass ☒ Drop

3. Enter the following details in the Application quick view:

Fields	Description
Alias	Enter the alias name for the application.
Enable	Enable the box to enable SSL Decryption.
Key Map	Select the Key Map from the list of available Key Maps. Refer to Key Mapping for more details on how to map the key to SSL Service.
In Port	Enter the source port number from which the traffic should be fetched.
Out Port	Enter the destination port number to which the decrypted traffic should be delivered.
Session Timeout	Enter the value in seconds after which the session should be timeout. The default value is 300 seconds.
Pending Session Timeout	Enter the value in seconds after which the session must timeout if the session is in pending state
Tcp Syn Timeout	Enter the value in seconds after which the session must timeout when the session does not synchronize TCP.
Decrypt Fail Action	Select Pass to allow the traffic to pass through the application when the decryption fails and select Drop to drop the traffic before passing through the application when the decryption fails.
Key Cache Timeout (sec)	Enter the value in seconds until which the key cache information can be reused for resumption.
Ticket Cache Timeout (sec)	Enter the value in seconds until which the ticket cache information can be reused for resumption.
Non-ssl Traffic	Select Pass to allow the non-SSL traffic to pass through the application and select Drop to drop the non- SSL traffic before passing through the application.

4. Click **Save**.
5. Click **Deploy**. The Select nodes to deploy the monitoring session page appears.
6. Select the GigaVUE V Series Nodes you want to deploy and select an interface for each GigaVUE V Series Node. Then, click **Deploy**.

Deploy Fabric Components using Generic Mode

In Generic Mode, you can deploy GigaVUE V Series Nodes using your own orchestration system. Provide the monitoring domain name and connection name in the user data during deployment.

GigaVUE-FM automatically creates the Monitoring Domain under the **Third Party Orchestration** monitoring domain page. It assigns the deployed fabric components to that domain after the deployment completes.

Acquire Traffic using UCT-V

This section outlines the workflow to acquire traffic directly from virtual machines and send it to GigaVUE V Series Nodes using UCT-V. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- [Install GigaVUE-FM on OCI](#)
- [Configure Role-Based Access](#)
- [Acquire Traffic using UCT-V](#)
- [Configure and Deploy GigaVUE Fabric Components using OCI- Generic Mode](#)
- [Configure and Deploy Monitoring Session](#)

Deployment Guidelines

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

- Get the required images from the OCI market place.
- Create the required VCN and subnets before launching the instances. For Linux-based components that require SSH access, assign a public IP address or ensure private network connectivity is available.
- Configure a minimum of two VNICs for the GigaVUE V Series Controller: one management VNIC and one or more data VNICs. OCI does not configure IP addresses on secondary VNICs. GigaVUE provisioning scripts apply IP settings only when the secondary VNICs (with private IPs) are present at boot or the instance is rebooted after attachment.
- For successful registration of fabric components, configure firewall rules to open ports.
 - For details on how to configure firewall rules, refer to [Use VPC firewall rules](#) topic in OCI documentation.
 - For details on required ports, refer to [Network Firewall Requirement](#).
- Deployments support IPv4-only and dual-stack (IPv4 and IPv6). IPv6-only deployments are not supported. Add a security rule for IPv6-ICMP with the Source CIDR value as .
- Use OCI-assigned private IPs or DHCP for GigaVUE V Series components.

- Registration data is stored in:
 - Linux:** /etc/gigamon-cloud.conf
 - Windows UCT-V:** C:\ProgramData\uctv\gigamon-cloud.conf
- Registration parameters follow the generic-mode format:
 - groupName: <Monitoring Domain Name>
 - subGroupName: <Connection Name>
 - token: <Token>
 - remoteIP: <Remote endpoint IP(s)>
 - remotePort: <Port>
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to [Configure Tokens](#).

NOTE: Deploy GigaVUE-FM before deploying any other fabric component. GigaVUE-FM provides the registration endpoint, issues API tokens, and manages configuration and monitoring services. Other components depend on GigaVUE-FM for registration and cannot operate until GigaVUE-FM is available.

Minimum Requirements

The following table lists the minimum requirements for deploying the fabric components:

Fabric Component	Recommended OCI shape(s)	Minimum OCPUs	Minimum RAM	Networking	Notes
GigaVUE-FM	VM.Standard3.Flex	2	16 GB	1 VNIC (mgmt)	GigaVUE-FM requires Native virtualization on import.
GigaVUE V Series Node	VM.Standard.E6.Flex (recommended) / VM.Optimized3.Flex (optional)	4	32 GB	2 VNICs (mgmt + data)	Attach secondary VNIC post-launch and reboot.
GigaVUE V Series Proxy	VM.Standard3.Flex	1	4 GB	1 VNIC (mgmt)	Register proxy with GigaVUE-FM and node with proxy if using proxy.
UCT-V Controller	VM.Standard3.Flex	2	8 GB	1 VNIC (mgmt)	Enable Basic Authentication for versions 6.9 and lower.
UCT-V	VM.Standard3.Flex	1	4 GB	1 VNIC (mgmt)	Register via Controller(s).

Install GigaVUE-FM on OCI

This step is optional and applies only when an existing GigaVUE-FM instance is not available.

GigaVUE-FM is deployed as a separate instance using a dedicated GigaVUE-FM image. Unlike other components, GigaVUE-FM requires a native mode image and additional boot volume configuration.

Launch GigaVUE-FM instance

To launch GigaVUE-FM, perform the following :

1. Get the GigaVUE-FM image from the OCI market place and select **Launch Instance**.
2. Select the **Compartment** and the **version**.
3. Accept the terms and conditions and select **Launch Instance**.
4. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**.
5. Provide an **instance name**.
6. Select the **compartment** and **availability domain**.
7. Under **Image and shape**
 - Select **Change shape** and choose a shape that meets or exceeds the GigaVUE-FM minimum requirements.
8. Under **Security**,
 - a. Enable the **Shielded instance** toggle.
 - b. Enable the **Secure Boot** toggle.

NOTE: Secure Boot is required for GigaVUE-FM on OCI. These settings are available only for Gigamon-recommended instance types. If the selected shape does not support Shielded Instance, select a Gigamon-recommended instance type before enabling Secure Boot. For supported instance types, see [Supported Compute Requirements for OCI](#).

9. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**.
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

10. Under **Boot volume**:

NOTE: The instance boots from a block volume created from the GigaVUE-FM custom image. Any required boot volume options (for example, performance or encryption) are configured according to deployment standards.

- Select **Attach block volume**, a new wizard opens.
- In the wizard, under **Volume**, select **Create new volume**.
- For **Attachment type**, select **Custom**.
- Under **Volume information**, enter the **Volume name**.
- Under **Volume size and performance**, select **Custom**, and specify the **volume size** (minimum 50 GB) and the required **VPUs**(Minimum 10/GB).
- Under **Encryption**, select **Encrypt using Oracle-managed keys**.
- For **Attachment type**, select **Custom**, and then select **Paravirtualized**.
- For **Access type**, select **Read/Write**, and then select **Attach**.

11. Under SSH Keys, either generate a new key pair or upload/paste an existing public key and click on **Next**.12. Review all settings and select **Create**.

After boot, GigaVUE-FM is available at the assigned IP address or FQDN. Default GigaVUE-FM credentials and initial configuration steps follow the same behavior; refer to the GigaVUE-FM [Getting Started documentation](#) for details.

Configure Role-Based Access

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

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

To add users:

1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
 - **Name:** Actual name of the user
 - **Username:** User name configured in GigaVUE-FM
 - **Email:** Email ID of the user
 - **Password/Confirm Password:** Password for the user.
 - **User Group:** Select the desired User Group to associate the user.
GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

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

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
 - **Role Name:** Name of the role.
 - **Description:** Description of the role.
 - **Select Permission:** From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

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

To create a new user group:

1. Go to **Settings**, and then select **Authentication > GigaVUE-FMUser Management > User Groups**.
2. Select **New Group**.
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Create Monitoring Domain

To create a monitoring domain in Third Party Orchestration:

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

New Monitoring Domain

Form elements with * are required.

Cancel Save

You can think of a Monitoring Domain as a geographic region in your overall deployment. The next step is to create a Monitoring Session to set filter rules for your application traffic to their destination.

Monitoring Domain Name*

Connection Name*

Traffic Acquisition Method*

Traffic Acquisition Tunnel MTU*

Enable IPv6 Preference ☐ Disabled

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

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. UCT-V: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM. The default MTU value is 1450. Customer Orchestrated Source: If you select the Customer Orchestrated Source option, the mirrored, tunneled or the raw traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	Enable this option if you wish to use the same monitoring session configuration for the GigaVUE V Series Node deployed under this monitoring domain. Note: Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.
Traffic Acquisition Tunnel MTU (When Traffic Acquisition Method is UCT-V)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The MTU value when using IPv4 tunnels: OCI - 1410 When using IPv4 tunnels, the MTU must be 50 bytes less than the native MTU. The MTU value when using IPv6 tunnels: OCI - 1390 When using IPv6 tunnels, the MTU must be 70 bytes less than the native MTU.
Enable IPv6 Preference	Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

4. Click **Save**.



Notes:

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

You can perform the following actions in the Monitoring domain page:

Actions	Description
Edit Monitoring Domain	Use to edit a monitoring domain.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Edit SSL Configuration	Use to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	
Manage Certificates	You can use this button to perform the following actions: • Re-issue- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • Renew- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the Certificate Settings page. Refer to Configure Certificate Settings for more details.
Download Cloud Configuration File	Use this option to download the cloud configuration file (gigamon-cloud.conf). The file contains monitoring domain connection details such as groupName, subGroupName, and token, and can be used to troubleshoot AMX deployment issues. Refer to Troubleshoot AMX Deployment for more information.

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

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

Configure and Deploy GigaVUE Fabric Components using OCI- Generic Mode

This section provides information on how to deploy and register GigaVUE fabric components in Oracle Cloud Platform (OCI) for Third Party Orchestration in Generic mode. It summarizes instance recommendations, deployment guidelines, registration methods, and basic verification and troubleshooting for the below listed fabric components:

- [Deploy and Register UCT-V Controller in OCI](#)
- [Acquire Traffic using UCT-V](#)
- [Deploy and Register GigaVUE V Series Nodes and V Series Proxy \(Optional\) in OCI](#)

Deploy and Register UCT-V Controller in OCI

You can configure more than one UCT-V Controller in a monitoring domain. The UCT-V Controller is deployed as a Linux instance in OCI using the UCT-V Controller custom image.

Refer to [Acquire Traffic using UCT-V](#) for importing the UCT-V Controller instance in paravirtualized mode.

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

- . Register UCT-V Controller during Instance Launch
- . Register UCT-V Controller after Instance Launch

Register UCT-V Controller during Instance Launch

Perform the following steps to register UCT-V Controller during instance launch:

1. Get the UCT-V Controller image from the OCI market place and select Launch Instance.
2. Select the **Compartment** and the **version**.
3. Accept the terms and conditions and select **Launch Instance**.
4. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**.
5. Provide an **instance name**.
6. Select the **compartment** and **availability domain**.
7. Under **Image and shape**:
 - Select **Change image** and from the options select **My Images**.
 - Select the **Custom images** from the list.
 - Select the **UCT-V Controller** image from **Custom images list** and click on **Select Image**.
 - Select **Change shape** and choose a shape that meets or exceeds the minimum requirements and click on **Select Shape**.

