



GigaVUE Cloud Suite for Azure - Deployment Guide

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 for Azure - Deployment Guide	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite Deployment Guide – Azure	10
Overview of GigaVUE Cloud Suite for Azure	11
GigaVUE-FM	12
UCT-V	12
Single Network Interface Configuration	13
Multiple Network Interface Configuration	13
Loopback Network Interface Configuration	14
UCT-V Controller	14
GigaVUE V Series Node	15
Monitoring Domain	15
Monitoring Session	15
Cloud Overview Page (Azure)	16
Top Menu	17
Viewing Charts on the Overview Page	18
Viewing Monitoring Session Details	20
Introduction to the Supported Features on GigaVUE Cloud Suite for Azure	20
Inline V Series (Azure)	21
Inline V Series Deployment Types	21
Architecture of Inline V Series Solution in Azure	22
Limitation	23
Secure Communication between GigaVUE Fabric Components	23
GigaVUE-FM acts as the PKI	24
Bring Your Own CA	25
Rules and Notes	25
Precryption™	25
How Gigamon Precryption Technology Works	26
Why Gigamon Precryption	27
Key Features	27
Key Benefits	27
How Gigamon Precryption Technology Works	28

Supported Platforms	29
Prerequisites	30
Secure Tunnels	31
Prefiltering	33
Monitor Cloud Health	33
Analytics for Virtual Resources	34
Virtual Inventory Statistics and Cloud Applications Dashboard	34
Customer Orchestrated Source - Use Case	40
Check for Required IAM Permissions in Azure	40
View Permission Status Reports	41
Traffic Acquisition using Azure Virtual Network TAP	42
Rules and Notes	43
Limitation	43
Licensing for GigaVUE Cloud Suite for Azure	43
Default Trial Licenses	44
License Requirements for Monitoring Sessions	45
Volume Based License (VBL)	45
Base Bundles	45
Add-on Packages	47
How GigaVUE-FM Tracks Volume-Based License Usage	47
Activate Volume-Based Licenses	48
Manage Volume-Based Licenses	48
Activate Volume-Based Licenses	50
Points to Note for GigaVUE Cloud Suite for Azure	51
Get Started with GigaVUE Cloud Suite for Azure	52
Prerequisites for GigaVUE Cloud Suite for Azure	52
Resource Group	52
Virtual Network	53
Subnets for VNet	53
Network Interfaces (NICs) for VMs	53
Network Security Groups	54
GigaVUE FM	54
UCT-V Controller	57
UCT-V	58
GigaVUE V Series Node	59
Giga VUE V Series Proxy(Optional)	60
UCT-C Controller - deployed in Kubernetes worker mode	61
UCT-V Controller	62
GigaVUE V Series Node	62
GigaVUE V Series Proxy(Optional)	62
Virtual Network Peering	63
Access control (IAM)	63

Default Login Credentials	63
GigaVUE-FM Version Compatibility	63
Recommended Instance Types	63
VPN Connectivity	64
Obtain GigaVUE-FM Image	64
GigaVUE Cloud Suite Cloud Suite in Azure Public Cloud	64
GigaVUE Cloud Suite Cloud Suite in Azure Government	64
Install and Upgrade GigaVUE-FM	64
Cloud	65
On-premise	65
Enable Subscription for GigaVUE Cloud Suite for Azure	65
Enable Subscription using CLI	66
Enable Subscription using Azure Portal	67
Install GigaVUE-FM on Azure	67
Install GigaVUE-FM Using Azure VM Dashboard	68
Install GigaVUE-FM Using Azure Marketplace	68
Permissions and Privileges (Azure)	70
Prerequisite	70
Managed Identity (recommended)	70
Application ID with client secret	72
Configure Role-Based Access for Third Party Orchestration	78
Role	78
Users	79
User Groups	79
Configure Tokens	80
Prerequisite	81
Rules and Notes	81
Create Token	82
Revoke Tokens	82
Export Token	83
Deployment Options for GigaVUE Cloud Suite for Azure ..	83
Deploy GigaVUE Fabric Components using Azure	84
Traffic Acquisition Method as UCT-V	84
Traffic Acquisition Method as vTAP	84
Deploy GigaVUE Fabric Components using GigaVUE-FM	85
Traffic Acquisition Method as UCT-V	85
Traffic Acquisition Method as vTAP	86
Traffic Acquisition Method as Customer Orchestrated Source	87
Deploy GigaVUE Cloud Suite for Azure	87
Create Azure Credentials	88
Install UCT-V	89
Supported Platforms	90

Supported Operating Systems for UCT-V	90
Linux UCT-V Installation	91
Windows UCT-V Installation	100
Create Images with the Agent Installed	106
Uninstall UCT-V	106
Upgrade UCT-V	107
Upgrade UCT-V through GigaVUE-FM (Recommended Method)	107
Upgrade UCT-V Manually	110
Integrate Private CA	110
Rules and Notes	110
Generate CSR	110
Upload CA Certificate	111
Adding Certificate Authority	111
Create Monitoring Domain	112
Check Permissions while Creating a Monitoring Domain	116
Manage Monitoring Domain	118
Configure GigaVUE Fabric Components in GigaVUE-FM	121
Configure UCT-V Controller	123
Configure GigaVUE V Series Proxy	126
Configure GigaVUE V Series Node	126
Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM	128
Configure GigaVUE Fabric Components in Azure - Integrated Mode	130
Overview of Third-Party Orchestration	130
Prerequisites	130
Disable GigaVUE-FM Orchestration in Monitoring Domain	132
Configure UCT-V Controller in Azure	133
Configure UCT-V in Azure	136
Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure	137
Configure Secure Communication between Fabric Components in FMHA	140
Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure	140
Prerequisite	141
Upgrade UCT-V Controller	141
Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy	142
Acquire Traffic using Inline V Series Solution	146
Create a Resource Group	147
Create Virtual Networks	147
Create a Virtual Network Peering	148
Create a Network Security Group	148
Create a Load Balancer	148
Create a Gateway Load Balancer	148
(Optional) Create a Standard Load Balancer	150

Install GigaVUE-FM on Azure	152
Enable System Assigned Managed Identity	154
Create Gigamon Custom Role	154
Assign Role to Resource Group	155
Assign Role to GigaVUE-FM Instance	156
Create a GigaVUE-FM Token	156
Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template	157
Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)	158
Assign VMSS to GWLB Backend Pools	161
Create Monitoring Domain	161
Deploy GigaVUE V Series Nodes for Inline V Series Solution	162
(Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)	163
Configure Monitoring session	165
Tier 1 Monitoring Session:	166
Deploy Monitoring Session (Tier 1)	167
Tier 2 Monitoring Session (Optional):	167
Deploy Monitoring Session Tier 1 to Tier 2	169
Configure Secure Tunnel (Azure)	169
Precrypted Traffic	169
Mirrored Traffic	170
Prerequisites	170
Notes	170
Configure Secure Tunnel from UCT-V to GigaVUE V Series Node	170
Configure Secure Tunnel between GigaVUE V Series Nodes	172
Viewing Status of Secure Tunnel	176
Create Prefiltering Policy Template	177
Create Precryption Template for UCT-V	178
Rules and Notes:	178
Create Precryption Template for Filtering based on Applications	179
Create Precryption Template for Filtering based on L3-L4 details	179
Configure Monitoring Session	183
Create a Monitoring Session (Azure)	183
Monitoring Session Page (Azure)	184
Configure Monitoring Session Options (Azure)	186
Create Ingress and Egress Tunnels (Azure)	191
Create Raw Endpoint (Azure)	199
Create a New Map (Azure)	200
Example- Create a New Map using Inclusion and Exclusion Maps	203
Map Library	204
Add Applications to Monitoring Session (Azure)	205
Interface Mapping (Azure)	205

Deploy Monitoring Session (Azure)	205
View Monitoring Session Statistics (Azure)	209
Visualize the Network Topology (Azure)	210
Configure Precryption in UCT-V	212
Rules and Notes	212
Validate Precryption connection	212
Limitations	213
Migrate Application Intelligence Session to Monitoring Session	213
Post Migration Notes for Application Intelligence	214
Monitor Cloud Health	216
Configuration Health Monitoring	216
Traffic Health Monitoring	217
Supported Resources and Metrics	218
Create Threshold Templates	220
Apply Threshold Template	221
Clear Thresholds	222
View Health Status	223
View Health Status of an Application	223
View Operational Health Status of an Application	223
View Health Status for Individual GigaVUE V Series Nodes	225
View Application Health Status for Individual V Series Nodes	226
Administer GigaVUE Cloud Suite for Azure	226
Configure Certificate Settings	226
Set Up Email Notifications	227
Configure Email Notifications	227
Configure Proxy Server	228
Configure Azure Settings	230
Role Based Access Control	232
About Events	233
About Audit Logs	235
Analytics for Virtual Resources	236
Virtual Inventory Statistics and Cloud Applications Dashboard	237
Analytics for Inline V Series Solution (Azure)	242
Debuggability and Troubleshooting	244
Sysdumps	245
Sysdumps—Rules and Notes	245
Generate a Sysdump File	245

FAQs - Secure Communication between GigaVUE Fabric Components (Azure)	246
Additional Sources of Information	250
Documentation	250
How to Download Software and Release Notes from My Gigamon	253
Documentation Feedback	253
Contact Technical Support	254
Contact Sales	255
Premium Support	255
The VUE Community	255
Glossary	256

GigaVUE Cloud Suite Deployment Guide – Azure

This guide describes how to install, configure and deploy the GigaVUE Cloud solution on the Microsoft® Azure cloud. Use this document for instructions on configuring the GigaVUE Cloud components and setting up the traffic monitoring sessions for the Azure Cloud.

Refer to the following sections for details:

- [Overview of GigaVUE Cloud Suite for Azure](#)
- [Introduction to the Supported Features on GigaVUE Cloud Suite for Azure](#)
- [Licensing for GigaVUE Cloud Suite for Azure](#)
- [Points to Note for GigaVUE Cloud Suite for Azure](#)
- [Get Started with GigaVUE Cloud Suite for Azure](#)
- [Deployment Options for GigaVUE Cloud Suite for Azure](#)
- [Deploy GigaVUE Cloud Suite for Azure](#)
- [Configure Secure Tunnel \(Azure\)](#)
- [Create Prefiltering Policy Template](#)
- [Create Precryption Template for UCT-V](#)
- [Configure Monitoring Session](#)
- [Configure Precryption in UCT-V](#)
- [Check for Required IAM Permissions in Azure](#)
- [Migrate Application Intelligence Session to Monitoring Session](#)
- [Monitor Cloud Health](#)
- [Administer GigaVUE Cloud Suite for Azure](#)

Overview of GigaVUE Cloud Suite for Azure

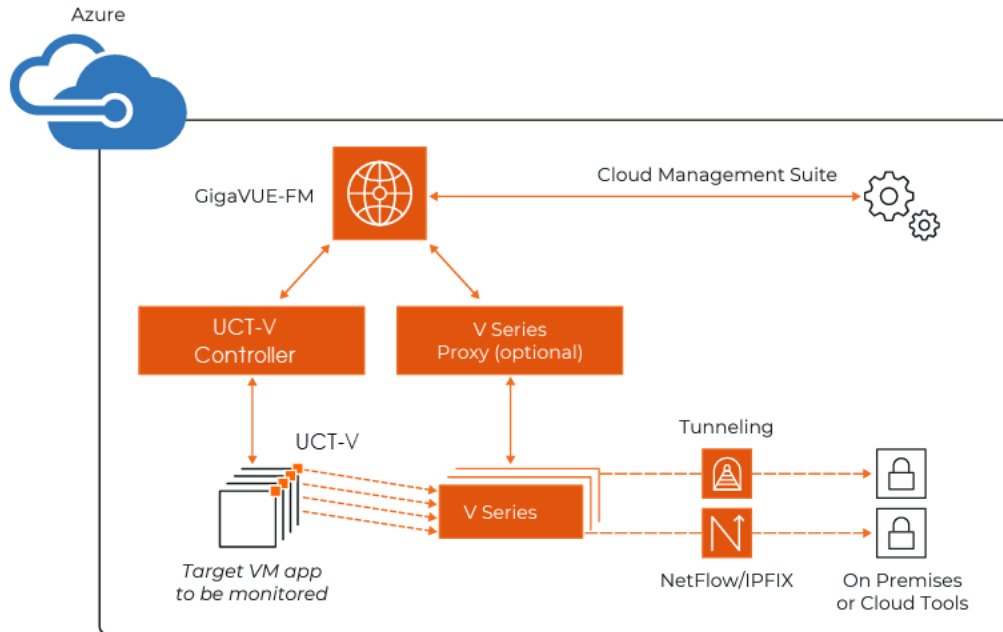
GigaVUE Cloud Suite for Azure gives you clear visibility into your workloads in Azure. It helps your security and monitoring tools find and respond to threats quickly using detailed, real-time network data.

This cloud-native solution runs entirely within your Azure Virtual Networks (VNets). It gathers traffic from all areas of your cloud environment—including Azure's native traffic mirroring. Then it processes that traffic to create useful metadata. This helps you monitor activity, spot issues early, and keep your cloud environment secure.

All parts of GigaVUE Cloud Suite for Azure live in the cloud. They collect traffic using UCT-V, small agent-like components installed on each Virtual Machine (VM). As your VMs change, Gigamon automatically adjusts to keep pace.

Benefits

- **Improves tool capacity:** Offloads security and monitoring work from your tools. This improves performance and reduces cost.
- **Fully automates the infrastructure:** Finds new or moved workloads on its own. It also launches visibility components and updates traffic rules without manual setup.
- **Simplifies operation:** Provides one dashboard for monitoring and control—across hybrid and cloud networks.
- **Helps accelerate cloud migrations:** Connects on-premises and cloud setups with a single visibility system. This makes migrations faster and easier.



GigaVUE-FM

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

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

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

For more information on installing GigaVUE-FM on Azure, see [Install GigaVUE-FM on Azure](#).

UCT-V

Universal Cloud Tap - Virtual Machine(**UCT-V**) (earlier known as G-vTAP Agent) is a standalone service that is installed in the VM instance. UCT-V mirrors the selected traffic from the instances (virtual machines) to the GigaVUE V Series Node. The UCT-V is offered

as a Debian (.deb), Redhat Package Manager (.rpm) package, ZIP and MSI .

Next generation UCT-V is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the UCT-V mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the UCT-V to GigaVUE V Series Node and in-turn reduces the load on the GigaVUE V Series Node. Next generation UCT-V gets activated on Windows and also on Linux systems with a Kernel version above 4.18.

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

Single Network Interface Configuration

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

Example

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

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

Sample Configuration

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

Grant permission to monitor ingress and egress traffic at iface

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

Multiple Network Interface Configuration

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

Example

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

In the UCT-V configuration, you can configure:

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

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

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

Grant permission to monitor ingress and egress traffic at iface

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

Loopback Network Interface Configuration

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

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

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

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

UCT-V Controller

UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series Nodes. GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A UCT-V Controller can only manage UCT-Vs that has the same version.

For example, the UCT-V Controller 6.14.00 can only manage UCT-Vs 6.14.00. If you have the previous version of UCT-V still deployed in the Virtual Network, you must configure both UCT-V Controller 6.14.00 and the previous version. While configuring the UCT-V Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the UCT-Vs to the GigaVUE V Series Nodes.

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to [Authentication Type](#).

GigaVUE V Series Node

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

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to [Authentication Type](#).

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

Monitoring Domain

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

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

Monitoring Session

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

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

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

Cloud Overview Page (Azure)

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

This page shows key information at a glance, including:

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

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

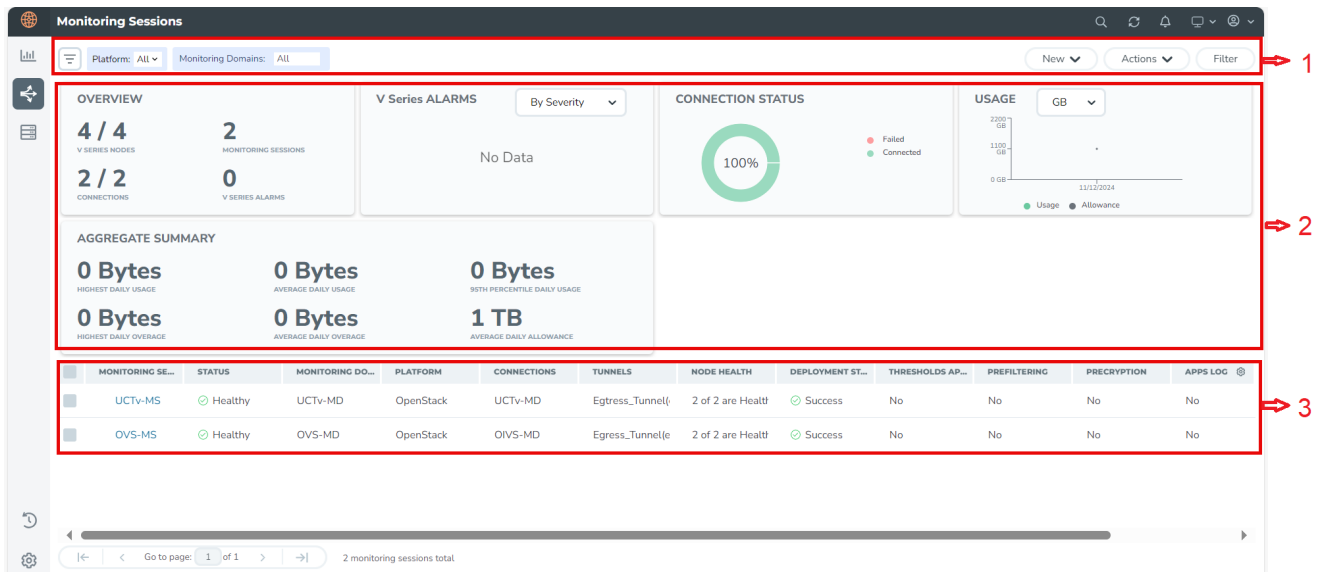
How to Access the Overview Page

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

Perform one of the following:

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

The **Monitoring Sessions** page appears.



Page Layout for Easy Use

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

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

Top Menu

The Top menu consists of the following options:

Options	Description
New	Allows to create a new Monitoring Session and new Monitoring Domain.
Actions	Allows the following actions: Edit: Opens the edit page for the selected Monitoring Session. Delete: Deletes the selected Monitoring Session. Clone: Duplicates the selected Monitoring Session. Deploy: Deploys the selected Monitoring Session. Undeploy: Undeploys the selected Monitoring Session. Apply Threshold: Applies the threshold template created for monitoring cloud traffic health. For details, refer to the <i>Monitor Cloud</i> section. Apply Policy: Enables functions like Precryption, Prefiltering, or Secure Tunnel.

Options	Description
Filter	You can filter the Monitoring Session details based on a criterion or a combination of criteria. For more information, refer to Cloud Overview Page (Azure) .

Filters

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

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

Filter on the left corner



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

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

Filter on the right corner



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

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

Viewing Charts on the Overview Page

You can view the following charts on the overview page:

- Overview
- V Series Alarms
- Connection Status

- Usage
- Aggregate Summary

Overview

This chart shows:

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

V Series Alarms

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

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

Connection Status

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

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

Usage

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

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

Aggregate Summary

This summary shows key volume usage stats:

- Highest daily volume usage
- Average daily volume usage
- Highest daily over-usage
- Average daily over-usage

- 95th percentile daily usage
- Average daily volume allowance

Viewing Monitoring Session Details

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

Details	Description
Monitoring Sessions	Displays the name of each session. Select a name to open the Monitoring Session's page in the selected cloud platform.
Status	Displays the Health status of the Monitoring Session.
Monitoring Domain	Displays the name of the Monitoring Domain to which the Monitoring Session is associated.
Platform	Indicates the Cloud platform in which the session is created.
Connections	Displays Connection details of the Monitoring Session.
Tunnels	Lists the Tunnel details related to the Monitoring Session.
Node Health	Displays the Health status of the GigaVUE V Series Node.
Deployment Status	Displays the status of the deployment.
Threshold Applied	Specifies if the threshold is applied.
Prefiltering	Specifies if Prefiltering is configured.
Precryption	Specifies if Precryption is configured.
APPS logging	Specifies if APPS logging is configured.
Traffic Mirroring	Specifies if Traffic Mirroring is configured.

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

Introduction to the Supported Features on GigaVUE Cloud Suite for Azure

GigaVUE Cloud Suite for Azure supports the following features:

- [Inline V Series \(Azure\)](#)
- [Secure Communication between GigaVUE Fabric Components](#)
- [Precryption™](#)

- [Secure Tunnels](#)
- [Prefiltering](#)
- [Monitor Cloud Health](#)
- [Analytics for Virtual Resources](#)
- [Customer Orchestrated Source - Use Case](#)

Inline V Series (Azure)

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

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

You can use this solution for forwarding inline traffic and traffic processing. When traffic reaches the Inline V Series Node, a copy of the packet is taken as out-of-band traffic. You can forward the copied traffic to a GigaVUE V Series Node for additional processing or directly to monitoring tools. During boot-up, the Inline V Series Node initializes with the default Inline application.

A Monitoring Session is required to:

- Tap the inline traffic
- Create a copy for out-of-band forwarding
- Send the traffic to the desired tools.

Inline V Series Deployment Types

Single Tier Deployment

You can use this deployment model when traffic has to be tapped, filtered, and directly sent to tools without any processing.

Multi-Tier Deployment

Use this model when you need to process traffic through GigaVUE V Series applications before forwarding it to the tools. The first tier taps the traffic, and the second tier processes it using the GigaVUE V Series applications and forwards it to the tools.

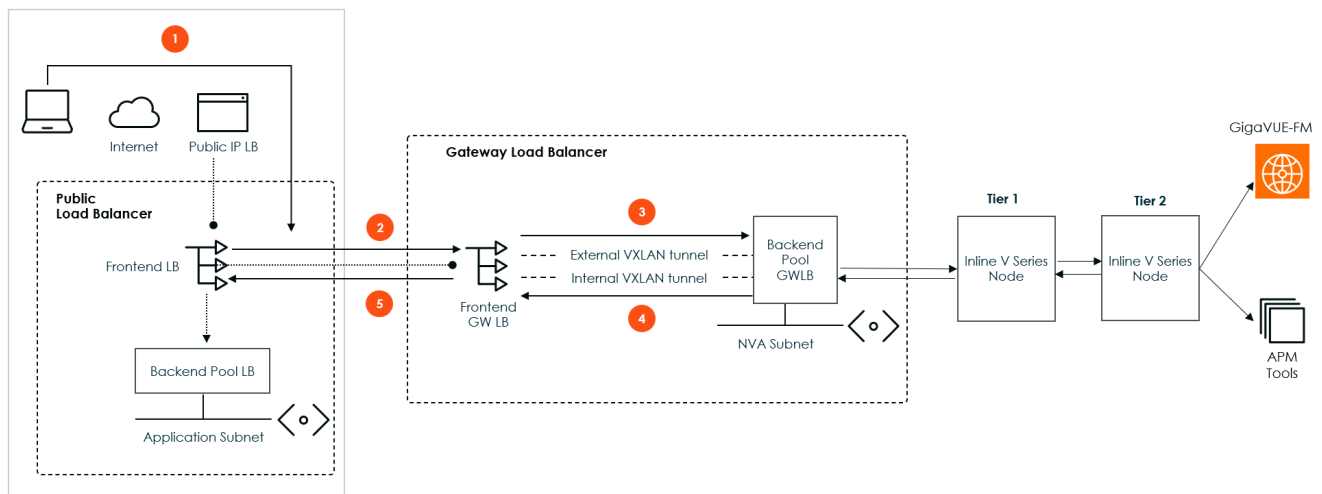
Architecture of Inline V Series Solution in Azure

Components required for configuring Inline V Series Solution in Azure:

- Application VNet
- Appliance VNet
- Public Load balancer
- Gateway Load balancer
- Inline V Series Node

Application VNet consists of multiple workload VMs, Public Load Balancer, Public IP Load Balancer, and Application Server in the Backend pool. The appliance VNet consists of Gateway Load Balancer, Inline V Series Node. Any traffic reaching the Gateway Load Balancer will be routed to the Inline V Series Node.

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



Traffic from the internet to the application server:

1. The traffic from the internet is sent to the Public Load Balancer configured in Application VNet using an Public IP LB configuration.
2. This traffic is routed the Gateway Load balancer.