8. Under **Advanced options**,

- In the **Initialization Script, Choose/Paste/Drop** the cloud-init script in the following format and click on **Next**.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteAddress: <IP address of the GigaVUE-FM>
      sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC
deployments to specify which UCT-V interface to use for communicating with the UCT-V
Controller.)
      remotePort: 443
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

9. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

10. Under SSH Keys, either generate a new key pair or upload/paste an existing public key and click on **Next**.

NOTE: If you do not specify an SSH key during instance creation, the instance uses the default credentials (username: gigamon, password: Gigamon123!). If you provide an SSH key, the instance allows key-based authentication login only.

11. Review the configuration and select **Create** to launch the instance.

After successful registration, the UCT-V Controller deployed in your OCI, appears in the Third Party Orchestration Monitoring Domain page and sends periodic heartbeat messages to GigaVUE-FM.

Register UCT-V Controller after Instance Launch

You can register UCT-V Controller after launching a Virtual Machine using a configuration file.

Perform the following steps:

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

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  token: <Token>
  remoteAddress: <IP address of the GigaVUE-FM>
  sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
  deployments to specify which UCT-V Controller interface to use for communicating with
  GigaVUE-FM.)
  remotePort: 443
```

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


```
$ sudo service uctv-cntlr restart
```
5. Verify that the UCT-V Controller appears in GigaVUE-FM and that the status is **Healthy**.

The UCT-V Controller deployed in OCI appears on the Third Party Orchestration Monitoring Domain page of GigaVUE-FM and registers with the GigaVUE-FM.

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

Deploy and Register UCT-V in OCI

Linux and Windows platforms support Deployment of GigaVUE fabric components through a third-party orchestrator.

Refer to [Acquire Traffic using UCT-V](#) for importing the UCT-V instance in paravirtualized mode.

Install the Windows UCT-V

Perform the following steps:

1. Deploy Windows server in OCI. For details, refer to [Create a Windows Server VM instance in Compute Engine](#) topic in Oracle documentation.
2. Follow the instruction in the *Connect to the VM instance by using RDP* section of [Set up Chrome Remote Desktop for Windows on Compute Engine](#) topic in the Oracle documentation.
3. Download UCT-V build in your desktop and copy it to the RDP session.
4. Turn off the Windows Firewall Defender.
5. Install the Windows UCT-V. For details, refer to [Windows UCT-V Installation](#) for step-by-step instructions on how to install Windows UCT-V.

Install the Linux UCT-V

NOTE:

- These firewall updates apply only to Canonical Ubuntu 22.04.
- Oracle Linux 9.6, CentOS 8, and Windows Server 2025 do not require any changes to their default firewall settings.

Linux-based UCT-V's require additional firewall rules to allow communication with GigaVUE-FM. Before installation, run the following commands to open the required ports:

```
sudo iptables -I INPUT 1 -p tcp --dport 8301 -j ACCEPT
sudo iptables -I INPUT 1 -p tcp --dport 9902 -j ACCEPT
sudo netfilter-persistent save
```

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

Register UCT-V during Instance Launch

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8892.

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

In your OCI, to launch the instance and register the UCT-V, perform the following steps:

1. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**. For details, refer to [Create and Start instance](#) topic in the OCI documentation.
2. Provide an **instance name**.
3. Select the **compartment** and **availability domain**.
 - Under **Image and shape**, select **Windows** for Windows UCT-V or select from the **Linux** options for Linux UCT-V.
Select the **UCT-V** image from **Custom images list** and click on **Select Image**.
 - Select **Change shape** and choose a shape that meets or exceeds the minimum requirements and click on **Select Shape**.

4. Under **Advanced options**,

- In the **Initialization Script, Choose/Paste/Drop** the cloud-init script in the following format and click on **Next**.
 - **/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.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteAddress: <IP address of the GigaVUE-FM>
      sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC
      deployments to specify which UCT-V interface to use for communicating with the UCT-V
      Controller.)
      remotePort: 443
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

5. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

6. Review the configuration and select **Create** to launch the instance.

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

Register UCT-V after Instance Launch

To register UCT-V after launching a Virtual Machine using a configuration file, perform the following steps:

1. Install the UCT-V in the Linux or Windows platform.
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, perform the following steps:
 - a. Go to File Explorer and open the File Location.
 - b. On the top navigation bar, select **View**.
 - c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  token: <Token>
  remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
  Controller 2>
  sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments
  to specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

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


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

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration, the UCT-V sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, UCT-V status appears as **Unhealthy**. If

more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If that fails as well, then GigaVUE-FM unregisters the UCT-V and it is removed from GigaVUE-FM.

Deploy and Register GigaVUE V Series Nodes and V Series Proxy (Optional) in OCI

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

Refer to [Acquire Traffic using UCT-V](#) for importing the GigaVUE V Series instance in paravirtualized mode.

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

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

1. Get the UCT-V Controller image from the OCI market place and select Launch Instance.
2. Select the **Compartment** and the **version**.
3. Accept the terms and conditions and select **Launch Instance**.
4. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**. For details, refer to [Create VMs with multiple network interfaces](#) topic in the OCI documentation.
5. Provide an **instance name**.
6. Select the **compartment** and **availability domain**.

7. Under **Image and shape**:

- Select **Change image** and from the options select **My Images**.
- Select the **Custom images** from the list.
- Select the **GigaVUE V Series / GigaVUE V Series Proxy**(optional) image from **Custom images list** and click on **Select Image**.
- Select **Change shape** and choose a shape that meets or exceeds the minimum requirements and click on **Select Shape**.

8. Under **Advanced options**,

- In the **Initialization Script, Choose/Paste/Drop** the cloud-init script in the following format and click on **Next**.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
      remotePort: 443
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

9. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

10. Under SSH Keys, either generate a new key pair or upload/paste an existing public key and click on **Next**.

NOTE: If you do not specify an SSH key during instance creation, the instance uses the default credentials (username: gigamon, password: Gigamon123!). If you provide an SSH key, the instance allows key-based authentication login only.

11. To register GigaVUE V Series Nodes directly with GigaVUE-FM:

- Set remoteIP to GigaVUE-FM IP address.
- Set remotePort to 443.

12. To register GigaVUE V Series Nodes through V Series Proxy:

- Set remoteIP to V Series Proxy IP address.
- Set remotePort to 8892.

13. Launch the instance.

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

You can register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file.

To register,

1. Launch the GigaVUE V Series Node or V Series Proxy instance using the appropriate custom image.
2. Log in to the node (SSH for Linux).

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

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  token: <Token>
  remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the proxy>
  remotePort: 443
```

4. For direct registration, set:
 - remoteIP to GigaVUE-FM IP address.
 - remotePort to 443.
5. For proxy-based registration, set:
 - remoteIP to V Series Proxy IP address.
 - remotePort to 8892.
6. Save the file.
7. Restart the GigaVUE V Series node or proxy service.
 - V Series node:
`$ sudo service vseries-node restart`
 - V Series proxy:
`$ sudo service vps restart`

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

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

Add additional VNICs for Vseries and handle OCI IP assignment

For GigaVUE V Series, a minimum of two VNICs is required. Because the OCI UI allows only one VNIC during instance creation, additional VNICs must be added after launch.

1. After the GigaVUE V Series instance reaches the Running state, navigate to the instance details page in the OCI Console.
2. Under Attached VNICs, verify that the primary VNIC is attached.
3. Attach a secondary VNIC:
 - Select Attach VNIC.
 - Provide a name (for example, NIC2).
 - Select the required subnet.
 - For the second subnet, do not assign a public IP address if public access is not required.
 - Complete the attachment.
4. Verify that the new VNIC appears under Attached VNICs with a private IP address assigned in the console.

NOTE: Important (OCI limitation)- OCI does not automatically configure IP addresses on secondary VNICs inside the guest OS. The private IP appears in the OCI Console, but the guest OS will not show an IP address on the corresponding interface until provisioning scripts run with the VNIC present at boot.

5. Reboot the GigaVUE V Series instance after all required secondary VNICs are attached so that:
 - GigaVUE V Series scripts can read the assigned IP addresses at boot, and
 - IP configuration for additional interfaces is applied correctly.

This reboot step is mandatory for GigaVUE V Series in OCI when additional interfaces are attached after the initial boot.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to [Configure Monitoring Session](#) section for more details.

1. **Access the Monitoring Session Page:**
 - a. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**.
 - b. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.

2. Add components to the canvas:

- a. Drag and drop the required components to the canvas.
- b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

3. Deploy the Monitoring Session:

- a. From the **Actions** menu, select **Deploy**.
- b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

Post-Deployment Verification

1. After deploying and registering the OCI-based fabric components, verify their status and basic connectivity:.
2. In GigaVUE-FM, verify that:
 - UCT-V Controller, UCT-V, GigaVUE V Series Nodes, V Series Proxy, and GigaVUE-FM appear under the expected Monitoring Domain and Connection.
 - The status for each component is Healthy.
3. For connectivity or registration issues:
 - Validate VCN, subnet, routing, and security lists/NSGs.
 - Confirm that /etc/gigamon-cloud.conf or C:\ProgramData\uctv\gigamon-cloud.conf contains correct registration values.
 - Check OCI console logs and instance serial console output for cloud-init or provisioning errors.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.

Acquire Traffic using Customer Orchestrated Source

This section outlines the workflow to acquire traffic directly from virtual machines and send it to GigaVUE V Series Nodes using UCT-V. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- [Install GigaVUE-FM on OCI](#)
- [Configure Role-Based Access](#)
- [Create Monitoring Domain](#)
- [Configure and Deploy GigaVUE Fabric Components using OCI - Generic Mode](#)
- [Configure and Deploy Monitoring Session](#)

Deployment Guidelines

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

- Get the required images from the OCI market place.
- Create the required VCN and subnets before launching the instances. For Linux-based components that require SSH access, assign a public IP address or ensure private network connectivity is available.
- Configure a minimum of two VNICs for the GigaVUE V Series Controller: one management VNIC and one or more data VNICs. OCI does not configure IP addresses on secondary VNICs. GigaVUE provisioning scripts apply IP settings only when the secondary VNICs (with private IPs) are present at boot or the instance is rebooted after attachment.
- For successful registration of fabric components, configure firewall rules to open ports.
 - For details on how to configure firewall rules, refer to [Use VPC firewall rules](#) topic in OCI documentation.
 - For details on required ports, refer to [Network Firewall Requirement](#).
- Deployments support IPv4-only and dual-stack (IPv4 and IPv6). IPv6-only deployments are not supported. Add a security rule for IPv6-ICMP with the Source CIDR value as .
- Use OCI-assigned private IPs or DHCP for GigaVUE V Series components.
- Registration data is stored in:
 - **Linux:** /etc/gigamon-cloud.conf
 - **Windows UCT-V:** C:\ProgramData\uctv\gigamon-cloud.conf
 - Registration parameters follow the generic-mode format:
groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
token: <Token>
remoteIP: <Remote endpoint IP(s)>
remotePort: <Port>

- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to [Configure Tokens](#).

NOTE: Deploy GigaVUE-FM before deploying any other fabric component. GigaVUE-FM provides the registration endpoint, issues API tokens, and manages configuration and monitoring services. Other components depend on GigaVUE-FM for registration and cannot operate until GigaVUE-FM is available.