3. The Gateway Load Balancer in the Appliance VNet forwards the traffic to the Inline V Series Nodes. The following actions are performed in the Inline V Series Node:
 - Once the traffic reaches the Inline V Series Nodes, a copy of the packet is taken as out of band traffic.
 - The Out of Band traffic is forwarded to the GigaVUE V Series Node for further processing or it can be forwarded to the tools.
 - The Inline V Series swaps the IP address and the Mac of the packets, where the source and destination are interchanged. As a result the Inline V Series Node becomes the source and Gateway Load Balancer becomes the destination.

NOTE: Packets sent from the Gateway Load Balancer will be VXLAN encapsulated and forwarded to the Inline V Series Nodes.

4. The inline traffic is sent back to the Gateway Load Balancer.
5. The Gateway Load Balancer forwards the inline traffic to the application servers in the Application VNet.

For a detailed workflow on acquiring traffic through the Inline V Series, refer to [Acquire Traffic using Inline V Series Solution](#) .

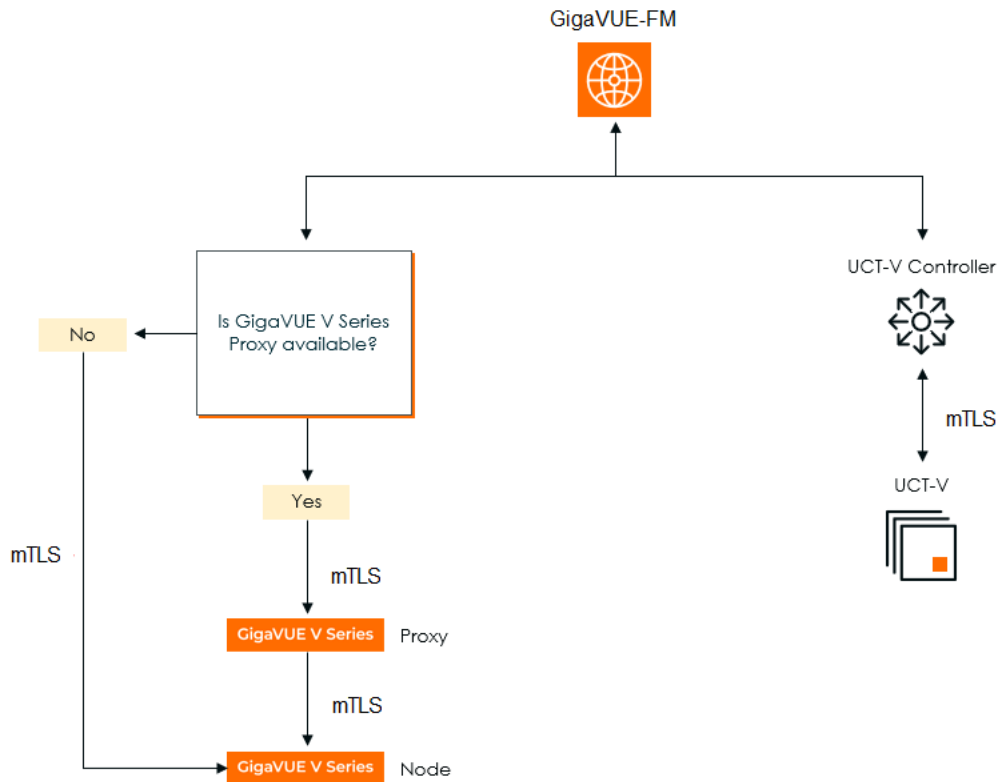
Limitation

This solution can be implemented only to tap the North-South traffic.

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

- 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.

Precryption™

License: Precryption 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:

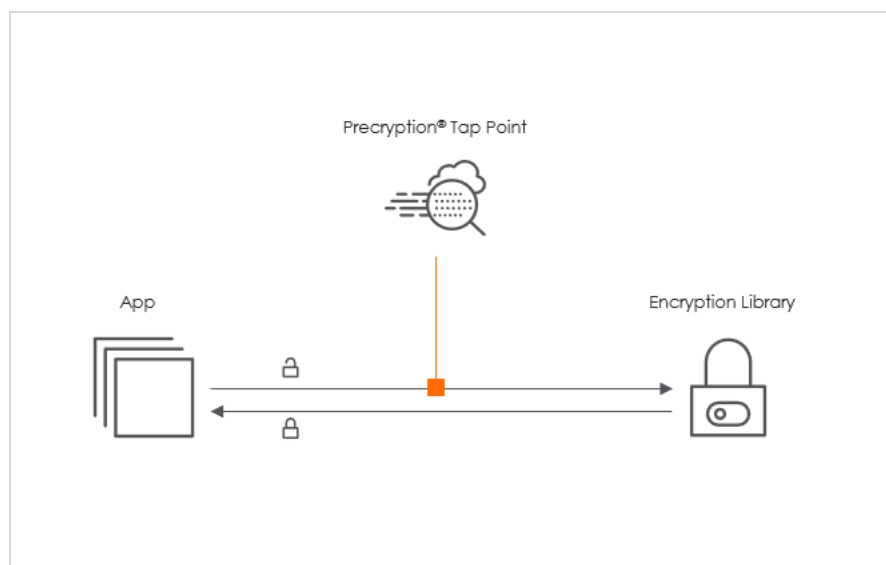
- [How Gigamon Precryption Technology Works](#)
- [Why Gigamon Precryption](#)

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.

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

How Gigamon Precryption Technology Works

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



Key Highlights

- 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.

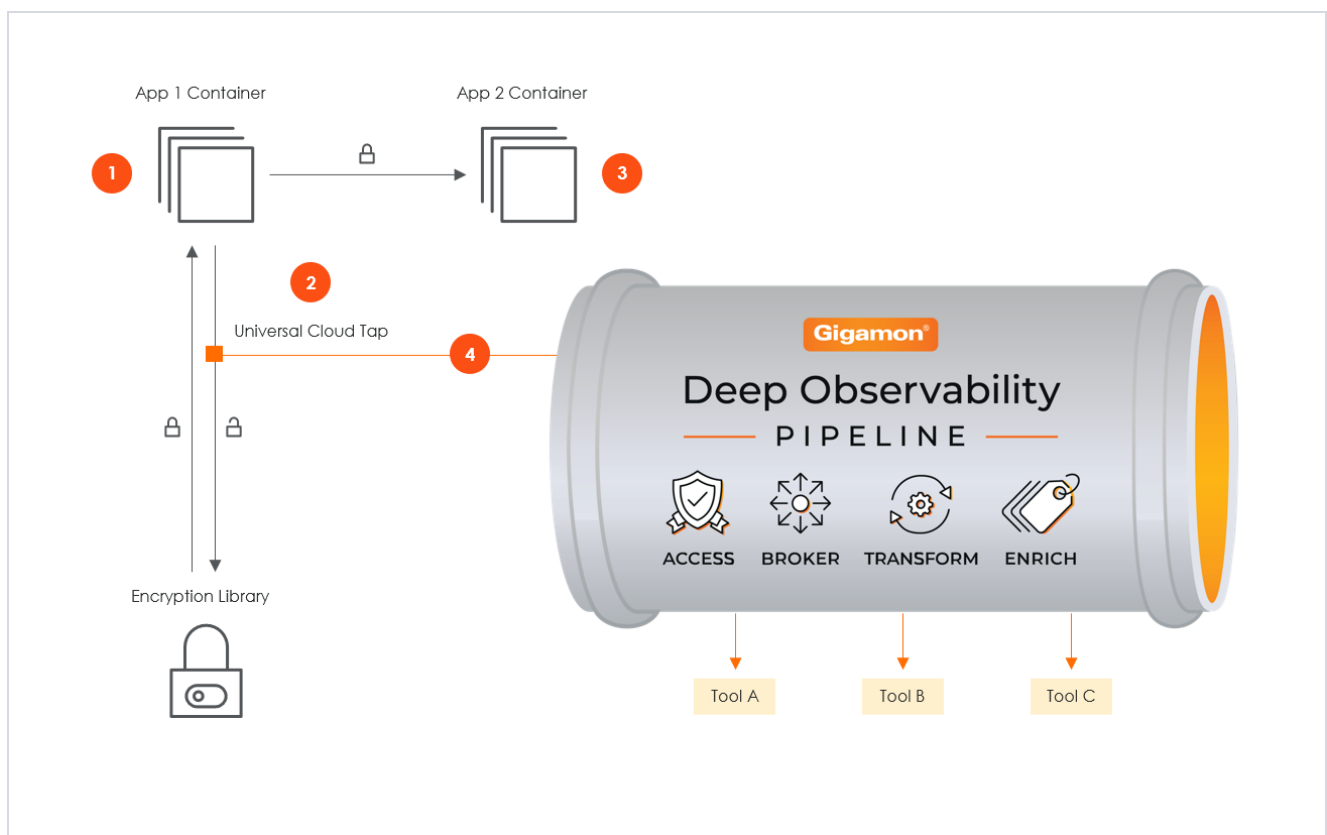
- Leverages a 5–7x performance boost for security tools by consuming unencrypted data.
- Supports a Zero Trust architecture founded on deep observability.
- Maintains privacy and compliance adherence associated with decrypted traffic management.

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](#)

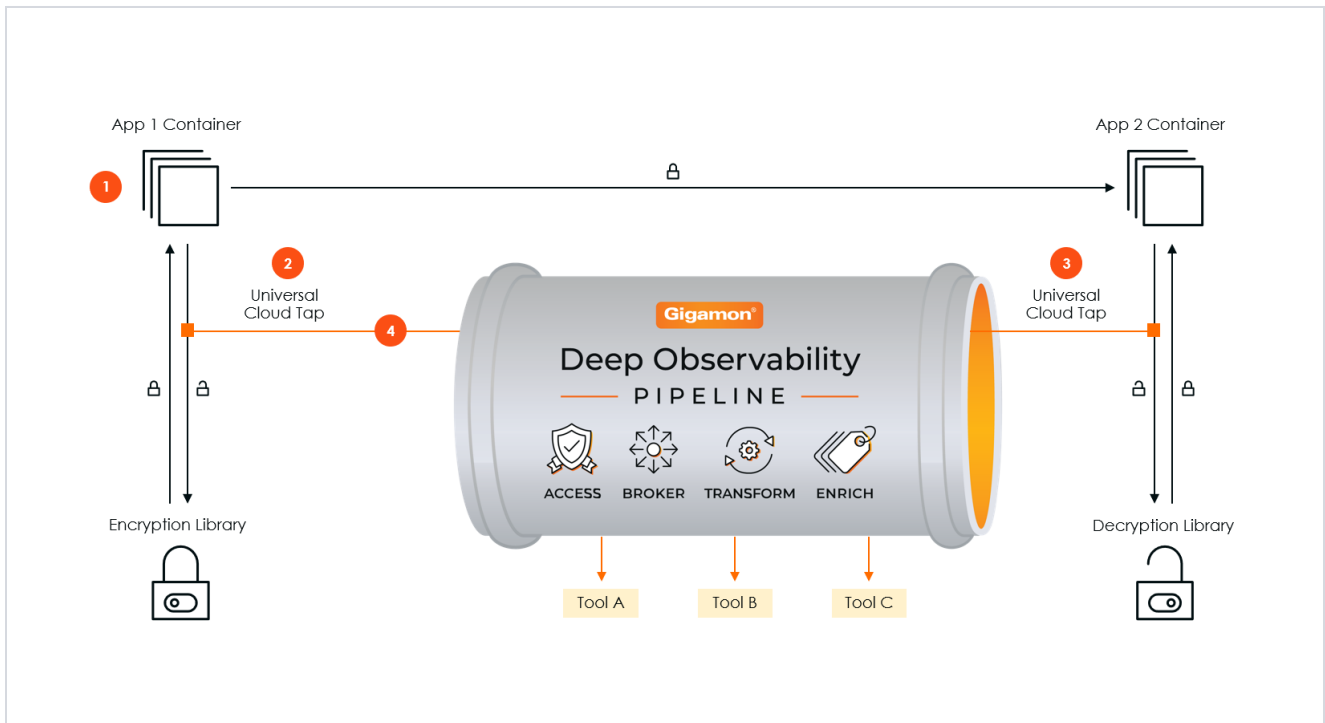
Precryption Technology on Single Node



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.