Minimum Requirements

The following table lists the minimum requirements for deploying the fabric components:

Fabric Component	Recommended OCI shape(s)	Minimum OCPUs	Minimum RAM	Networking	Notes
GigaVUE-FM	VM.Standard3.Flex	2	16 GB	1 VNIC (mgmt)	GigaVUE-FM requires Native virtualization on import.
GigaVUE V Series Node	VM.Standard.E6.Flex (recommended) / VM.Optimized3.Flex (optional)	2	16 GB	2 VNICs (mgmt + data)	Attach secondary VNIC post-launch and reboot.
GigaVUE V Series Proxy	VM.Standard3.Flex	1	4 GB	1 VNIC (mgmt)	Register proxy with GigaVUE-FM and node with proxy if using proxy.
UCT-V Controller	VM.Standard3.Flex	2	16 GB	1 VNIC (mgmt)	Enable Basic Authentication for versions 6.9 and lower.
UCT-V	VM.Standard3.Flex	1	4 GB	1 VNIC (mgmt)	Register via Controller(s).

Install GigaVUE-FM on OCI

This step is optional and applies only when an existing GigaVUE-FM instance is not available.

You can install GigaVUE-FM in an OCI environment by using the OCI Console.

GigaVUE-FM is deployed as a separate instance using a dedicated GigaVUE-FM image. Unlike other components, GigaVUE-FM requires a native mode image and additional boot volume configuration.

Refer to [Acquire Traffic using Customer Orchestrated Source](#) for importing the GigaVUE-FM instance in native mode.

1. All settings must use paravirtualized drivers:

Launch GigaVUE-FM instance

To launch GigaVUE-FM, perform the following :

1. Get the GigaVUE-FM image from the OCI market place and select **Launch Instance**.
2. Select the **Compartment** and the **version**.
3. Accept the terms and conditions and select **Launch Instance**.
4. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**.
5. Provide an **instance name**.
6. Select the **compartment** and **availability domain**.
7. Under **Image and shape**:
 - Select **Change image** and choose the **GigaVUE-FMcustom image** (native mode).
 - Select **Change shape** and choose a shape that meets or exceeds the GigaVUE-FM minimum requirements.
8. Under **Security**,
 - a. Enable the **Shielded instance** toggle.
 - b. Enable the **Secure Boot** toggle.

NOTE: Secure Boot is required for GigaVUE-FM on OCI. These settings are available only for Gigamon-recommended instance types. If the selected shape does not support Shielded Instance, select a Gigamon-recommended instance type before enabling Secure Boot. For supported instance types, see [Supported Compute Requirements for OCI](#).

9. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**.
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

10. Under **Boot volume**:

NOTE: The instance boots from a block volume created from the GigaVUE-FM custom image. Any required boot volume options (for example, performance or encryption) are configured according to deployment standards.

- Select **Attach block volume**, a new wizard opens.
- In the wizard, under **Volume**, select **Create new volume**.
- For **Attachment type**, select **Custom**.
- Under **Volume information**, enter the **Volume name**.
- Under **Volume size and performance**, select **Custom**, and specify the **volume size** (minimum 50 GB) and the required **VPUs**(Minimum 10/GB).
- Under **Encryption**, select **Encrypt using Oracle-managed keys**.
- For **Attachment type**, select **Custom**, and then select **Paravirtualized**.
- For **Access type**, select **Read/Write**, and then select **Attach**.

11. Under SSH Keys, either generate a new key pair or upload/paste an existing public key and click on **Next**.

12. Review all settings and select **Create**.

After boot, GigaVUE-FM is available at the assigned IP address or FQDN. Default GigaVUE-FM credentials and initial configuration steps follow the same behavior; refer to the GigaVUE-FM [Getting Started documentation](#) for details.

On-premises- To install and upgrade GigaVUE-FM in your enterprise data center, refer to the GigaVUE-FM documentation available in the [Gigamon Documentation Library](#).

Configure Role-Based Access

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

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

To add users:

1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
 - **Name:** Actual name of the user
 - **Username:** User name configured in GigaVUE-FM
 - **Email:** Email ID of the user
 - **Password/Confirm Password:** Password for the user.
 - **User Group:** Select the desired User Group to associate the user.
GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

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

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
 - **Role Name:** Name of the role.
 - **Description:** Description of the role.
 - **Select Permission:** From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.

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

Create a Custom User Group and Assign the Custom Role and the User

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

To create a new user group:

1. Go to **Settings**, and then select **Authentication > GigaVUE-FM User Management > User Groups**.
2. Select **New Group**.
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Create Monitoring Domain

To create a monitoring domain in Third Party Orchestration:

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

New Monitoring Domain

Form elements with * are required.

Cancel Save

You can think of a Monitoring Domain as a geographic region in your overall deployment. The next step is to create a Monitoring Session to set filter rules for your application traffic to their destination.

Monitoring Domain Name*

Connection Name*

Traffic Acquisition Method*

Traffic Acquisition Tunnel MTU*

Enable IPv6 Preference ☐ Disabled

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

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. • UCT-V: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM. The default MTU value is 1450. • Customer Orchestrated Source: If you select the Customer Orchestrated Source option, the mirrored, tunneled or the raw traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	Enable this option if you wish to use the same monitoring session configuration for the GigaVUE V Series Node deployed under this monitoring domain. Note: Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.
Traffic Acquisition Tunnel MTU (When Traffic Acquisition Method is UCT-V)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The MTU value when using IPv4 tunnels: OCI - 1410 When using IPv4 tunnels, the MTU must be 50 bytes less than the native MTU. The MTU value when using IPv6 tunnels: OCI - 1390 When using IPv6 tunnels, the MTU must be 70 bytes less than the native MTU.
Enable IPv6 Preference	Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

4. Click **Save**.



Notes:

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

You can perform the following actions in the Monitoring domain page:

Actions	Description
Edit Monitoring Domain	Use to edit a monitoring domain.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Edit SSL Configuration	Use to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	
Manage Certificates	You can use this button to perform the following actions: • Re-issue- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • Renew- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the Certificate Settings page. Refer to Configure Certificate Settings for more details.
Download Cloud Configuration File	Use this option to download the cloud configuration file (gigamon-cloud.conf). The file contains monitoring domain connection details such as groupName, subGroupName, and token, and can be used to troubleshoot AMX deployment issues. Refer to Troubleshoot AMX Deployment for more information.

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

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

Configure and Deploy GigaVUE Fabric Components using OCI - Generic Mode

This section information on how to deploy and register GigaVUE fabric components in Oracle Cloud Platform (OCI) for Third Party Orchestration in Generic mode. It summarizes instance recommendations, deployment guidelines, registration methods, and basic verification and troubleshooting for the below listed fabric components:

- [Deploy and Register UCT-V Controller in OCI](#)
- [Deploy and Register UCT-V in OCI](#)
- [Deploy and Register GigaVUE V Series Nodes and V Series Proxy\(Optional\) in OCI](#)

Deploy and Register UCT-V Controller in OCI

You can configure more than one UCT-V Controller in a monitoring domain. The UCT-V Controller is deployed as a Linux instance in OCI using the UCT-V Controller custom image.

Refer to [Acquire Traffic using Customer Orchestrated Source](#) for importing the UCT-V Controller instance in paravirtualized mode.

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

Register UCT-V Controller during Instance Launch

Perform the following steps to register UCT-V Controller during instance launch:

1. Get the UCT-V Controller image from the OCI market place and select **Launch Instance**.
2. Select the **Compartment** and the **version**.
3. Accept the terms and conditions and select **Launch Instance**.
4. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**.
5. Provide an **instance name**.
6. Select the **compartment** and **availability domain**.
7. Under **Image and shape**:
 - Select **Change image** and from the options select **My Images**.
 - Select the **Custom images** from the list.
 - Select the **UCT-V Controller** image from **Custom images list** and click on **Select Image**.
 - Select **Change shape** and choose a shape that meets or exceeds the minimum requirements and click on **Select Shape**.

8. Under **Advanced options**,

- In the **Initialization Script, Choose/Paste/Drop** the cloud-init script in the following format and click on **Next**.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteAddress: <IP address of the GigaVUE-FM>
      sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC
      deployments to specify which UCT-V interface to use for communicating with the UCT-V
      Controller.)
      remotePort: 443
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

9. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

10. Under SSH Keys, either generate a new key pair or upload/paste an existing public key and click on **Next**.

NOTE: If you do not specify an SSH key during instance creation, the instance uses the default credentials (username: gigamon, password: Gigamon123!). If you provide an SSH key, the instance allows key-based authentication login only.

11. Review the configuration and select **Create** to launch the instance.

After successful registration, the UCT-V Controller deployed in your OCI, appears in the Third Party Orchestration Monitoring Domain page and sends periodic heartbeat messages to GigaVUE-FM.

Register UCT-V Controller after Instance Launch

You can register UCT-V Controller after launching a Virtual Machine using a configuration file.

Perform the following steps:

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

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  token: <Token>
  remoteAddress: <IP address of the GigaVUE-FM>
  sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
  deployments to specify which UCT-V Controller interface to use for communicating with
  GigaVUE-FM.)
  remotePort: 443
```

3. Save the file.
4. Restart the UCT-V Controller service.
\$ sudo service uctv-cntlr restart
5. Verify that the UCT-V Controller appears in GigaVUE-FM and that the status is **Healthy**.

The UCT-V Controller deployed in OCI appears on the Third Party Orchestration Monitoring Domain page of GigaVUE-FM and registers with the GigaVUE-FM.

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

Deploy and Register UCT-V in OCI

Linux and Windows platforms support Deployment of GigaVUE fabric components through a third-party orchestrator.

Refer to [Acquire Traffic using Customer Orchestrated Source](#) for importing the UCT-V instance in paravirtualized mode.

Install the Windows UCT-V

Perform the following steps:

1. Deploy Windows server in OCI. For details, refer to [Create a Windows Server VM instance in Compute Engine](#) topic in Oracle documentation.
2. Follow the instruction in the *Connect to the VM instance by using RDP* section of [Set up Chrome Remote Desktop for Windows on Compute Engine](#) topic in the Oracle documentation.
3. Download UCT-V build in your desktop and copy it to the RDP session.
4. Turn off the Windows Firewall Defender.
5. Install the Windows UCT-V. For details, refer to [Windows UCT-V Installation](#) for step-by-step instructions on how to install Windows UCT-V.

Install the Linux UCT-V

NOTE:

- These firewall updates apply only to Canonical Ubuntu 22.04.
- Oracle Linux 9.6, CentOS 9, and Windows Server 2025 do not require any changes to their default firewall settings.

Linux-based UCT-V's require additional firewall rules to allow communication with GigaVUE-FM. Before installation, run the following commands to open the required ports:

```
sudo iptables -I INPUT 1 -p tcp --dport 8301 -j ACCEPT
sudo iptables -I INPUT 1 -p tcp --dport 9902 -j ACCEPT
sudo netfilter-persistent save
```

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

Register UCT-V during Instance Launch

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8892.

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

In your OCI, to launch the instance and register the UCT-V, perform the following steps:

1. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**. For details, refer to [Create and Start instance](#) topic in the OCI documentation.
2. Provide an **instance name**.
3. Select the **compartment** and **availability domain**.
 - Under **Image and shape**, select **Windows** for Windows UCT-V or select from the **Linux** options for Linux UCT-V. Select the **UCT-V** image from **Custom images list** and click on **Select Image**.
 - Select **Change shape** and choose a shape that meets or exceeds the minimum requirements and click on **Select Shape**.
4. Under **Advanced options**,
 - In the **Initialization Script, Choose/Paste/Drop** the cloud-init script in the following format and click on **Next**.
 - **/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.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteAddress: <IP address of the GigaVUE-FM>
      sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC
      deployments to specify which UCT-V interface to use for communicating with the UCT-V
      Controller.)
      remotePort: 443
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

5. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

6. Review the configuration and select **Create** to launch the instance.

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

Register UCT-V after Instance Launch

To register UCT-V after launching a Virtual Machine using a configuration file, perform the following steps:

1. Install the UCT-V in the Linux or Windows platform.
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, perform the following steps:
 - a. Go to File Explorer and open the File Location.
 - b. On the top navigation bar, select **View**.
 - c. In the **View** tab, enable the **File name extensions** check box.

Registration:

```

groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
token: <Token>
remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments
to specify which UCT-V interface to use for communicating with the UCT-V Controller.)

```

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


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

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

Deploy and Register GigaVUE V Series Nodes and V Series Proxy(Optional) in OCI

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if the user does not wish to reveal the IP addresses of the nodes, then you can register

your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

Refer to [Acquire Traffic using Customer Orchestrated Source](#) for importing the GigaVUE V Series instance in paravirtualized mode.

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

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

1. Get the GigaVUE V Series image from the OCI market place and select Launch Instance.
2. Select the **Compartment** and the **version**.
3. Accept the terms and conditions and select **Launch Instance**.
4. image from the OCI market place and select Launch Instance.
5. Select the **Compartment** and the **version**.
6. Accept the terms and conditions and select **Launch Instance**.
7. In the OCI Console, navigate to **Compute > Instances** and select **Create instance**. For details, refer to [Create VMs with multiple network interfaces](#) topic in the OCI documentation.
8. Provide an **instance name**.
9. Select the **compartment** and **availability domain**.
10. Under **Image and shape**:
 - Select **Change image** and from the options select **My Images**.
 - Select the **Custom images** from the list.
 - Select the **GigaVUE V Series / GigaVUE V Series Proxy**(optional) image from **Custom images list** and click on **Select Image**.
 - Select **Change shape** and choose a shape that meets or exceeds the minimum requirements and click on **Select Shape**.

11. Under **Advanced options**,

- In the **Initialization Script, Choose/Paste/Drop** the cloud-init script in the following format and click on **Next**.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
      remotePort: 443
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

12. Under **Networking**:

- Select the **Networking Launch Option** as **Paravirtualized Networking**.
- Go to **Primary VNIC** and enter the **VNIC Name**
- From the **Primary network** list choose **Select existing virtual cloud network**.
- Select the **Virtual cloud network compartment** and **Virtual cloud network** from the dropdown.
- Select the required **subnet**, and specify whether to assign a **public IPv4/IPv6 address** by enabling the respective toggle.

13. Under SSH Keys, either generate a new key pair or upload/paste an existing public key and click on **Next**.

NOTE: If you do not specify an SSH key during instance creation, the instance uses the default credentials (username: gigamon, password: Gigamon123!). If you provide an SSH key, the instance allows key-based authentication login only.

14. To register GigaVUE V Series Nodes directly with GigaVUE-FM:

- Set remoteIP to GigaVUE-FM IP address.
- Set remotePort to 443.

15. To register GigaVUE V Series Nodes through V Series Proxy:

- Set remoteIP to V Series Proxy IP address.
- Set remotePort to 8892.

16. Launch the instance.

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

You can register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file.

To register,

1. Launch the GigaVUE V Series Node or V Series Proxy instance using the appropriate custom image.
2. Log in to the node (SSH for Linux).
3. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  token: <Token>
  remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the proxy>
  remotePort: 443
```

4. For direct registration, set:

- remoteIP to GigaVUE-FM IP address.
- remotePort to 443.

5. For proxy-based registration, set:

- remoteIP to V Series Proxy IP address.
- remotePort to 8892.

6. Save the file.

7. Restart the GigaVUE V Series node or proxy service.

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

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

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

Add additional VNICs for Vseries and handle OCI IP assignment

For GigaVUE V Series, a minimum of two VNICs is required. Because the OCI UI allows only one VNIC during instance creation, additional VNICs must be added after launch.

1. After the GigaVUE V Series instance reaches the Running state, navigate to the instance details page in the OCI Console.
2. Under Attached VNICs, verify that the primary VNIC is attached.
3. Attach a secondary VNIC:
 - Select Attach VNIC.
 - Provide a name (for example, NIC2).
 - Select the required subnet.
 - For the second subnet, do not assign a public IP address if public access is not required.
 - Complete the attachment.

4. Verify that the new VNIC appears under Attached VNICs with a private IP address assigned in the console.

NOTE: Important (OCI limitation)- OCI does not automatically configure IP addresses on secondary VNICs inside the guest OS. The private IP appears in the OCI Console, but the guest OS will not show an IP address on the corresponding interface until provisioning scripts run with the VNIC present at boot.

5. Reboot the GigaVUE V Series instance after all required secondary VNICs are attached so that:
 - GigaVUE V Series scripts can read the assigned IP addresses at boot, and
 - IP configuration for additional interfaces is applied correctly.

This reboot step is mandatory for GigaVUE V Series in OCI when additional interfaces are attached after the initial boot.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to [Configure Monitoring Session](#) section for more details.

1. **Access the Monitoring Session Page:**
 - a. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**.
 - b. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
2. **Create an ingress REP:**
 - a. In the canvas, from the **New** expand menu, drag and drop New Tunnel to the graphical workspace.
 - b. On the new tunnel icon, select the  menu button and select **Details**. The **Add Tunnel Spec** quick view page appears.
 - c. Enter the **Alias**, **Description**, and the **Type** details and click **Save**.
3. **Add components to the canvas:**
 - a. Drag and drop the required components to the canvas.
 - b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
4. **Deploy the Monitoring Session:**

- a. From the **Actions** menu, select **Deploy**.
- b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.

Configure Secure Tunnel for OCI

You can configure the Secure tunnels on:

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

Precrypted Traffic

Secure tunnels help protect sensitive precrypted traffic by framing packets in PCAPng format and transmitting them through a TLS socket. When you enable secure tunnel for both precrypted and mirrored traffic, the system creates two separate TLS sessions.

Recommendation: Always enable secure tunnels for precrypted traffic to ensure secure data transmission.

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

Mirrored Traffic

You can also 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](#)
- [Configure Secure Tunnel between GigaVUE V Series Nodes](#)

Prerequisites

- While creating Secure Tunnel, you must provide the following details:
 - SSH key pair
 - CA certificate
- Port 11443 is enabled in security group settings. For details, refer to [Network Firewall Requirement](#).

Notes

- Protocol versions IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, your GigaVUE-FM and the fabric components version must run version 6.6.00 or above.
- For UCT-V with a version lower than 6.6.00, if the secure tunnel is enabled in the Monitoring Session, secure mirror traffic is transmitted over IPv4, regardless of IPv6 preference.
- After configuring secure tunnels, if a Monitoring Domain contains only one GigaVUE V Series Node and that GigaVUE V Series Node reboots or restarts, then you must manually add the SSL Keys to the Monitoring Domain again. For details, refer to [Edit SSL Configuration](#).

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

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

S. No	Task	Refer to
1.	Upload a Custom Authority Certificate (CA)	You must upload a Custom Certificate to UCT-V Controller to establish 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. Select New to add a new Custom Authority. The Add Custom Authority page appears. 3. Enter or select the following information. • Alias - Alias name of the CA. • File Upload - Choose the certificate from the desired location. 4. Select Save. For more information, refer to the section Adding Certificate Authority.
2.	Upload a SSL Key	You must add a SSL key to GigaVUE V Series Node. To add SSL Key, follow the steps in the section SSL Decrypt .
3	Enable the secure tunnel	You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:

S. No	Task	Refer to
		1. In the Edit Monitoring Session page, click Options. The Monitoring Session Options page appears. 2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic.
4.	Select the SSL Key and CA certificate, after deploying the fabric components.	You must select the added SSL Key and CA Authority in GigaVUE V Series Node after creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key and CA Authority in GigaVUE V Series Node.

Configure Secure Tunnel between GigaVUE V Series Nodes

You can create secure tunnel:

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

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

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

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

S. No	Task	Refer to
1.	Upload a Certificate Authority (CA) Certificate	You must upload a Custom Certificate to UCT-V Controller to establish 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. Select New to add a new Custom Authority. The Add Custom Authority page appears. 3. Enter or select the following information. • Alias - Alias name of the CA. • File Upload - Choose the certificate from the desired location. 4. Select Save. For more information, refer to the section Adding Certificate Authority.
2.	Upload an SSL Key	You must add an SSL key to GigaVUE V Series node. To add an SSL Key, follow the steps in the section Upload SSL Keys.
3	Create a secure tunnel between UCT-V and the first GigaVUE V Series Node	You should enable the secure tunnel feature to establish a connection between the UCT-V and the first GigaVUE V Series Node. To enable the secure tunnel feature follow these steps: 1. In the Edit Monitoring Session page, click Options. The Monitoring Session Options page appears. 2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic.
4	Select the SSL Key and CA certificate, after deploying the fabric components.	You must select the added SSL Key and CA Authority in GigaVUE V Series Node after creating a Monitoring Domain configuring the fabric components in GigaVUE-FM. Refer to Edit SSL Configuration for more detailed information on how to select the added SSL Key and CA Authority in GigaVUE V Series Node.
5	Create an Egress tunnel from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session.	You must create a tunnel for traffic to flow out from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session. Refer to Create Ingress and Egress Tunnels for more detailed information on how to create tunnels. 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.

S. No	Task	Refer to
		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: • Alias - The name of the tunnel endpoint. • Description - The description of the tunnel endpoint. • Type - Select TLS-PCAPNG for creating egress secure tunnel • Traffic Direction - Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: - o MTU- The default value is 1500. - o Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. - o DSCP - Enter the Differentiated Services Code Point (DSCP) value. - o Flow Label - Enter the Flow Label value. - o Source L4 Port- Enter the Source L4 Port value - o Destination L4 Port - Enter the Destination L4 Port value. - o Flow Label - o Cipher- Only SHA 256 is supported. - o TLS Version - Select TLS Version1.3. - o Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments. - o SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. - o Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments. • IP Version - The version of the Internet Protocol. IPv4 and IPv6 are supported. • Remote Tunnel IP - Enter the interface IP address of the the second GigaVUE V Series Node (Destination IP). 4. Select Save.
6	Select the added SSL Key after deploying the fabric components in the second GigaVUE V Series Node	You must select the added SSL Key in the second GigaVUE V Series Node. Select the the second GigaVUE V Series Node and follow the steps given in Edit SSL Configuration .

S. No	Task	Refer to
7	Create an ingress tunnel in the second GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session for the second GigaVUE V Series Node.	You must create a ingress tunnel for traffic to flow in from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session. Refer to Create a 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: • Alias - The name of the tunnel endpoint. • Description - The description of the tunnel endpoint. • Type - Select TLS-PCAPNG for creating egress secure tunnel. • Traffic Direction - Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from V Series node 1. Select or enter the values as described in Step 6. • IP Version - The version of the Internet Protocol. IPv4 and IPv6 are supported. • Remote Tunnel IP - Enter the interface IP address of the first GigaVUE V Series Node (Destination IP). 4. Select Save.