Precryption 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 Precryption technology, gets a copy of this message before it is encrypted on the network
3. Optionally, GigaVUE UCT enabled with Precryption can also acquire a copy of the message from the server end after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline.
5. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Supported Platforms

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

Platform Type	Platform
Public Cloud	• Azure • Azure • GCP (via Third Party Orchestration) • OCI (via Third Party Orchestration)
Private Cloud	• OpenStack • VMware ESXi (via Third Party Orchestration only) • VMware NSX-T (via Third Party Orchestration only) • Nutanix (via Third Party Orchestration only)

Container environments: Precryption™ is supported on the following container platforms 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 Tunnels

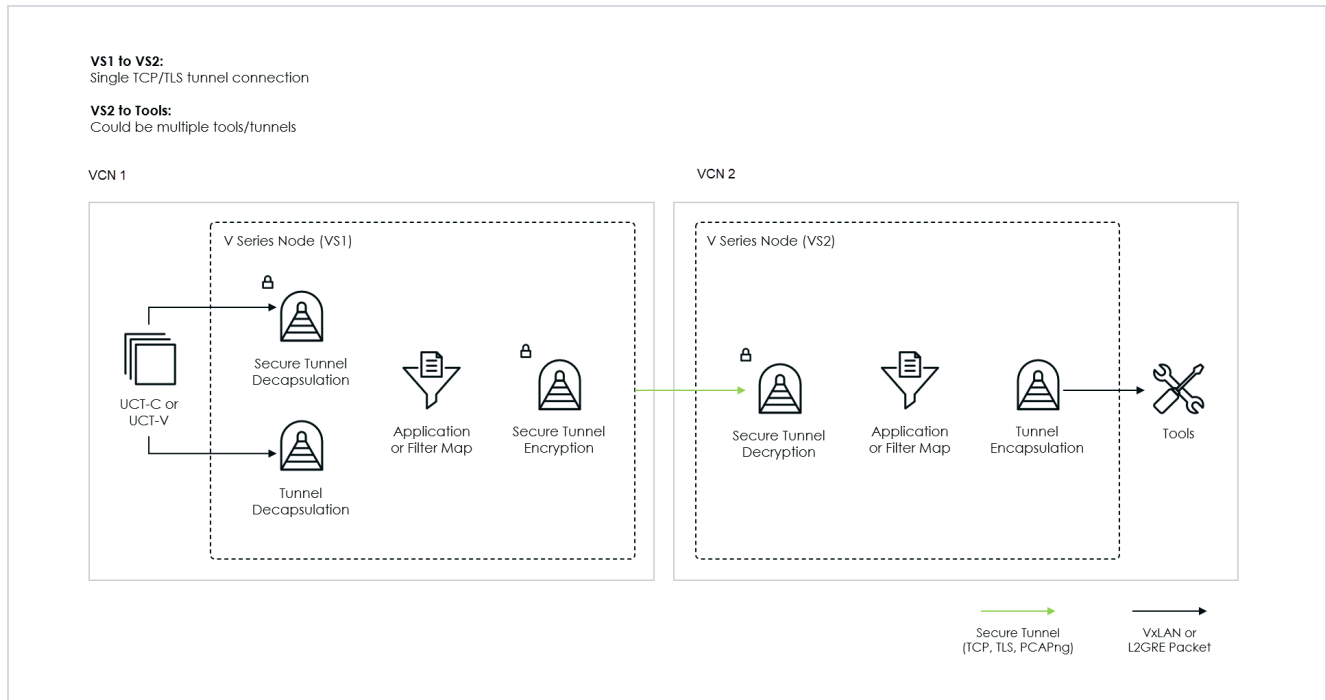
Secure Tunnel transfers the cloud captured packets from one GigaVUE V Series Node to another.

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

How Does it Work!

- 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](#).



Supported Platforms

Secure Tunnels are supported on:

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

For information about how to configure secure tunnels, refer to the section [Configure Secure Tunnel \(Azure\)](#).

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

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

For details, refer to [Create Prefiltering Policy Template](#)

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. For more information, see [Monitor Cloud Health](#).

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics¹, you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards.

You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. For details, refer to [Analytics](#).

Rules and Notes:

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

Virtual Inventory Statistics and Cloud Applications Dashboard

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

For details, refer to the [Analytics](#) section in *GigaVUE Fabric Management Guide* for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

How to access the dashboards

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

The following table lists the various virtual dashboards:

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

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

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

Dashboard	Displays	Visualizations	Displays
	- Platform - Connection - V Series Node	<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the de-duplicated packets received against the de-duplication application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated: • Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V Series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • V Series node: Management IP of the V Series node. Choose the required V Series node from the drop-down. • Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. The following statistics are displayed for the tunnel: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets	<i>Tunnel Bytes</i>	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	Visualizations	Displays
	- Received Dropped Packets - Transmitted Errored Packets - Transmitted Dropped Packets	<i>Tunnel Packets</i>	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node. You can select the following control filters, based on which the visualizations will get updated: Monitoring session V Series node Application: Select the required application. By default, the visualizations displayed includes all the applications. By default, the following statistics are displayed: - Received Bytes - Transmitted Bytes - Received Packets - Transmitted Packets - Errored Packets - Dropped Packets	<i>App Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

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

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

Customer Orchestrated Source - Use Case

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

When using Customer Orchestrated Source, you can directly configure tunnels or raw endpoints in the monitoring session, where you can use other applications like Slicing, Masking, Application Metadata, and Application Filtering, to process the tunneled traffic.

For details on how to configure Tunnels and Raw End Points in the Monitoring Session, refer to [Create Ingress and Egress Tunnels \(Azure\)](#) and [Create Raw Endpoint \(Azure\)](#).

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

Check for Required IAM Permissions in Azure

GigaVUE-FM allows you to validate whether the policy attached to the GigaVUE-FM using "Managed Identity" or "Application ID with client secret" has the required IAM permissions and notifies the users about the missing permissions. You can check permissions while creating a Monitoring Domain and deploying GigaVUE Fabric Components using GigaVUE-FM by clicking the **Check Permissions** button on the Create Monitoring Domain page and Azure Fabric Launch page. The GigaVUE-FM displays the minimum required IAM permissions.

IMPORTANT: "Microsoft.Authorization/roleAssignments/read" permission is required for validating the required permissions. Ensure to include "Microsoft.Authorization/roleAssignments/read" permission in your IAM policy.

Prerequisites to deploy GigaVUE Cloud Suite for Azure:

- IAM permissions: Check whether the minimum required permissions are granted for the instance where the GigaVUE-FM is deployed. For details, refer to [Permissions and Privileges \(Azure\)](#).
- Access to public cloud endpoints: Check for access to the Azure cloud endpoint APIs.
- Subscription to the GigaVUE Cloud Suite for Azure: Before deploying the solution, you must subscribe to the GigaVUE Cloud Suite components from the Azure marketplace. For details, refer to [Enable Subscription for GigaVUE Cloud Suite for Azure](#).
- Security Group: Checks whether the required ports are configured in the security group. For more information on the security groups, see [Network Security Groups](#)

After you press the **Check Permissions** button, GigaVUE-FM verifies the minimum required permissions. Any missing permissions are highlighted with the respective message against the permission in a dialog box. You can use the displayed IAM Policy JSON as a reference and update the policy that is attached to the GigaVUE-FM.

Points to Note

1. When using Managed Identity (MSI), the IAM policy modified in Azure Portal takes a long duration to reflect in GigaVUE-FM. For details, refer to the [Limitation of using managed identities for authorization](#) section in Azure Documentation.
2. The Check Permissions feature is not supported when the **Traffic Acquisition Method** is set to **vTAP**.

The following table lists the different available status and their descriptions.

Access Status	Description
Allowed	This status is displayed if permission is configured correctly.
Denied	This status is displayed if permission is missing. For Example: If a permission is not configured in the IAM policy or if the permission access is explicitly denied in Azure, then the status is displayed as Denied.
Failed	This status is displayed if GigaVUE-FM fails to validate a permission. The reason and the probable cause are also displayed.
Not Executed	This status is displayed if a higher level of permission is denied or not configured, then GigaVUE-FM cannot validate a permission. For Example: If a subscription level permission is in denied or failed state then the resource level permission cannot be validated.
Undeterminable	The "Microsoft.Authorization/roleAssignments/read" permission is required to validate the required permissions. If this permission is not configured, the status of several other permissions cannot be determined.

Refer to the following section for more detailed information:

- [Check Permissions while Creating a Monitoring Domain](#)
- [Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM](#)
- [View Permission Status Reports](#)

View Permission Status Reports

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

You can view the Permission Status Report in the following two ways:

- In the Monitoring Domain page, click **Actions > View Permission Status Report**.
- In the Monitoring Domain page, you can navigate to **Settings** and then click **Permission Status Report**

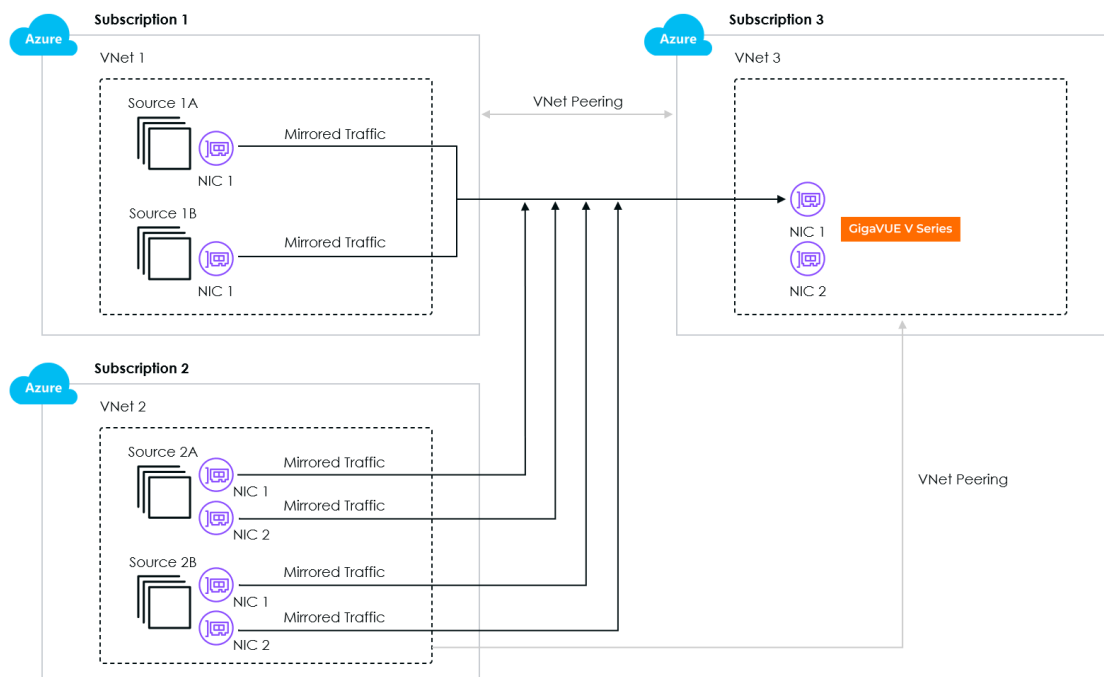
On the **Permission Status Report** page, you can use the Filter button to filter the reports based on File Name, Type, and Date.

To view or delete individual reports, select the report and click **Actions** button.

Traffic Acquisition using Azure Virtual Network TAP

NOTE: Microsoft Azure vTAPs are currently in Public Preview in select regions. Gigamon has fully tested our orchestration and automation against the current APIs to ensure compatibility. Refer to Microsoft's website: [Virtual network TAP](#) for the latest Azure vTAP release information and regional availability.

Azure Virtual Network TAP allows traffic mirroring directly from virtual machine network interfaces to designated target network interfaces. The mirrored traffic, a deep copy of inbound and outbound network packets, can be forwarded to a destination IP endpoint or an internal load balancer within the same or peered virtual networks. GigaVUE V Series Nodes receive traffic directly from source VMs using vTAP, simplifying traffic acquisition and visibility.



In the above diagram, the traffic from the source VMs are mirrored and forwarded to the GigaVUE V Series Node. GigaVUE-FM creates VTAP source configurations for each source VM NIC and a VTAP destination configuration for the GigaVUE V Series Node NIC. The source VMs and GigaVUE V Series Nodes can reside in different VNETs, provided the VNETs are peered. Multiple NICs can be configured for the same source VM and the traffic can be tapped and forwarded to GigaVUE V Series Node.

For more details on Azure virtual network TAP, refer to the [Virtual network TAP](#) Microsoft Azure documentation.

Rules and Notes

- Destination VM and Source VM must be in the same region.
- If workloads VMs are present in multiple resource groups or Virtual Network (VNet), then Virtual Network peering has to be enabled between workload VNets and VNet where the GigaVUE V Series Node is deployed.

DISCLAIMER: Keep in mind that these guidelines are inherent to Azure, subject to change, and beyond Gigamon's purview. Refer to the Azure documentation for the most up-to-date instructions.

Limitation

- IPv6 tunnels are not supported by Azure VTAP.
- The Check Permissions feature is not supported when the **Traffic Acquisition Method** is set to **VTAP**.

Licensing for GigaVUE Cloud Suite for Azure

You can license the GigaVUE Cloud Suite for Azure using the following method:

- [Volume Based License \(VBL\)](#)

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

For more detailed information on Volume-Based Licensing and instructions on how to generate and apply license, refer to the following topics:

- [Volume Based License \(VBL\)](#)
- [Activate Volume-Based Licenses](#)

- [Manage Volume-Based Licenses](#)

Default Trial Licenses

After installing GigaVUE-FM, you receive a one-time, free 1TB SecureVUE Plus trial Volume-Based License (VBL) for 60 days, starting from the installation date.

This license includes the following applications:

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

NOTE: If you do not have any other volume-based licenses installed, the deployed monitoring sessions are undeployed from the existing GigaVUE V Series Nodes after 60 days at the expiration of the trial license.

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

License Requirements for Monitoring Sessions

You must use one of the following GigaVUE Cloud Suite™ licenses to deploy any supported application in a Monitoring Session:

- CoreVUE Base Bundle (minimum required)
- NetVUE
- SecureVUE Plus

The default GigaVUE-FM licenses do not provide entitlement for deploying Monitoring Session applications.

The default trial VBL license (SecureVUE Plus) will support deploying applications in Monitoring Sessions only for the duration of the trial license.

Volume Based License (VBL)

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

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

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

Related Information

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

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUE Plus

The bundles are available as SKUs¹. The SKUs are named such that the number indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE indicates a daily volume allowance of 250 Terabytes (250T) for the CoreVUE bundle.

The features supported for base bundle licenses are given in the following table:

Feature	CoreVUE	NetVUE	SecureVUE Plus
Slicing	√	√	√
Masking	√	√	√
Advanced Load Balancing	√	√	√
Advanced Tunneling	√	√	√
Deduplication	-	√	√
NetFlow Generation	-	√	√
Adaptive Packet Filtering (APF)	-	-	√
Application Filtering Intelligence (AFI)	-	-	√
Application Metadata Intelligence (AMI)	-	-	√
Application Metadata Exporter (AMX)	-	-	√
Inline Decryption	-	-	√
OOB Decryption	-	-	√
Precryption	-	-	√
Gigamon Enriched Metadata	-	-	√

Bundle Replacement Policy

Refer to the following notes:

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

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

Add-on Packages

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

The following add-on SKUs are available:

- VBL-50T-ADD-5GC
- VBL-250T-ADD-5GC
- VBL-2500T-ADD-5GC
- VBL-25KT-ADD-5GC

Rules for add-on packages:

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

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

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

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only applications with active licenses.

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

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

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

Manage Volume-Based Licenses

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

View active Volume-Based License

To view active Volume-Based License (VBL):

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

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

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

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

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

View Inactive Volume-Based License

To view inactive Volume-Based License (VBL):

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

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

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

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

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

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

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

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

Points to Note for GigaVUE Cloud Suite for Azure

IMPORTANT: If you are using a Cloud Solution Provider (CSP) in Azure, we require your CSP tenant ID and company name to be included in our Azure publishing portal, contact Gigamon Sales.

- When tool is deployed outside Azure, ensure there is connectivity between GigaVUE V Series Node tool interface and the tool. You can create connectivity by configuring a Network Address Translation (NAT) gateway.
- When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. For details, refer to [Configuration Settings](#).
- Fragmentation in the network should be avoided from UCT-V to GigaVUE V Series Node and from GigaVUE V Series Node to tool by setting appropriate MTU for the interfaces as there is a chance of fragment packets getting reordered in the network before it is received in GigaVUE V Series Node and the tool. If the tool VM MTU is less than that of the GigaVUE V Series Node, then the GigaVUE V Series Node fragments the packets.

Get Started with GigaVUE Cloud Suite for Azure

This chapter describes how to plan and start the GigaVUE Cloud Suite for Azure deployment on the Microsoft® Azure cloud.

Refer to the following sections for details:

- [Prerequisites for GigaVUE Cloud Suite for Azure](#)
- [VPN Connectivity](#)
- [Obtain GigaVUE-FM Image](#)
- [Install and Upgrade GigaVUE-FM](#)
- [Enable Subscription for GigaVUE Cloud Suite for Azure](#)
- [Install GigaVUE-FM on Azure](#)
- [Permissions and Privileges \(Azure\)](#)
- [Configure Tokens](#)

Prerequisites for GigaVUE Cloud Suite for Azure

To enable the flow of traffic between the components and the monitoring tools, you must create the following requirements:

- [Resource Group](#)
- [Virtual Network](#)
- [Subnets for VNet](#)
- [Network Interfaces \(NICs\) for VMs](#)
- [Network Security Groups](#)
- [Virtual Network Peering](#)
- [Access control \(IAM\)](#)
- [Default Login Credentials](#)
- [GigaVUE-FM Version Compatibility](#)
- [Recommended Instance Types](#)

Resource Group

The resource group is a container that holds all the resources for a solution.

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

Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

You can only configure the GigaVUE fabric components in a Centralized VNet only. In case of a shared VNet, you must select a VNet as your Centralized VNet for GigaVUE fabric configuration.

To create a virtual network in Azure, refer to [Create a virtual network](#) topic in the Azure Documentation.

Subnets for VNet

The following table lists the two recommended subnets that your VNet must have to configure the GigaVUE Cloud Suite Cloud components in Azure.

You can add subnets when creating a VNet or add subnets on an existing VNet. For details, refer to [Add a subnet](#) topic in the Azure Documentation.

Subnet	Description
Management Subnet	Subnet that the GigaVUE-FM uses to communicate with the GigaVUE V Series Nodes and Proxy.
Data Subnet	A data subnet can accept incoming mirrored traffic from agents to the GigaVUE V Series Nodes or be used to egress traffic to a tool from the GigaVUE V Series Nodes. There can be multiple data subnets. ▪ Ingress is VXLAN from agents ▪ Egress is either VXLAN tunnel to tools or to GigaVUE HC Series tunnel port, or raw packets through a NAT when using NetFlow. Note: If you are using a single subnet, then the Management subnet will also be used as a Data Subnet.
Tool Subnet	A tool subnet can accept egress traffic to a tool from the GigaVUE V Series Nodes. There can be only one tool subnet. ▪ Egress is either VXLAN tunnel to tools or to GigaVUE HC Series tunnel port, or raw packets through a NAT when using NetFlow.

Network Interfaces (NICs) for VMs

When using UCT-V as the traffic acquisition method, for the UCT-Vs to mirror the traffic from the VMs, you must configure one or more Network Interfaces (NICs) on the VMs.

- **Single NIC**—If there is only one interface configured on the VM with the UCT-V, the UCT-V sends the mirrored traffic out using the same interface.
- **Multiple NICs**—If there are two or more interfaces configured on the VM with the UCT-V, the UCT-V monitors any number of interfaces but has an option to send the mirrored traffic out using any one of the interfaces or using a separate, non-monitored interface.

Network Security Groups

A network security group defines the virtual firewall rules for your VM to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE V Series Proxy, GigaVUE V Series Nodes, and UCT-V Controllers in your VNet, you add rules that control the inbound traffic to VMs, and a separate set of rules that control the outbound traffic.

To create a network security group and add in Azure, refer to [Create a network security group](#) topic in the Azure Documentation.

We recommend to create a separate security group for each component using the rules and port numbers.

In your Azure portal, select a network security group from the list. In the Settings section select the Inbound and Outbound security rules to the following rules.

Following are the 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 for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM using REST API.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.

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

UCT-V

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 (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.

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.

Virtual Network Peering

If workloads VMs are present in multiple resource groups or Virtual Network (VNet), then Virtual Network peering has to be enabled between workload VNets and VNet where the GigaVUE V Series Node is deployed. Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. Virtual Network Peering is only applicable when multiple Virtual Networks are used in a design. For details, refer to [Virtual Network Peering](#) topic in Azure documentation.

Access control (IAM)

You must have full resource access to the control the GigaVUE Cloud Suite cloud components. For details, refer to [Check access for a user](#) topic in the Azure documentation.

Default Login Credentials

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

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.
GigaVUE V Series proxy	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.
UCT-V Controller	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.14.00 supports the latest version (6.14.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, we recommend to use the latest version of fabric components with GigaVUE-FM.

Recommended Instance Types

NOTE: Additional instance types are supported. You can choose the instance type that best fits your deployment needs. If you're unsure which instance to select, contact Support, Sales, or Professional Services for deployment optimization.

Product	Instance Type	vCPU	RAM	Disk Size
GigaVUE V Series Node	Standard_D4s_v4	4 vCPU	16GB	10GB
	Standard_D8s_v4	8 vCPU	32GB	10GB
GigaVUE V Series Proxy	Standard_B1s	1 vCPU	1GB	
UCT-V Controller	Standard_B4ms	4 vCPU	16GB	4GB

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.

VPN Connectivity

GigaVUE-FM requires Internet access to integrate with the public API endpoints to integrate with the GigaVUE Cloud Suite Cloud platform. If there is no Internet access, refer to [Configure Proxy Server](#).

Obtain GigaVUE-FM Image

The image for the GigaVUE Cloud Suite Cloud is available in both the Azure Public Cloud and in the Azure Government portal.

GigaVUE Cloud Suite Cloud Suite in Azure Public Cloud

GigaVUE Cloud Suite Cloud is available in the Azure Marketplace with the Volume Based License options.

GigaVUE Cloud Suite Cloud Suite in Azure Government

Azure Government is an isolated Azure region that contains specific regulatory and compliance requirements of the US government agencies.

To monitor the VMs that contain all categories of Controlled Unclassified Information (CUI) data and sensitive government data in the Azure Government (US) Region, the Azure Government solution provides the same robust features in Azure Government as in the Azure public cloud.

Install and Upgrade GigaVUE-FM

You can install and upgrade the GigaVUE-FM fabric manager on cloud platforms or on-premises.

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

Cloud

- Azure - To install GigaVUE-FM inside your Azure environment, you can launch the GigaVUE-FM instance in your VNet.
 - Installation: Refer to [Install GigaVUE-FM on Azure](#).
 - Upgrade: Refer to Upgrade GigaVUE-FM in Azure topic in GigaVUE-FM Installation and Upgrade Guide.
- GigaVUE-FM can also be installed in any of the cloud platform. For details to install on in public, private or hybrid cloud platforms, refer to GigaVUE-FM Installation and Upgrade Guide.
 - Upgrade: For details, refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

On-premise

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

- Installation: Refer to GigaVUE-FM Installation and Upgrade Guide.
- Upgrade: Refer to Upgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

Enable Subscription for GigaVUE Cloud Suite for Azure

For GigaVUE-FM to be able to launch the fabric images,

- You must accept the terms of the end user license agreements (EULAs)
- Enable programmatic access in the Azure portal or through Azure Portal Cloud Shell.

For details, refer to the following topics:

- [Enable Subscription using CLI](#)
- [Enable Subscription using Azure Portal](#)

NOTE: For accepting EULA, you need to have Owner role on the Subscription.