Viewing Status of Secure Tunnel

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

To verify the status of secure tunnel,

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

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

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

Configure UCT-V Features

Refer to the following sections for more detailed information:

- [Configure Prefiltering](#)
- [Create Precryption Template for UCT-V](#)

Configure Prefiltering

For prefiltering the traffic, GigaVUE-FM enables you to create a prefiltering policy template and apply it to a Monitoring Session,

Considerations

- You can create and reuse a policy template across multiple monitoring sessions.
- Each monitoring session supports up to 16 prefiltering rules.
- You can edit the policy template during monitoring session configuration to customize rules and filter values.
- GigaVUE-FM does not save changes made to the template during monitoring session edits. These changes apply only to that specific session.

Rules and Notes

- Prefiltering is supported on UCT-V for Windows systems and Linux systems running Kernel version 4.18 or later.
- Prefiltering is supported for both Linux and Windows UCT-Vs .
- For single monitoring session only one prefiltering policy is applicable. All UCT-Vs in that monitoring sessions are configured with respective prefiltering policy .
- For multiple monitoring session using the same agent to acquire the traffic, if a monitoring session uses a prefilter and the other monitoring session does not use a prefilter, then you cannot apply the prefiltering policy. The policy is set to PassAll and prefiltering is not performed.

Create Prefiltering Policy Template

GigaVUE-FM allows you to create a prefiltering policy template with one or more rules. You can configure a rule with one or more filters. A single monitoring session supports a maximum of 16 rules.

To create a prefiltering policy template,

1. Go to **Traffic > Resources > Prefiltering** and select **UCT-V**.

2. Select **New**.
3. In the **Template Name** field, enter the name of the template,
4. In the **Rule Name** field, enter the name of a rule.
5. Select one of the following options:

- Pass: Allows the traffic.
- Drop: Blocks the traffic..

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

6. Select one of the following options:

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

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

7. Select a priority value from 1-8.

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

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

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

- L3
- L4

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

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

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

- Not Equal to

- Equal to

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

12. Select **Save**.

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

To enable prefiltering for a Monitoring Session, refer to

[Configure Monitoring Session Options](#).

Create Precryption Template for UCT-V

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

Rules and Notes:

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

Refer to the section the following sections for more detailed information:

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

Create Precryption Template for Filtering based on Applications

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

To create,

1. Step Go to **Traffic > Resources > Precryption**.

The **Precryption Policies** page appear

2. Step Select the **APPLICATION** tab.

3. Select **Add**.

The New Precryption Template page appears.

4. Select **csv** as the **Type**, if you wish to add applications using a .csv file.
 - a. Download the sample .csv file and edit it.
 - b. Save your .csv file.
 - c. Select **Choose File** and upload the file.
5. Select **Manual** as the **Type** if you wish to add the applications manually.
6. Enter the **Application Name** select + icon to add more applications.
7. Select **Save**.

You can view the added applications in the **APPLICATION** tab.

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

Create Precryption Template for Filtering based on L3-L4 details

To create,

1. Go to **Traffic > Resources > Precryption**. The **Precryption Policies** page appears.
2. Select the **L3-L4** tab.

3. Perform the following steps:

- a. In the **Template** field, enter a name for the template.
- b. In the **Rule Name** field, enter a name for the rule.
- c. For **Action**, select one of the following options:

- **Pass:** Passes the traffic.
- **Drop:** Drops the traffic.

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

- d. For **Direction**, select one of the following options:

- **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.

- e. In the **Priority** field, select one of the following values:

- 1: Select to pass or drop a rule in top priority.
- 2 to 8: Select to decide priority where 8 is used for setting a rule with the least priority.

NOTE: Drop rules are added based on the priority, and then pass rules are added.

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

- L3:
- L4

NOTE: You can use L4 Filter Type only with L3.

For L3, perform the following:

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

- IPv4 Source
- IPv4 Destination
- IPv6 Source
- IPv6 Destination
- Protocol: It is common for both IPv4 and IPv6.

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

- Not Equal to
- Equal to

iii. Enter or Select the Value based on the selected **Filter Name**.

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

For L4, perform the following:

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

- Source Port
- Destination Port

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

- Not Equal to
- Equal to

iii. Enter the source or destination port value.

4. Select **Save**.

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

The template is successfully created. To enable Precryption, refer to

[Configure Monitoring Session Options](#).

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

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

Configure Precryption in UCT-V

GigaVUE-FM allows you to turn on or off 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, change the option `precryption-path-mtu` in the 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.
- Using IPv6 tunnels requires GigaVUE-FM and the fabric components version 6.6.00 or above.

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

1. On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
The **Monitoring Sessions** page appears.
2. Select **New** to open the **Create a New Monitoring Session** page.
3. Enter the appropriate information for the monitoring session:
 - a. In the **Alias** field, enter the name of the monitoring session.
 - b. In the **Monitoring Domain** field, enter the name of the monitoring domain that you want to select.
 - c. In the **Connection** field, enter the desired connection(s) to include as part of the monitoring domain. You can select the connections required for the monitoring domain.
4. Select **Next**. The **Edit Monitoring Session** page appears with the new canvas.
5. Select **Options** button. The Monitoring Session options appear.
6. Select the **Precryption** tab.

7. Enable **Precryption**.
8. Select **Save**. The **Edit Monitoring Session** page appears. You can proceed to create map, tunnels, and add applications.

NOTE: We recommend enabling the secure tunnel feature whenever the Precryption feature is enabled. Secure tunnel helps to securely transfer the cloud-captured packets or precrypted data to a GigaVUE V Series Node. For more information, refer to Secure Tunnel .

Validate Precryption connection

To validate the Precryption connection, follow these steps:

- Navigate to the **Monitoring Session** dashboard and check the Precryption option. The **yes** status indicates an active state.
- Select **Status** to view the rules configured.

Limitations

During precryption, the agent generates a TCP message and captures the payload in clear text. It probes the SSL connect and accept APIs to extract Layer 3 and Layer 4 (L3/L4) details from the packet. When the agent receives the SSL data on a specific interface, it sets the default gateway's MAC address as the destination MAC address for the TCP packet. If the gateway is misconfigured, the agent sets the destination MAC address to all zeros.

Configure Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances available in your environment. You can design your monitoring session to include or exclude the instances that you want to monitor. You can also choose to monitor egress, ingress, or all traffic.

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

To design your monitoring session, refer to the following sections:

- [Create a Monitoring Session](#)
- [Create Tunnel Endpoint](#)
- [Create Raw Endpoint](#)
- [Create Map](#)
- [Add Applications to Monitoring Session](#)
- [Interface Mapping](#)

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

Create a Monitoring Session

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

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

Target Instance

- When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds it to your Monitoring Session based on your selection criteria. Similarly, when an instance is removed, it updates the Monitoring Sessions.

You can create multiple Monitoring Sessions within one Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select **New Monitoring Session** to open the New Monitoring Session configuration page.
3. In the configuration page, perform the following:
 - In the **Alias** field, enter the name of the Monitoring Session.
 - From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or select **Create New** to create a Monitoring Domain. For details, refer to the Create a Monitoring Domain section in the respective cloud guides.
 - From the **Connections** drop-down list, select the required connections to include as part of the Monitoring Domain.
 - From the **VPC** drop-down list, select the required VPCs to include as part of the Monitoring Domain.
 - Enable the **Distributed Deduplication** option to identify duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.
4. Select **Save**.
The Monitoring Session Overview page appears.

Monitoring Session Page

The table outlines core tabs in the Monitoring Session interface, each enabling targeted configuration, traffic analysis, and infrastructure visibility to support efficient session management.

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics .
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and edit the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. Note: In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold template, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options for more detailed information.
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as name of the V Series Node, health status, deployment status, Host VPC, version, and Management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping section for details.
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (Third Party Orchestration) .

NOTE: Ensure that the GigaVUE V Series Node and GigaVUE-FM are time synchronized or configure NTP time synchronization.

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

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

You can use the  icon on the left side of the Monitoring Session page to view the Monitoring Sessions list. Click  to filter the Monitoring Sessions list. In the side bar, you can:

- Create a new Monitoring Session
- Rename a Monitoring Session
- Hover over, click the check box of the required Monitoring Session(s) and perform bulk actions (Delete, Deploy, or Undeploy).

Monitoring Session Options

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

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

Access the TRAFFIC PROCESSING tab

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

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. On the left pane with the Monitoring Sessions list view, select a Monitoring Session.
3. Select the **TRAFFIC PROCESSING** tab.

Apply Threshold Template

You can apply the Threshold configuration to a Monitoring Session before deployment.

To apply a threshold,

1. In the **TRAFFIC PROCESSING** page, select **Options > Thresholds**.
2. Select an existing threshold template from the **Select Template** drop-down list. You can create a template using **New Threshold Template** option and apply it.
3. Select **Apply**.

For more information, refer to the [Traffic Health Monitoring](#) section.

The template is added to the Monitoring Session.

**Notes:**

- Undeploying the Monitoring Session does not remove the applied Thresholds.
- You can also view the details related to the applied thresholds, such as traffic element, metrics, type, trigger values, and time intervals, in the threshold window.

Select **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User-Defined Applications

To enable a defined application,

1. In the Monitoring Session **TRAFFIC PROCESSING** page, select **Options > User Defined Applications**.
2. Enable the **User-defined Applications** toggle button.
3. From the **Actions** drop-down, add one of the existing applications or create a User-Defined Application.

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

Enable Distributed De-duplication

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

To enable,

1. In the **TRAFFIC PROCESSING** page, select **Options > Distributed De-duplication**.
2. Enable the toggle.

**Notes:**

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

Create Ingress and Egress Tunnel

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

Create a new tunnel endpoint

To create,

1. Perform one of the following and navigate to the **TRAFFIC PROCESSING** tab:
 - Create a new monitoring session
 - Select **Actions > Edit** on an existing monitoring session.

The GigaVUE-FM Monitoring Session canvas page appears.

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

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

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

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

5. Select **Save**.

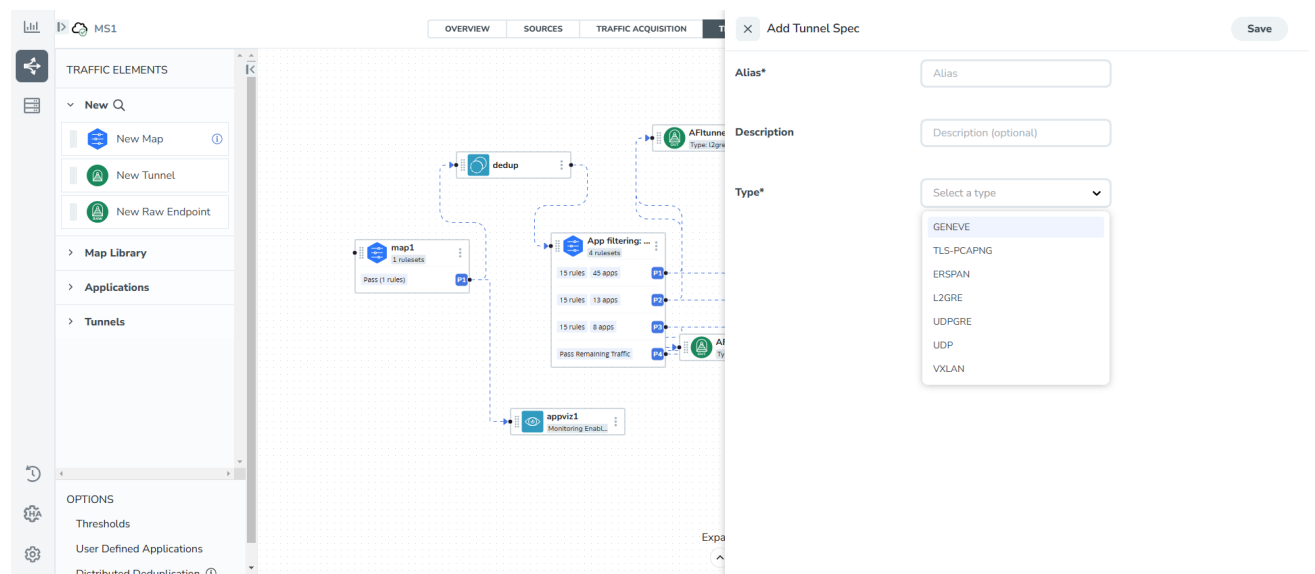


Table 2: Details - Add Tunnel Specifications

Field	Description
Alias	The name of the tunnel endpoint.
Description	The description of the tunnel endpoint.

Field	Description	
Admin State Note: This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable or down tools. Each egress tunnel configured on the GigaVUE V SeriesNode has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. GigaVUE-FM only disable the tunnels when it receives a notification via REST API indicating that a tool or group of tools is down. Note: This option is not supported for TLS-PCAPNG tunnels.	
Type	The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to configure secure tunnels on your physical device conveniently. For details, refer to Secure Tunnels .		
In	Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value that is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port used to establish the connection to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port used to establish the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint.	
	Remote Tunnel IP/FQDN	For egress tunnels, specify the destination endpoint by using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN). FQDN support applies only to VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address changes. If the FQDN resolves to both IPv4 and IPv6 addresses, the system selects the address based on the preferred IP stack configured for the monitoring domain.
	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.

Field	Description
DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
Multi Tunnel	Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support.  Notes: - You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session. - When you enable Multi-Tunnel on a VXLAN tunnel and set the number of tunnels, GigaVUE-FM automatically creates the additional VXLAN tunnel endpoints. Any later changes to the original VXLAN tunnel, such as disabling Multi-Tunnel or modifying Domain Tagging do not update these auto created endpoints. They continue to retain the configuration that existed at the time they were created. To apply updated settings, you must delete the VXLAN TEP and the associated LB application, then recreate the LB and VXLAN TEP with the new configuration, and re-establish the link between them.
Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping.

Field	Description	
		NOTE: This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UDPGRE/L2GRE tunnels. It routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device. For details, refer to the Secure Tunnels .		
In	Choose In (decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UDPGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP/FQDN	For egress tunnels, specify the destination endpoint by using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN). FQDN support applies only to VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address

Field	Description	
		changes. If the FQDN resolves to both IPv4 and IPv6 addresses, the system selects the address based on the preferred IP stack configured for the monitoring domain.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. NOTE: This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.
ERSPAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to Secure Tunnels section.		

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

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

Managing Tunnel Endpoints

Apply a threshold template to Tunnel End Points

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

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

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

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

Delete Tunnel Endpoints

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

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.

NOTE: The maximum number of links that can egress from any endpoint in V Series is four.

To add Raw Endpoint to the Monitoring Session,

1. Drag and drop **New Raw Endpoint** from the **New** expand menu to the graphical workspace.
2. On the new raw endpoint icon, click the  menu button and select **Details**. The **Raw** quick view page appears.
3. Enter the Alias and Description details for the Raw End Point and click **Save**.

4. Perform the following steps to deploy the Monitoring Session after adding the Raw Endpoint:
 - a. On the **TRAFFIC PROCESSING** page, select **Actions>Deploy**. The **Deploy Monitoring Session** dialog box appears.
 - b. Select the desired V Series Nodes to deploy the Monitoring Session.
 - c. Select the interfaces for each of the REPs and the TEPs deployed in the Monitoring Session from the drop-down menu for the selected individual V Series Nodes.
 - d. Select **Deploy**.
5. Select **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map

Terms to know before creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	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 $\cap$ 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 • VM Tag Source The traffic direction is as follows: • 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. • Use the GigamonNode Tag to exclude any Gigamon devices from the target. • When using VM Name filter for selecting the Virtual Machines using Inclusion and Exclusion Maps, wild-cards in VM names are not supported. You must use the prefix of the Virtual Machine name.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

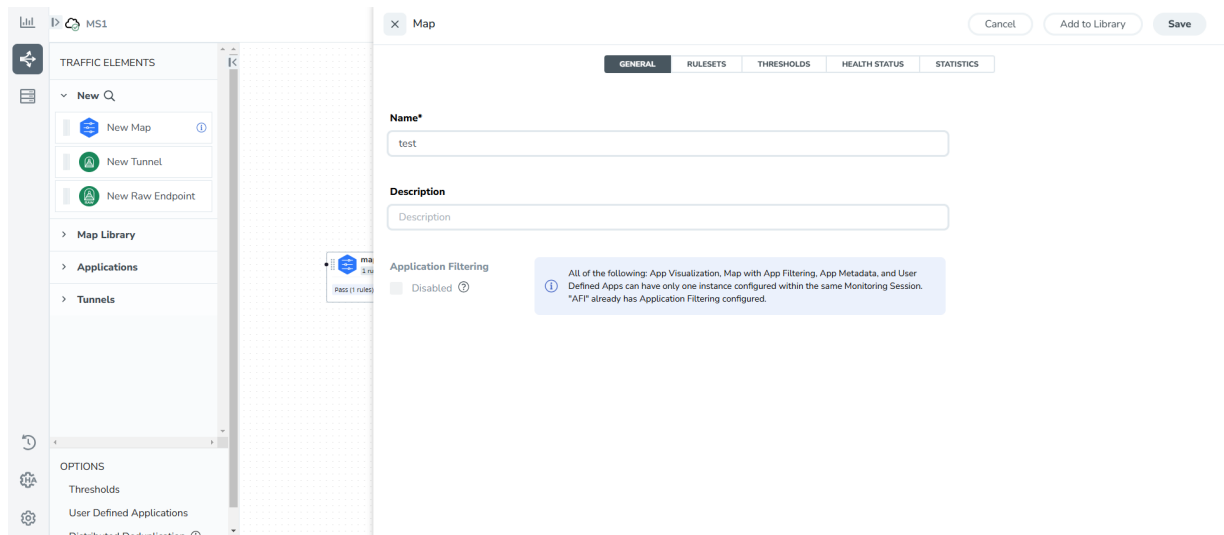
Rules and Notes:

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

- If a packet is fragmented then all the fragments are destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. For details, refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide*.

To create a new map:

1. Drag and drop **New Map** from the **New** expand menu to the graphical workspace. The **Map** quick view appears.



2. On the new Map quick view, select the **General** tab and enter the required information as described below.
 - a. Enter the **Name** and **Description** of the new map.
 - b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence.
Enabling this option allows you to filter traffic based on Application name or family. Refer to [Application Filtering Intelligence](#).

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

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

3. Select the **Rule Sets** tab.a. **To create a new rule set:**

- i. Select **Actions > New Ruleset**.
- ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
- iii. Enter the Application Endpoint in the Application EndPoint ID field.
- iv. Select a required condition from the drop-down list.
- v. Select the rule to **Pass** or **Drop** through the map.

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

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

4. Select **Save**.

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

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

- To edit a map, select the  menu button of the required map on the canvas and click **Details**, or select **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, select on the Thresholds tab. For more details on how to create or apply threshold templates, refer to [Monitor Cloud Health](#).
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Select the rules and apps buttons to open the quick view menu for RULESETS.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a Monitoring Session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. In the **GENERAL** tab, enter the name as Map 1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.

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

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

Map Library

Map Library is available in the **TRAFFIC PROCESSING** canvas page. You can add and use the maps from the Monitoring Session.

To add a map,

1. From the **Monitoring Session** screen, select **TRAFFIC PROCESSING**.

The GigaVUE-FMCanvas page appears.

2. From the page, select the desired map and save it as a template.
3. Select **Details**.

The Application quick view appears.

4. Select **Add to Library** and perform one of the following:
 - From the **Select Group** list, select an existing group.
 - Select **New Group** to create a new one.
5. In the **Description** field, add details, and select **Save**.

The map is added to Map Library. You can use the added map for all the monitoring sessions.

Reusing a map

From the **Map Library**, drag and drop the saved map.

Add Applications to Monitoring Session

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

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

- Application Metadata Intelligence
- Application Filtering Intelligence

Deploy Monitoring Session

You can deploy the Monitoring Session on all the nodes and view the report.

To deploy the Monitoring Session,

1. **Add components to the canvas**

Drag and drop the following items to the canvas as required:

- **Ingress tunnel** (as a source): From the **New** section.
- **Maps**: From the **Map Library** section.
- **Inclusion and Exclusion maps**: From the Map Library to their respective section at the bottom of the workspace.
- GigaSMART **apps**: From the **Applications** section.
- **Egress tunnels**: From the **Tunnels** section.

2. **Connect components**

Perform the following steps after placing the required items in the canvas.

- a. Hover your mouse on the map
- b. Select the dotted lines
- c. Drag the arrow over to another item (map, application, or tunnel).

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

3. (Optional) Review Sources

Select the **SOURCES** tab to view details about the subnets and monitored instances.

The monitored instances and the subnets are visible in orange.

Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method.

4. Deploy the Monitoring Session

From the **Actions** menu, select **Deploy**.

After successful deployment on all the V Series Nodes, the status appears as **Success** on the **Monitoring Sessions** page.



Important:

Bulk Deploy: Select one or more monitoring sessions, and then choose Deploy from the available actions to deploy them simultaneously.

When deploying multiple monitoring sessions, GigaVUE-FM checks for sessions with undeployed changes. If any are found, GigaVUE-FM displays a warning message before proceeding the action. Bulk Deploy uses the previously deployed configuration for those sessions by default. Your latest changes are not applied.

To include the latest changes in a **Bulk Deploy** action:

1. Deploy the monitoring session with undeployed changes individually. From the **Actions** menu, select **Deploy**.
2. After the deployment completes, run **Bulk Deploy** again.

If you run **Bulk Deploy** without deploying the individual monitoring session first, GigaVUE-FM continues to use the previously deployed configuration.

View the Deployment Report

You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.

- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
 - **Success:** Not deployed on one or more instances due to V Series Node failure.
 - **Failure:** Not deployed on all V Series Nodes or Instances.

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

The Monitoring Session Deployment includes two key configuration:

- [Interface Mapping](#)
- [Tool Exclusion](#)

Interface Mapping

It allows to associate specific network interfaces (from monitored instances) with monitoring tools. This ensures that traffic from selected sources is accurately mirrored and routed for analysis. You can:

- Select interfaces from available instances.
- Map each interface to one or more monitoring tools.
- Apply filters or conditions to refine traffic selection.