Enable Subscription using CLI

1. **BYOL FM:** The following example shows how to accept EULA for BYOL FM using Azure Portal Cloud Shell

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite-
v2:gfm-azure-v6.14.xx:6.14.00
{
  "accepted": true,
  "id": "<Enter Subscription ID>",
  "licenseTextLink": "<Provide License text file link>",
  "marketplaceTermsLink": "<Provide Market Place Terms text file link>",
  "name": "gfm-azure",
  "plan": "gfm-azure",
  "privacyPolicyLink": "https://www.gigamon.com/privacy-policy.html",
  "product": "gigamon-gigavue-cloud-suite",
  "publisher": "gigamon-inc",
  "retrieveDatetime": "2023-05-02T20:09:36.1347592Z",
  "signature":
    "SZL3CYR5MMU5QC5FEBIDHLMOYE7DD4CBSMLOVRMCKAAUD5CKLG4RIWPALULYWCFWCENMFF7
    7RCXM4CM2B24WV3PGEFWW7UL4VMI3BVI",
  "systemData": {
    "createdAt": "2023-05-02T20:09:38.101210+00:00",
    "createdBy": "6447eb55-9d09-481b-89bc-52e96bb52823",
    "createdByType": "ManagedIdentity",
    "lastModifiedAt": "2023-05-02T20:09:38.101210+00:00",
    "lastModifiedBy": "6447eb55-9d09-481b-89bc-52e96bb52823",
    "lastModifiedByType": "ManagedIdentity"
  },
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

2. **Fabric Images (need to accept on all 3):** The following examples show how to accept EULA for different fabric components using Azure Portal Cloud Shell

For UCT-V Controller

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite-
v2:uctv-cntlr-v6.14.xx:6.14.00
{
  "accepted": true,
  .....
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

For GigaVUE V Series Node

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite-
v2:vseries-node-v6.14.xx:6.14.00
{
  "accepted": true,
  .....
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

For GigaVUE V Series Proxy

```
az vm image terms accept --urn gigamon-inc:gigamon-gigavue-cloud-suite-
v2:vseries-proxy-v6.14.xx:6.14.00
{
  "accepted": true,
  .....
  "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

Enable Subscription using Azure Portal

Enable the subscription for GigaVUE-FM and its fabric components like GigaVUE V Series Node, UCT-V Controller, and GigaVUE V Series Proxy.

Perform the following steps to accept the terms using Azure Portal:

1. Go to Market Place and search Gigamon.
2. From the search results, select **Gigamon GigaVUE Cloud Suite for Azure**.
3. From the **Plan** drop-down menu, select the required image.
4. Select the "**Want to deploy programmatically? Get started**" link.
5. Review the terms of service and the subscription name and then select **Enable**.

Install GigaVUE-FM on Azure

You can launch GigaVUE-FM from the Azure VM dashboard or Azure Marketplace.

Install GigaVUE-FM Using Azure VM Dashboard

To install,

1. Go to **Azure VM Dashboard > Virtual Machines** and select **Create** to create an Azure Virtual Machine.

For details, refer to [Create a Linux virtual machine in the Azure](#) in Azure Documentation.

2. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#).

Install GigaVUE-FM Using Azure Marketplace

You can install GigaVUE-FM using the Azure Marketplace.

To install,

1. Go to Azure Marketplace and search for Gigamon.

The latest version of Gigamon GigaVUE Cloud Suite for Azure appears.

2. Open the latest version of GigaVUE-FM.
3. Review and accept the terms for Gigamon GigaVUE Cloud Suite for Azure.

For details, refer to [Enable Subscription for GigaVUE Cloud Suite for Azure](#).

4. For details, refer to [Create a Linux virtual machine in the Azure](#) in Azure Documentation.
5. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#).

The following table describes the important fields.

Table 1: GigaVUE-FM Installation Steps

Field	Description
Basics	
Subscription	Select your subscription.
Resource Group	Select an existing resource group or create a new resource group. For more information, refer to Create a resource group topic in the Azure Documentation.
System-assigned managed identity	Use a system-assigned managed identity when a resource needs to authenticate to other services, and you want the identity to be created and deleted with the resource. Note: If you update any role it would take more than an hour to

Field	Description
	reflect in GigaVUE-FM, however, if you use APP registration it would take between 5-10 minutes to update in GigaVUE-FM.
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Availability Zone	Choose your availability zone
Security Type	To enable UEFI secure boot, select Trusted launch virtual machines from the drop-down list. Click Configure security features and ensure that the Enable secure boot check box is enabled.
Image	Select the latest GigaVUE-FM images. Note: You cannot select multiple images for a VM. Refer to Configure GigaVUE Fabric Components in Azure - Integrated Mode for more details on configuring GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in Azure.
Size	The recommended instance types are as follows: - GigaVUE-FM - Standard_D4s_v3 - UCT-V Controller - Standard_B4ms - V Series Node - Standard_D4s_v4 - V Series Proxy - Standard_Bms
Authentication Type	We support only SSH public key authentication type - SSH public key - Enter the administrator username for the VM. - Enter the SSH public key pair name. - Password - Enter the administrator username for the VM. - Enter the administrator password.
Disks	
Disk Size	The required disk size for GigaVUE-FM is 2 x 40GB .
Networking	
Virtual Network	Select an existing VNet or create a new VNet. For more information, refer to Create a virtual network topic in the Azure Documentation. On selecting an existing VNet, the Subnet and the Public IP values are auto-populated.
Configure network security group	Select an existing network security group or create a new network security group. For more information, refer to Network Security Groups . Configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components.

NOTE: Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in Azure, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

Permissions and Privileges (Azure)

When you first connect GigaVUE-FM to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for GigaVUE-FM to integrate with Azure APIs and to automate the fabric deployment and management.

IMPORTANT: "Microsoft.Authorization/roleAssignments/read" permission is required for validating the required permissions. Ensure to include "Microsoft.Authorization/roleAssignments/read" permission in your IAM policy.

Prerequisite

- Pre-defined custom roles or
- Create new custom roles that you can attach to the resource group or subscription level.

For details, refer to [Custom Roles](#) topic.

GigaVUE-FM supports two types of authentications with Azure. Refer to the following sections for more detailed information on how to enable each type of authentication for GigaVUE-FM and how to assign the above created custom roles for GigaVUE-FM:

- [Managed Identity \(recommended\)](#)
- [Application ID with client secret](#)

Managed Identity (recommended)

NOTE: The following information applies only to **System assigned managed identity**.

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.

Managed Identity (MSI) is only available when GigaVUE-FM is launched inside Azure. If GigaVUE-FM is launched in one VNet and the GigaVUE V Series Nodes are deployed in a different VNet, then Virtual Network Peering must be configured. For details, refer to [Virtual Network Peering](#).

IMPORTANT: When using Managed Identity (MSI), the IAM policy modified in Azure portal can take up to **1 hour** to propagate and appear in GigaVUE-FM. Refer to the [Limitation of using managed identities for authorization](#) section in Azure Documentation for more detailed information.

To work with MSI,

1. Enable MSI on the VM running in GigaVUE-FM. It can be done in using Azure portal or CLI.
 - Azure Portal: Refer to [Configure managed identities using the Azure portal](#) in the Azure documentation for detailed instructions.
 - Azure CLI:

- Enable system-assigned managed identity : **az vm identity assign -g <Resource group where GigaVUE-FM is deployed> -n <myVmName>**

For more information, refer to [Configure managed identities for Azure resources using Azure CLI](#) topic in the Azure Documentation.

2. Assign permissions to this VM on all the resources where you need GigaVUE-FM to manage.

After enabling MSI, you can assign custom roles to GigaVUE-FM at a resource group level or subscription level.



NOTE: Use a system-assigned managed identity in Azure when a single resource needs to authenticate to other services, and you want the identity's lifecycle tied to the resource's. This means the identity is created and deleted along with the resource.

Assign a Custom Role using CLI

1. Assign a custom role at resource group level where you will deploy the fabric:

```
az vm identity assign -g <Resource group where GigaVUE-FM is deployed>
--role <Custom Role> -n <GigaVUE-FM name> --scope <resource group id>
```

2. Assign a custom role at the subscription level to view the complete account details:

```
az vm identity assign -g <Resource group where GigaVUE-FM is deployed>
-role <Custom Role> -n <GigaVUE-FM name> --scope <subscription id>
```

If you want to update the Role, you can edit the JSON file, and then update the Role in Azure using the following CLI command:

```
az role definition update --role-definition <Custom Role>.json
```

You can run these commands in the Azure Portal in a cloud shell (icon in the upper right of the portal as seen here): .

Assign a Custom Role using Azure Portal

You can assign roles to GigaVUE-FM using Azure Portal for Resource Group Level or Subscription Level. For details, refer to [Assign Azure roles](#) topic in Azure Documentation.

Application ID with client secret

GigaVUE-FM supports application id with client secret authentication. When using GigaVUE-FM to connect to Azure, it uses a service principal. A service principal is an account for a non-human such as an application to connect to Azure. When GigaVUE-FM is launched outside Azure, Application ID with client secret is preferred.

To create a service principal in Azure, refer to the following topics in the Azure Documentation:

- [Create an Azure service principal with the Azure CLI](#)
- [Create an Azure service principal with Azure PowerShell](#)
- [Create an Azure service principal with Azure Portal](#)



GigaVUE-FM must be able to access the URLs listed in the [Allow the Azure portal URLs on your firewall or proxy server](#) in order to connect to Azure. Following are the required endpoints for Azure:

- login.microsoftonline.com
- management.azure.com
- login.microsoftonline.us (for Azure Gov cloud deployments)
- management.usgovcloudapi.net (for Azure Gov cloud deployments)

After creating service principal in Azure, you can add custom roles. For details, refer to [Assign a Custom Role using CLI](#) or [Assign a Custom Role using Azure Portal](#).

The key fields required for GigaVUE-FM to connect to Azure are Subscription ID, Tenant ID, Application ID, and Application Secret.

- When creating the service principal using the Azure CLI, the output of that command will display the "appId" and "password" fields. These two are the Application ID and Application Secret fields that are required for GigaVUE-FM to connect to Azure. Copy them.
- Now, using the Azure CLI again, do an 'account show' command and copy the Subscription ID and the Tenant ID of your subscription.

The Subscription ID, Tenant ID, Application ID, and Application Secret will be used when creating credentials in GigaVUE-FM. For instructions, refer to [Create Azure Credentials](#).

Custom Roles

The 'built-in' roles provided by Microsoft are open to all resources. You can create a custom role if required. For more information, refer to [Azure custom roles](#) topic in the Azure Documentation.

You can use the following command to create custom roles in CLI:

```
az role definition create --role-definition {roleDefinition}
```

{roleDefinition} - You can provide the input either as a JSON object or by specifying the path to a JSON file (e.g., ~/roles/vmoperator.json).

The following examples provides the minimum permissions that are required for GigaVUE-FM to deploy the fabric components and/or inventory the UCT-V. The permissions can be applied at the resource group level or subscription level.

You can use the following snippet in the example JSON file mentioned below to assign your custom role at either resource group level or subscription level.

For Subscription level: Assigning roles at the subscription level grants access to all resource groups and resources within that subscription.

```
"assignableScopes": [  
  "/subscriptions/<Subscription ID>/"  
],
```

For Resource group level: Assigning roles at the resource group level provides granular control. You can limit access to specific sets of resources by assigning roles only to selected resource groups.