Tool Exclusion

It excludes specific monitoring tools from receiving mirrored traffic during a monitoring session. This option is available only when the Traffic Acquisition method is set to **VPC Traffic Mirroring**.

Deploy Monitoring Session

INTERFACE MAPPING **TOOL EXCLUSION**

Tool instances should be excluded to avoid traffic looping. Review the instances with the same IP address below and select the tool instance to exclude.

IP ADDRESS	TOOL EXCLUSION
10.10.10.100	Excluded
10.10.10.200	--
10.10.10.300	Excluded

VM NAME	ID
VM100	i-0cae6ab7c57a9d237
☒ Tool	i-0cae6ab7c57a9d328
VM200	i-0cae6ab7c57a9f395

Cancel Deploy

- Review the list of available monitoring tools.
- Select the tools to exclude from traffic flow.
- Confirm the exclusion before deploying the session.

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](#)
- [View Health Status](#)
- [Traffic Health](#)
- [Monitoring Session Statistics](#)
- [Visualize Network Topology](#)

Configuration Health Monitoring

The configuration health status provides detailed information about the configuration and deployment status of the deployed monitoring session.

It supports specific fabric components and features on the respective cloud platforms.

Configuration Health Monitoring	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware	GigaVUE Cloud Suite for Nutanix	GigaVUE Cloud Suite for OCI
GigaVUE V Series Nodes	✓	✓	✓	✓	✓	✓
UCT-V	✓	✓	✓	✗	✗	✓
VPC Mirroring	✓	✗	✗	✗	✗	✗
OVS Mirroring and VLAN Trunk Port	✗	✗	✓	✗	✗	✗

Refer to the [View Health Status](#) section to view the configuration health status.

View Health Status

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

View Health Status of an Application

To view the health status of an application across an entire Monitoring Session,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
2. Select a Monitoring Session and navigate to the **TRAFFIC PROCESSING** tab.
3. Select the application for which you wish to see the health status and select **Details**. The quick view page appears.
4. Select the **HEALTH STATUS** tab.

This displays the application's **Configuration Health**, **Traffic Health**, and the **Operational Health**, along with the thresholds applied to each.

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

View Operational Health Status of an Application

When you configure the Application Metadata Exporter to use **Kubernetes** as the workload platform, the V Series Node transmits failure and error events to GigaVUE-FM, which processes them and updates the node's health status on the Monitoring Session page. When interacting with Kubernetes workloads, the system may encounter errors while retrieving resources such as pods, services, nodes, or endpoints. Refer to [Errors](#) for additional error details.

Operational events for Exporter:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Server Type>_<Message>

Server Types: CLOUD EXPORT, KAFKA

Message	Description
UPLOAD_MAX_TRIES_EXCEED	Upload retries exceeded the maximum limit Example: CLOUDEXPORTER_UPLOAD_MAX_TRIES_EXCEED
REACHABILITY_FROM_AMX_TO_TOOLS	AMX failed to reach the tool (Cloud Exporter server or Kafka server) Example: CLOUDEXPORTER_REACHABILITY_FROM_AMX_TO_TOOLS

Message	Description
NO_IP_ADDRESS	No IP address was configured on the interface Example: CLOUDEXPORTER_NO_IP_ADDRESS
EXPORTER_UPLOAD_ERROR	Upload to the exporter failed Example: CLOUDEXPORTER_EXPORTER_UPLOAD_ERROR

Operational events for Enrichment:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Operation Type>_<Message>

Operation Types: GETSERVICES, GETPODS, GETNODES, GETENDPOINTS, WATCHALL

Message	Description
K8S_AUTHORIZATION_FAILURE	The request was denied due to insufficient permissions Example: GETPODS_K8S_AUTHORIZATION_FAILURE
K8S_AUTHENTICATION_FAILURE	Authentication failed. Verify your credentials Example: GETPODS_K8S_AUTHENTICATION_FAILURE
K8S_UNHANDLED_ERROR	An unspecified error occurred. Check the error description Example: GETPODS_K8S_UNHANDLED_ERROR

View Health Status for Individual GigaVUE V Series Nodes

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

1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. In the **Overview** tab, view the health status of the required GigaVUE V Series Node from the chart options.

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, select the required Monitoring Session from the list view.
2. On the Overview tab, select the GigaVUE V Series Node from the All V Series Nodes drop-down menu.

The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

Traffic Health Monitoring

GigaVUE-FM monitors the traffic health of the entire Monitoring Session and each individual GigaVUE V Series Node in that session. It checks for issues like packet drops or traffic overflows.

When it detects a problem, GigaVUE-FM updates the health status of the related Monitoring Session. It monitors traffic health in near real-time.

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. Then, GigaVUE-FM then uses this data to calculate traffic health.

If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, you must add the GigaVUE-FM public IP address as the Target Address in the Data Notification Interface on the Event Notifications page.

For details, refer to the section in the *GigaVUE Administration Guide*.

For instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status, refer to the following topics:

- [Supported Resources and Metrics](#)
- [Create Threshold Templates](#)
- [Apply Threshold Template](#)
- [Clear Thresholds](#)

Consideration to configure a threshold template

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session reapplies all the threshold policies associated with that Monitoring Session.
- Deleting the Monitoring Session clears all the threshold policies associated with that Monitoring Session.

- Threshold configuration is applied before deploying a Monitoring Session and remains even if the session is undeployed.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring. Refer to [Create Threshold Templates](#) and [Apply Threshold Template](#) sections for details on Threshold types and Threshold events.

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
AMX	1. Tx Packets 2. Rx Packets 3. Packets Dropped 4. Ingestor - Rx packets 5. Ingestor - Packets Dropped 6. Ingestor - Rx Octets 7. Ingestor - Octets Dropped 8. Ingestor - Records Dropped	1. Difference 2. Derivative	1. Over 2. Under

	9. Workload - Records Dropped 10. Workload - Req Auth Errors 11. Workload - Req Timedout Errors 12. Workload - Req Errors 13. Exporter - Avg File Size 14. Exporter - File Uploads 15. Exporter - File Uploads Errors 16. Enrichment - One Minute Percent		
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SBIPOE	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
PCAPNG	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Templates

To create threshold templates:

1. Go to **Inventory > Resources > Threshold Templates**.

The **Threshold Templates** page appears.

2. Select **Create** to open the New Threshold Template page.

- Enter the appropriate information for the threshold template as described in the following table:

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Traffic Element	Select the resource for which you wish to apply the threshold template. Ex: TEP, REP, Maps, Applications like Slicing, De-dup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that need to be monitored. For example: Tx Packets, Rx Packets.
Type	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.

- Select **Save**.
The newly created threshold template is saved, and it appears on the **Threshold templates** page.

Apply Threshold Template

You can apply your threshold template across the entire Monitoring Session and also to a particular application.

Apply Threshold Template to Monitoring Session

To apply the threshold template across a Monitoring Session, follow these steps:

- On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
- In the **TRAFFIC PROCESSING** tab, select **Options>Thresholds** menu.
- From the **Select Template** drop-down list, select the template you wish to apply across the Monitoring Session.
- Select **Apply**.

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

Apply Threshold Template to Applications

Applying threshold template across Monitoring Session does not overwrite the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it overwrites the existing threshold value for that particular application.

To apply the threshold template to a particular application in the Monitoring Session, follow these steps:

1. On the **Monitoring Session** page, select **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Select on the application for which you wish to apply or change a threshold template and select **Details**. The **Application** quick view opens.
3. Select the **Thresholds** tab.
4. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
5. Select **Save**.

Clear Thresholds

You can clear the thresholds across the entire Monitoring Session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the Monitoring Session, follow these steps:

1. On the **Monitoring Session** page, select the **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Select the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Select the **Thresholds** tab.
4. Select **Clear All** and then select **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session, follow these steps:

1. On the left navigation pane in GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Select the Monitoring Session and navigate to **TRAFFIC PROCESSING > Options >**

Thresholds,

3. Select **Clear Thresholds**.
4. On the **Clear Threshold** pop-up appears, select **Ok**.

NOTE: Clearing thresholds at Monitoring Session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application, refer to [Clear Thresholds for Applications](#)

View Monitoring Session Statistics

The Monitoring Session **OVERVIEW** page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.

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

- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.
- You can filter the traffic and view the statistics based on factors such as **Incoming, Outgoing, Ratio (Out/In), Incoming Packets, Outgoing Packets, Ratio (Out/In) Packets**. You can select the options from the drop-down list box in the **TOTAL TRAFFIC** section of the **OVERVIEW** page.
- You can also view the statistics of the Monitoring Session deployed in the individual V Series Nodes. To view the statistics of the individual GigaVUE V Series Node, select the name of the **V Series Node** for which you want to view the statistics from the GigaVUE V Series Node drop-down list on the bottom left corner of the **OVERVIEW** page.

Visualize the Network Topology

You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

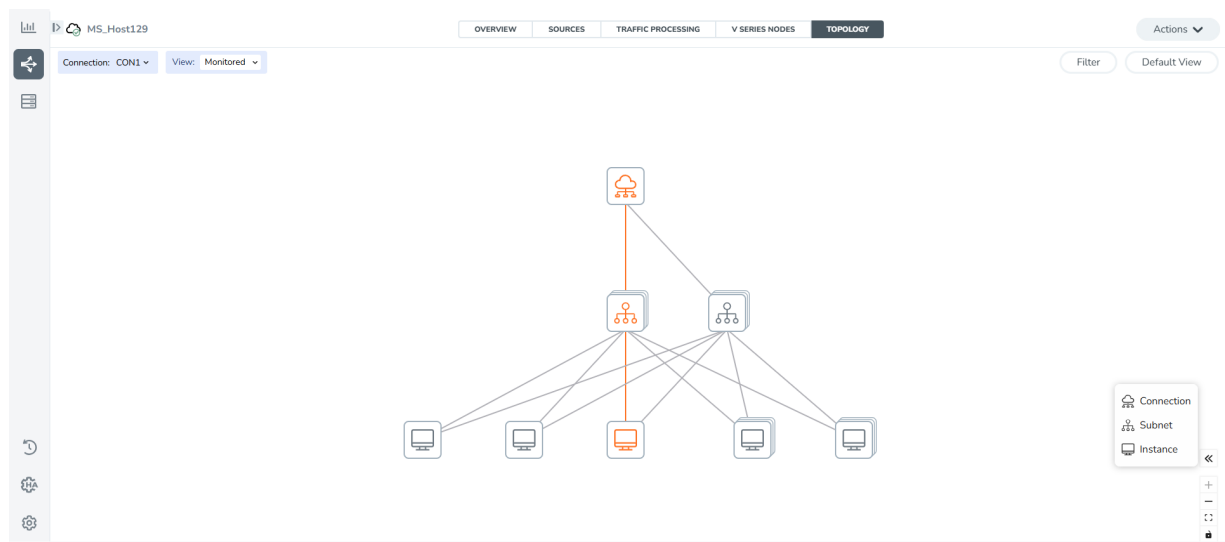
To view the topology in GigaVUE-FM:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
The **Monitoring Sessions** landing page appears.
2. Create a Monitoring Session or select an existing Monitoring Session,
3. Open the **TOPOLOGY** tab.
4. From the **Connection** list on the Topology page, select a connection.

The topology view of the monitored subnets and instances in the selected session is displayed.