```
"assignableScopes": [  
  "/subscriptions/<Subscription ID>/resourceGroups/<resourceGroup name>"  
],
```

Example 1: Create Custom Role for GigaVUE-FM to deploy visibility fabric components and inventory UCT-V

```
{
  "Name": "CustomRoleFabricDeploymentAndInventory",
  "description": "The minimum requirements for FM to deploy Fabric Components and inventory UCT-V",
  "assignableScopes": [
    "/subscriptions/<Subscription ID>"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/start/action",
        "Microsoft.Compute/virtualMachines/powerOff/action",
        "Microsoft.Compute/virtualMachines/restart/action",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/locations/vmSizes/read",
        "Microsoft.Compute/images/read",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/disks/delete",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Resources/subscriptions/locations/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Resources/subscriptions/resourcegroups/resources/read"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ]
}
```

Example 2: Create Custom Role for GigaVUE-FM to only inventory UCT-V

```
{
```

```
"Name":"CustomRoleInventoryUCT-V",
"description":" Minimum requirements for FM to inventory UCT-V ",
"assignableScopes":[
  "/subscriptions/<Subscription ID>"
],
"permissions":[
  {
    "actions":[
      "Microsoft.Compute/virtualMachines/read",
      "Microsoft.Compute/virtualMachines/instanceView/read",
      "Microsoft.Compute/images/read",
      "Microsoft.Compute/disks/read",
      "Microsoft.Network/networkInterfaces/read",
      "Microsoft.Network/virtualNetworks/subnets/read",
      "Microsoft.Network/publicIPAddresses/read",
      "Microsoft.Network/virtualNetworks/read",
      "Microsoft.Network/virtualNetworks/virtualMachines/read",
      "Microsoft.Network/networkSecurityGroups/read",
      "Microsoft.Network/publicIPAddresses/read",
      "Microsoft.Resources/subscriptions/locations/read",
      "Microsoft.Resources/subscriptions/resourceGroups/read",
      "Microsoft.Resources/subscriptions/resourcegroups/resources/read"
    ],
    "notActions":[],
    "dataActions":[],
    "notDataActions":[]
  }
]
}
```

Example 3: Create Custom Role for GigaVUE-FM to deploy visibility fabric components, inventory VMs and configure vTAPs in Azure

```
{
  "Name":"CustomRolevTAP",
  "description":"Minimum requirements for GigaVUE-FM to deploy visibility fabric components,
inventory VMs and configure vTAPs in Azure",
  "assignableScopes":[
    "/subscriptions/<Subscription ID>"
  ],
  "permissions":[
    {
      "actions":[
        "Microsoft.Network/virtualNetworkTaps/read",
        "Microsoft.Network/virtualNetworkTaps/delete",
        "Microsoft.Network/virtualNetworkTaps/write",
        "Microsoft.Network/virtualNetworkTaps/join/action",
        "Microsoft.Network/networkInterfaces/tapConfigurations/read",
        "Microsoft.Network/networkInterfaces/tapConfigurations/write",
        "Microsoft.Network/networkInterfaces/tapConfigurations/delete",
        "Microsoft.Network/networkInterfaces/ipconfigurations/join/action",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/start/action",
        "Microsoft.Compute/virtualMachines/powerOff/action",

```

```

        "Microsoft.Compute/virtualMachines/restart/action",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/locations/vmSizes/read",
        "Microsoft.Compute/images/read",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/disks/delete",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Resources/subscriptions/locations/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Resources/subscriptions/resourcegroups/resources/read"
    ],
    "notActions":[],
    "dataActions":[],
    "notDataActions":[]
  }
]
}

```

Example 4: Create Custom Role for GigaVUE-FM to only inventory VMs and configure vTAPs in Azure

```

{
  "Name":"CustomRoleInventoryvTAP",
  "description":"Minimum requirements for GigaVUE-FM to only inventory VMs and configure vTAPs in Azure",
  "assignableScopes":[
    "/subscriptions/<Subscription ID>"
  ],
  "permissions":[
    {
      "actions":[
        "Microsoft.Network/virtualNetworkTaps/read",
        "Microsoft.Network/virtualNetworkTaps/delete",
        "Microsoft.Network/virtualNetworkTaps/write",
        "Microsoft.Network/virtualNetworkTaps/join/action",
        "Microsoft.Network/networkInterfaces/tapConfigurations/read",
        "Microsoft.Network/networkInterfaces/tapConfigurations/write",
        "Microsoft.Network/networkInterfaces/tapConfigurations/delete",

```

```
        "Microsoft.Network/networkInterfaces/ipconfigurations/join/action",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/images/read",
        "Microsoft.Compute/disks/read",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/virtualNetworks/subnets/read",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Resources/subscriptions/locations/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Resources/subscriptions/resourcegroups/resources/read"
    ],
    "notActions":[],
    "dataActions":[],
    "notDataActions":[]
  }
}
}
```

Example 5: Create Custom Role for GigaVUE-FM to configure Inline V Series in Azure

```
{
  "Name":"CustomRoleForInline",
  "description":"Minimum requirements for FM in inline tapping",
  "assignableScopes":[
    "/subscriptions/<Subscription ID>"
  ],
  "permissions":[
    {
      "actions":[
        "Microsoft.Resources/subscriptions/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/backendPoolAddresses/read",
        "Microsoft.Compute/virtualMachineScaleSets/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigurations/read",
        "Microsoft.Compute/virtualMachines/read"
      ],
      "notActions":[],
      "dataActions":[],
      "notDataActions":[]
    }
  ]
}
```

NOTE: Add the `Microsoft.Compute/sshPublicKeys/read` permission only when you want GigaVUE-FM to pull SSH keys from Azure. This permission is optional and not required for all deployments.

To add a role assignment, refer to [Steps to assign an Azure role](#).

DISCLAIMER: These are general guidelines for enabling a deployment in Azure. Since the Azure interface is subject to change and is outside Gigamon's purview, please see Azure documentation for instructions on using Azure.

Configure Role-Based Access for Third Party Orchestration

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

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

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

Role

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

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

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.

Users

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:

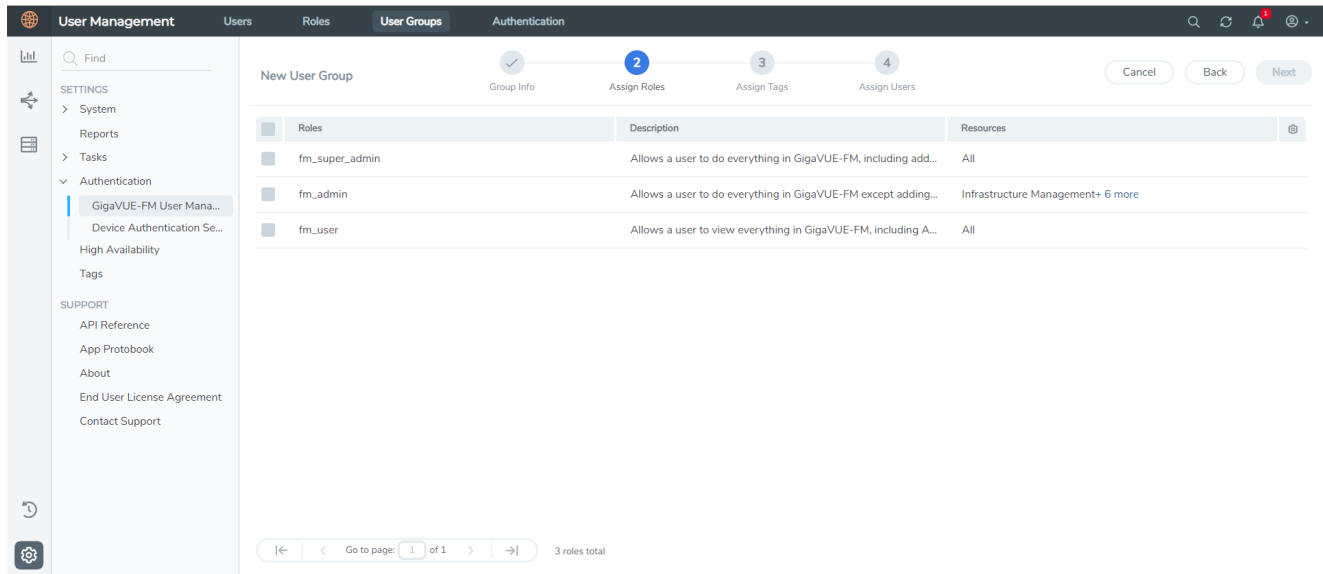
1. Go to **Settings** and select **Authentication > GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
 - **Name:** Actual name of the user
 - **Username:** User name configured in GigaVUE-FM
 - **Email:** Email ID of 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.

User Groups

A user group consists of a set of roles and set of tags associated with users in that group. You can associate a new user 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 Wizard, perform the following steps.
 - a. Select **Next** to progress forward and **Back** to navigate backward.
 - b. In the **Group Info** tab, enter the following details:
 - **Group Name**
 - **Description**
 - c. In the **Assign Roles** tab, select the role that you want to assign to the user group.
 - d. In the **Assign Tags** tab, select the required tag key and tag value.
 - e. In the **Assign Users** tab, select the required users.
 - f. Select **Apply** to save the configuration.

NOTE: Select **Skip and Apply** to skip this step and proceed without adding users.

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

Select the ellipses to perform the following operations:

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

Configure Tokens

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

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

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

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

Prerequisite

You must create user groups in GigaVUE-FM. For details, refer to

Rules and Notes

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

This section explains about the following:

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

- [Export Token](#)
- [Configure Tokens](#)

Create Token

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

To create a token, follow these steps:

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

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

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

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

Copy and Paste a Token

1. Select the token that you want to copy.
2. Select **Actions>Copy Token**.

The token is copied.

3. Paste the copied token in the required areas.

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

Revoke Tokens

You can revoke tokens that other users create.

Prerequisite: Write access in GigaVUE-FM Security Management.

To revoke tokens,

1. Go to , select **Authentication > GigaVUE-FM User Management**.
2. In the **User Management** page, select **Tokens**.
3. From the drop-down, select **Token Management**. You can view the created tokens.
4. Select the token that you want to revoke.
5. Select **Action> Revoke**.

Export Token

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

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

Deployment Options for GigaVUE Cloud Suite for Azure

This section provides detailed information on the multiple ways in which you can configure GigaVUE Cloud Suite for Azure to provide visibility for physical and virtual traffic. Using three different options, you can configure GigaVUE Cloud Suite for Azure based on the traffic acquisition method and the method in which you want to deploy fabric components. For details, refer to the [Prerequisites for GigaVUE Cloud Suite for Azure](#).

For more detailed information and the work flow, refer to the following topics:

- [Deploy GigaVUE Fabric Components using Azure](#)
 - [Traffic Acquisition Method as UCT-V](#)
 - [Traffic Acquisition Method as vTAP](#)
- [Deploy GigaVUE Fabric Components using GigaVUE-FM](#)
 - [Traffic Acquisition Method as UCT-V](#)
 - [Traffic Acquisition Method as vTAP](#)
 - [Traffic Acquisition Method as Customer Orchestrated Source](#)

Deploy GigaVUE Fabric Components using Azure

You can deploy GigaVUE fabric components using Azure with one of the following two traffic acquisition methods:

Traffic Acquisition Method as UCT-V

Refer the following table for the step-by-step instructions:

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure
3	Check and provide permissions and privileges	Permissions and Privileges (Azure)
4	Install UCT-V	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
5	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials
6	Create a Monitoring Domain Note: - Ensure that the Use FM to Launch Fabric toggle button is disabled. - Select UCT-V as the Traffic Acquisition Method.	Create Monitoring Domain
7	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in Azure - Integrated Mode
8	Create Monitoring session	Configure Monitoring Session
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (Azure)
10	Deploy Monitoring Session	Deploy Monitoring Session (Azure)
11	View Monitoring Session Statistics	View Monitoring Session Statistics (Azure)

Traffic Acquisition Method as vTAP

Perform the following steps to use vTAP as your traffic acquisition method.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure

Step No	Task	Refer the following topics
3	Check and provide permissions and privileges	Permissions and Privileges (Azure)
4	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials
5	Create a Monitoring Domain Note: - Ensure that the Use FM to Launch Fabric toggle button is disabled. - Select vTAP as the Traffic Acquisition Method.	Create Monitoring Domain
6	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in Azure - Integrated Mode
7	Create Monitoring session	Create a Monitoring Session (Azure)
8	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (Azure)
9	Deploy Monitoring Session	Deploy Monitoring Session (Azure)
10	View Monitoring Session Statistics	View Monitoring Session Statistics (Azure)

Deploy GigaVUE Fabric Components using GigaVUE-FM

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

Traffic Acquisition Method as UCT-V

Follow instruction in the below table, if you wish to use UCT-V as your traffic acquisition method. When using UCT-V the traffic from the Virtual Machines are acquired using the UCT-V and it is sent to the GigaVUE V Series Nodes.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure
3	Check and provide permissions and privileges	Permissions and Privileges (Azure)
4	Install UCT-V	For Linux: Linux UCT-V Installation For Windows: Windows UCT-V Installation
5	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials

Step No	Task	Refer the following topics
6	Create a Monitoring Domain Note: - Ensure that the Use FM to Launch Fabric toggle button is enabled. - Select UCT-V as the Traffic Acquisition Method.	Create Monitoring Domain
7	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in Azure - Integrated Mode
8	Create Monitoring session	Configure Monitoring Session
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (Azure)
10	Deploy Monitoring Session	Deploy Monitoring Session (Azure)
11	View Monitoring Session Statistics	View Monitoring Session Statistics (Azure)

Traffic Acquisition Method as vTAP

Perform the following steps to use vTAP as your traffic acquisition method.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure
3	Check and provide permissions and privileges	Permissions and Privileges (Azure)
4	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials
5	Create a Monitoring Domain Note: - Ensure that the Use FM to Launch Fabric toggle button is enabled. - Select vTAP as the Traffic Acquisition Method.	Create Monitoring Domain
6	Configure GigaVUE Fabric Components	Configure GigaVUE Fabric Components in GigaVUE-FM
7	Create Monitoring session	Create a Monitoring Session (Azure)
8	Add Applications to the Monitoring Session	Add Applications to Monitoring Session (Azure)
9	Deploy Monitoring Session	Deploy Monitoring Session (Azure)
10	View Monitoring Session Statistics	View Monitoring Session Statistics (Azure)

Traffic Acquisition Method as Customer Orchestrated Source

Follow instruction in the below table if you wish to use Customer Orchestrated Source as your traffic acquisition method. In this case you can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying UCT-V or UCT-V controllers.

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

Deploy GigaVUE Cloud Suite for Azure

This chapter describes how to connect, launch, and deploy the fabric components of GigaVUE Cloud Suite for Azure.

Refer to the following topics for details:

- [Create Azure Credentials](#)
- [Install UCT-V](#)
- [Integrate Private CA](#)
- [Configure a Gateway Load Balancer in Azure for Inline V Series Solution](#)

- [Adding Certificate Authority](#)
- [Create Monitoring Domain](#)
- [Configure GigaVUE Fabric Components in GigaVUE-FM](#)
- [Disable GigaVUE-FM Orchestration in Monitoring Domain](#)
- [Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure](#)

For details, refer to [Deploying GigaVUE Cloud Suite for Azure using V Series with Hybrid architecture](#).

Create Azure Credentials

You can monitor workloads across multiple Azure subscriptions within one monitoring domain. All the deployed GigaVUE fabric components are shared among many Azure subscriptions to reduce the cost. Earlier, each Azure subscription carried a set of GigaVUE fabric components.

- After launching GigaVUE-FM in Azure, the **Managed Identity** authentication credential is automatically added to the Azure Credential page as the default credential.
- You can only add the **Application ID with Client Secret** authentication credentials to the Azure Credential page.

To create Azure credentials,

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Credential**.
3. In the Azure Credential page, select **Add**.

The **Configure Credential** wizard appears.

The screenshot shows the 'Configure Credential' wizard interface. It includes a sidebar with navigation icons and a main form area. The form fields are as follows:

Field Label	Value / Selection
Name*	Credential Name
Authentication Type	Application ID with Client Secret
Tenant ID*	Tenant ID
Application ID*	Application ID
Application Secret*	Application Secret
Azure Environment	Azure Environment... (Dropdown menu open showing 'Azure' and 'AZURE_US_GOVERNMENT')

4. Enter or select the appropriate information for the Azure credential:

a. **Name:** An alias used to identify the Azure credential.

b. **Authentication Type:**

Application ID with Client Secret: Connection with Azure with a service principal. Enter the values for the following fields.

- **Tenant ID:** A unique identifier of the Azure Active Directory instance.
- **Application ID:** A unique identifier of an application in Azure platform.
- **Application Secret:** a password or key to request tokens.

For details on how to create service principal and assign custom roles, refer to [Application ID with client secret](#)

c. **Azure Environment:** Select an Azure environment where your workloads are located. For example, Azure_US_Government.

5. Select **Save**.

You can view the list of available credentials in the Azure Credential page.

Install UCT-V

UCT-V is the primary Gigamon monitoring module that you install on your Virtual Machines (VMs). UCT-V mirrors the selected traffic from a source interface to a destination mirror interface. UCT-V encapsulates the mirrored traffic using GRE or VXLAN tunneling and then forwards to the GigaVUE V Series Node.

NOTE: Install UCT-V only when the UCT-V is your traffic acquisition method.

The Workflow

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

You can configure a source interface with one or more Network Interfaces. While configuring a source interface, specify the traffic direction to monitor: ingress, egress, or both.

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

Supported Platforms

UCT-V is compatible with the following platforms when used with GigaVUE-FM:

- AWS
- Azure
- OpenStack

UCT-V is compatible with the following platforms when used with Third Party Orchestration:

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

Refer to the following sections for more information:

- [Supported Operating Systems for UCT-V](#)
- [Linux UCT-V Installation](#)
- [Windows UCT-V Installation](#)
- [Create Images with the Agent Installed](#)

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V¹ is 6.5.00, 6.6.00, 6.7.00, 6.8.00, 6.9.00, 6.10.00, 6.11.00, 6.12.00, 6.13.00, 6.13.00

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

Operating System	Supported Versions
Ubuntu/Debian	Versions 16.04 through 22.04
CentOS	Versions 7.5 through 9.0

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

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

GigaVUE-FM version 6.14 supports UCT-V version 6.14 as well as (n-2) versions. We recommend to use the latest version of UCT-V with GigaVUE-FM for better compatibility.

Linux UCT-V Installation

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

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

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

Refer to the following sections:

- [Linux Network Firewall Requirements](#)
- [Install Linux UCT-Vs](#)
- [Register Linux UCT-V](#)

Prerequisites

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

Linux Network Firewall Requirements

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

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

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

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

Install Linux UCT-Vs

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

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

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

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

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

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

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

- a. Download the UCT-V **6.14.00** Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
- b. Copy this package to your instance and Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

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

- a. Download the UCT-V6.14.00 RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
- b. Copy this package to your instance and install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
```

```
$ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
```