5. From **View**, select one of the following instance types:

- Fabric
- Monitored



6. (Optional) Hover over the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances.
7. Select the subnet or VM group icons to explore the subnets or instances within the group.

In the Topology page, you can also perform the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.

- Apply Navigation controls, such as:
 - Use the arrows at the bottom-right corner to move the topology page up, down, left, or right.
 - Use **+** or **-** icons to zoom in and zoom out of the topology view.
 - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

Administer GigaVUE Cloud Suite for OCI

You can perform the following administrative tasks in GigaVUE-FM :

- [Configure Certificate Settings](#)
- [Interface Mapping](#)
- [Configure Third Party Orchestration Settings](#)
- [Role Based Access Control](#)

Configure Certificate Settings

To configure certificate settings:

1. Go to **Inventory > VIRTUAL**.
2. Select your cloud platform.
3. Select **Settings > Certificate Settings**.
The **Certificate Settings** page appears.
4. From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

NOTE: If selecting RSA 8192, the certificate generation may take longer due to the increased key size.

5. In the **Validity** field, enter the total validity period of the certificate.
6. In the **Auto Renewal** field, enter the number of days before expiration of the auto-renewal process should begin.
7. Select **Save**.

Interface Mapping

You can remap interfaces for individual GigaVUE V Series Nodes within a Monitoring Session.

Note: When using Raw and Tunnel In, Interface Mapping is mandatory before you deploy the Monitoring Session.

To perform interface mapping,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.

The **Monitoring Sessions** landing page appears.

2. Navigate to the **V SERIES NODES** tab and select **Interface Mapping**.

The **Deploy Monitoring Session** dialog box appears.

3. Select the GigaVUE V Series Nodes to which you wish to map the interface.
4. From the drop-down menu of the GigaVUE V Series Nodes, select the interfaces for the following deployed in the Monitoring Session:

- REPs (Raw Endpoints)
- TEPs (Tunnel Endpoints)

5. Select **Deploy**.

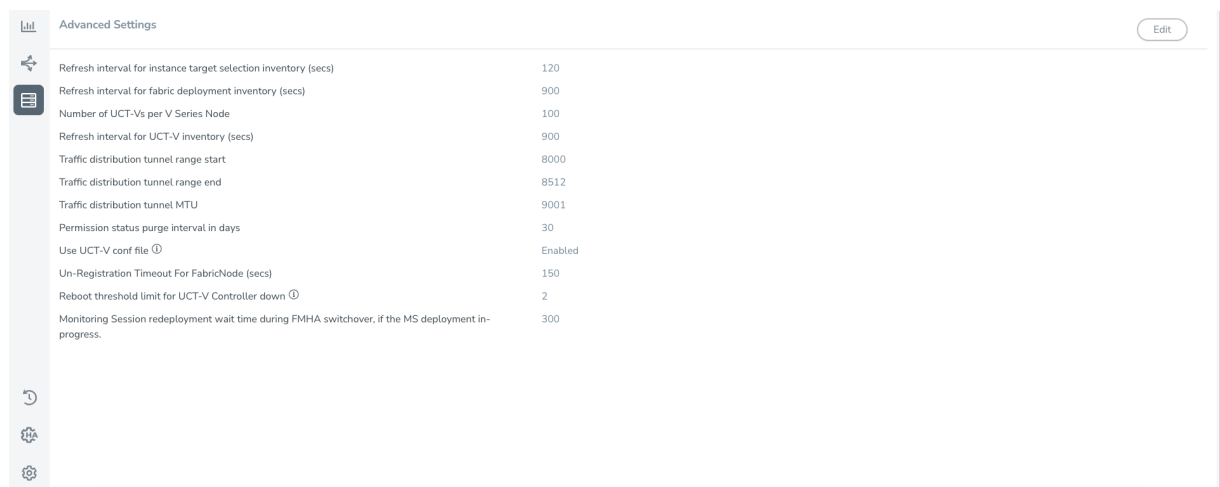
NOTE: The updated mappings take effect when deployed.

Configure Third Party Orchestration Settings

This topic allows you to set the maximum number of connections, adjust refresh intervals for instance and non-instance inventory, and define the maximum batch size for monitoring session updates.

To configure these settings,

1. In GigaVUE-FM, go to **Inventory > VIRTUAL > Third-Party Orchestration**.
2. Select **Settings**.
3. In the **Settings** page, select the **Advanced** tab and update the required values.



Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of the instances.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric components
Number of UCT-Vs per V Series Node	Specifies the maximum number of UCT-Vs that you can assign to the GigaVUE V Series Node. Points to Note: - At the time of GigaVUE V Series Node deployment, GigaVUE-FM maps the UCT-Vs equally to all the available GigaVUE V Series Node. For example, there are 10 UCT-Vs, two GigaVUE V Series Nodes, and 10 f UCT-Vs per V Series Node. Even though the first GigaVUE V Series Node can accommodate all the ten UCT-Vs, it is shared equally between the two GigaVUE V Series Node to balance the traffic load. - When a new GigaVUE V Series Node is added to the deployment, GigaVUE-FM does not re-balance the UCT-Vs to the new GigaVUE V Series Node unless the number of UCT-Vs mapped to the GigaVUE V Series Node is greater than the Number of UCT-Vs per V Series Node.
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available. Note: When you upgrade to version 6.5 or above, GigaVUE-FM resets the UCT-V Refresh Interval field to its default. To retain your custom value, you must manually reconfigure it.
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.

Settings	Description
Traffic distribution tunnel MTU	Specifies the MTU value for the traffic distribution tunnel.
Use UCT-V conf file	Enable this option to allow interface mirroring to follow the configuration defined in the file. Disable it to mirror traffic from all physical interfaces. Note: - When changing the UCT-V conf file option from enabled to disabled, ensure to undeploy the Monitoring Session and delete the Monitoring Domain. Once changed, you should create a new Monitoring Domain and configure the Monitoring Session. - When changing the UCT-V conf file option from disabled to enabled, do the following: - Edit the uctv.conf file Windows: C:\ProgramData\Uctv\uctv.conf Linux: /etc/uctv/uctv.conf - Delete the skipConf file from the backup folder Windows: C:\ProgramData\Uctv\bak\skipConf Linux: /var/lib/uctv/bak/skipConf - Restart the UCT-V Windows: Restart from the Task Manager Linux: sudo service uctv restart
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.

About Audit Logs

Audit logs track the changes and activities that occur in the virtual nodes due to user actions. You can filter the logs to view specific information.

Access Audit Logs

Navigate to **Dashboard > SYSTEM > Audit Logs**. The **All Audit Logs** page appears.

All Audit Logs

Filter Manage

Filter : none

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags	
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS			
2020-1...	admin	logout fmUser a...	User	fm			SUCCESS			
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS			
2020-1...	admin	update resource...	Monitoring	...			SUCCESS			

Go to page: 1 of 16 Total Records: 106

Parameters

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 the system logs. For example, - Log in and Log out based on users. - Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details about the usage either in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	For failed status provides a brief update on the reason..

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

Filtering the audit logs

You can filter to view specific type of logs based on the following criteria:

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

To filter the audit logs,

1. Select **Filter**.

A quick view for Audit Log Filters displays.

2. Specify one or all of the following:

- **Start Date** and **End Date** to display logs within a specific time range.
- **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
- **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
- **Where** narrows the logs to particular of system that the log is related to. Select **All Systems** apply both GigaVUE-FM and device to the filter criteria. **Result** narrows the logs related to failures or successes. Select **All Results** to apply both success and failure to the filter criteria.

3. Select **OK** to apply the selected filters to the **Audit Logs** page.

Debuggability and Troubleshooting

Use the following information to help diagnose and resolve GigaVUE V Series Nodes issues.

Sysdumps

A sysdump is a log and system data package generated when a GigaVUE V Series Node experiences a crash (such as kernel, application, or hardware failure). These files are essential for debugging.

You cannot download sysdump files if the associated fabric component is deleted or unreachable.

Sysdumps—Rules and Notes

Consider the following points before you generate sysdumps:

- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when generation of another sysdump file is in progress.
- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- You can download only one sysdump file per GigaVUE V Series Node at a time.
- You can delete sysdump files in bulk for a GigaVUE V Series Node.

- To ensure efficient usage, the system limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

Generate a Sysdump File

To generate a sysdumps file:

1. Select the required node, and use one of the following options to generate a sysdump file:
 - Select **Actions > Generate Sysdump**.
 - In the lower pane, go to **Sysdump**, and select **Actions > Generate Sysdump**.
2. View the latest status, click **Refresh**.

The screenshot displays the 'Third Party Orchestration' interface. The top navigation bar includes 'Monitoring Domain', 'UCT-V Upgrade', and 'Settings'. A sidebar on the left contains icons for various functions. The main area shows a table of monitoring domains and their connections. Below this, a detailed view for 'Fabric Node: 10.114.83.148' is shown, including a 'Sysdump' tab. This tab contains a table of generated sysdump files.

MONITORING DOMAIN	CONNECTIONS	MANAGEMENT IP	TYPE	VERSION	STATUS
md					
	md-1				Connected
	md1				Connected
		10.114.83.148	V Series Node	6.11.00	Ok
md2					
	md2-conn				Connected

FILE NAME	STATUS	DATE CREATED	FILE SIZE
sysdump-vseries-20250221-060550.tgz.bz2	Completed	2025-02-21 06:06:57	12.604 KB
sysdump-vseries-20250221-054728.tgz.bz2	Completed	2025-02-21 05:48:46	13.558 KB
sysdump-vseries-20250221-053539.tgz.bz2	Completed	2025-02-21 05:36:55	14.725 KB
sysdump-vseries-20250221-053241.tgz.bz2	Completed	2025-02-21 05:33:50	12.272 KB
sysdump-vseries-20250221-052713.tgz.bz2	Completed	2025-02-21 05:28:34	15.125 KB

Other Actions

- To download a sysdump file, select the file in the lower pane, and then click **Actions > Download**.
- To delete a sysdump file,
 1. Select the file in the lower pane.
 2. Select the desired sysdump file.

3. Select **Actions > Delete**.

- To bulk delete, select all the sysdump files, and then select **Actions > Delete All**.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

Documentation

©This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.14 Hardware and Software Guides	
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.	
Hardware	
how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices	
GigaVUE-HC1 Hardware Installation Guide	
GigaVUE-HC3 Hardware Installation Guide	
GigaVUE-HC1-Plus Hardware Installation Guide	
GigaVUE-HCT Hardware Installation Guide	
GigaVUE-TA25 Hardware Installation Guide	
GigaVUE-TA25E Hardware Installation Guide	
GigaVUE-TA100 Hardware Installation Guide	
GigaVUE-TA200 Hardware Installation Guide	

GigaVUE Cloud Suite 6.14 Hardware and Software Guides
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
GigaVUE Inline Solutions Guide (NEW) (previously included in the GigaVUE Fabric Management Guide)
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite 6.14 Hardware and Software Guides

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Universal Cloud TAP - Container Deployment Guide

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions

Reference Guides

GigaVUE-OS CLI Reference Guide

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices

Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.

Release Notes

GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;
important notes regarding installing and upgrading to this release

Note: Release Notes are not included in the online documentation.

Note: Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software and Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

In-Product Help

GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

1. Log in to [My Gigamon](#).
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

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

Documentation Feedback

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

documentationfeedback@gigamon.com

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

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

For Online Topics	Online doc link	(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)