- Use the command given below to perform pre-check, installation, and configuration functionalities.

sudo uctv-wizard

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

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

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

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

**Notes:**

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

Linux UCT-V Installation Scenarios

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

Install Linux UCT-Vs using Manual Configuration

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

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

- Download the UCT-V**6.14.00** Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
- Copy this package to your instance.

3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

4. Modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Save the file.

6. Restart the UCT-V service.

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

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

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

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

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

1. Download the UCT-V6.14.00 RPM (.rpm) package from the [Gigamon Customer Portal](#).
For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
```

```
$ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
```

4. Modify the **/etc/uctv/uctv.conf** file to configure and register the source and destination interfaces.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
$ sudo service uctv restart
```

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

```
$ sudo service uctv status
```



Notes:

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

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

Post Deployment Check:

After installing UCT-V, you can perform the following to verify the version of UCT-V:

1. Enter the command:

```
sudo uctvl uctv-show
```

2. Manually execute the following command:

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

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **GigaVUE-FM Orchestration:** Perform the following steps:
 - a. Log in to the UCT-V.
 - b. Create a local configuration file and enter the following user data.
/etc/gigamon-cloud.conf is the local configuration file in the Linux platform.

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

- c. Restart the UCT-V service.

Linux platform:

```
$ sudo service uctv restart
```

For more details on how to create tokens, refer to .

- **Third Party Orchestration:** The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of the user to register with GigaVUE-FM. You can register UCT-V to GigaVUE-FM using Third Party Orchestration with the following two modes:
 - a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
 - b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

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

Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This option helps you get granular control over the monitored and mirrored traffic.

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

- [Windows Network Firewall Requirements](#)
- [Install Windows UCT-Vs](#)
- [Register Windows UCT-V](#)

Windows Network Firewall Requirements

If your environment uses network firewall rules or security groups, you must open specific ports for the virtual machine. For details, refer to [Network Firewall Requirement for GigaVUE Cloud Suite](#).

Ensure to use UCT-V Wizard with the `configure` option to configure Windows local firewall rules. Refer to [Install Windows UCT-Vs using Installation Script](#) for more details.

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.

- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to [Configure Tokens](#).
- Do not manually edit the UCT-V Windows service registry settings. Use the supported installation and upgrade workflows instead.

You can install the UCT-Vs with MSI package using one of the following options:

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



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

- **Visual C++ Redistributable 2019 (x86)**
- **Npcap (v1.81 OEM)**

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

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

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **6.14.00** MSI package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator**.
The UCT-V service starts automatically.

3. Use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

uctv-wizard

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

Options	Use Command	Description
pre-check	uctv-wizard pre-check	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added. NOTE: We recommend to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.
adapter-setup	uctv-wizard adapter-setup	Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup. You can choose between the following: • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as y. • Enter N if you wish to set it up manually. For details, refer to Windows UCT-V Installation.

Options	Use Command	Description
adapter-restore	uctv-wizard adapter-restore	Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the uctv-wizard adapter-setup step. NOTE: You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: - If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as y. - Enter N if you wish to restore it manually. For details, refer to
configure	uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the C:\Users\<username>\AppData\Local location). If available, UCT-V will use that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. - If you wish to skip the prompts to add the required firewall policy, enter your option as y. The console interface adds the firewall rules automatically. - Enter N if you wish to configure manually.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

**Notes:**

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

uctv-wizard help

Windows UCT-V Installation Scenarios

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

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V **6.14.00** MSI package from the [Gigamon Customer Portal](#). For assistance, contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

3. Modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

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



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

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

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

For IPv4:

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

For IPv6:

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

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

For IPv4:

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

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

For IPv6:

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

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

4. Save the file.

5. Restart the Windows UCT-V using one of the following actions:
 - From the command prompt, run **sc stop uctv** and **sc start uctv**.
 - From the Windows Task Manager, restart the UCT-V.

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

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

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

Create Images with the Agent Installed

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

To save the UCT-V as an image, refer to [the Capture VM to managed image](#) topic in the Microsoft Azure Documentation.

Uninstall UCT-V

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

Uninstallation Method

- Linux:
 - Uninstall the UCT-V in Ubuntu/Debian, RPM, Red Hat Enterprise Linux, and CentOS packages
 - Use the following command: **sudo uctv-wizard uninstall**
- Windows
 - Uninstall the UCT-V in the MSI package.
 - Use the following command: **CMD uctv-wizard uninstall**

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

Upgrade UCT-V

You can upgrade UCT-V in your virtual machine using the following options:

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

Refer to the below sections for detailed information and instructions.

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

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

NOTE: This method is complicated if you need to upgrade UCT-Vs for a large number of VMs. However, you can upgrade UCT-V in the workload VM without any hands-on involvement through GigaVUE-FM.

Refer to the sections below for details and instructions:

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

Rules and Notes:

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

Upload the UCT-V Images

Perform the following steps to upload UCT-V image files in GigaVUE-FM:

1. Go to **Inventory > Virtual** and select your cloud platform.
The **Monitoring Domain** page appears.
2. Select the **UCT-V Upgrade** drop-down menu and select **Images**.
3. In the **Images** page, click **Upload**. The **Upload Internal Image Files** wizard appears.
4. Select **Choose File**, upload the UCT-V files from your local, and select **Ok**.



Notes:

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

5. Verify if the uploaded UCT-V images is listed in the **Images** page.

Delete the file

You can delete one or multiple images.

1. In the **Images** page, select **Filter** to find the images based on Image Name, Version, and Image Type.
2. Select the required images.
3. From the Actions drop-down menu, select **Delete** or **Delete All**.

You can only delete those image files that are not associated with any tasks created for the upgrade process.

Upgrade the UCT-V

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

1. In the **UCT-V Upgrade** drop-down menu, select **Dashboard** to view the UCT-V upgrade landing page.
In the Dashboard page, you can view the upgrade status of individual UCT-Vs and the stages of the upgrade process (Fetch, Install, Verify). The page also displays the overall progress of the upgrade.
2. Select the required UCT-Vs, and from the **Actions** drop-down menu, select **Upgrade**.
The **UCT-V Upgrade task** page appears.

3. Enter the task name.
4. In the **Image Version** drop-down menu, select the required version you want to upgrade to from the list of available image versions. You can choose to upgrade immediately or schedule a time for the upgrade to happen.
5. Select the required option in the **Time Selection** field. If you prefer to schedule the upgrade, enter the choice of your date and time in the respective fields. Do not schedule the upgrade for a time in the past.
6. Select **Create**.
The image upgrade task is now created.



Note:

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

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



Notes:

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

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

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



Notes:

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

Upgrade UCT-V Manually

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

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

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

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

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**.

Create Monitoring Domain

Before configuring, you must establish a connection between GigaVUE-FM and your Azure environment. A Monitoring Domain in GigaVUE-FM allows you to define and manage this connection. Once established, GigaVUE-FM can deploy and manage UCT-V Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes within your specified VNets and Resource Groups.

GigaVUE-FM connects to Azure using either an Application ID and Client Secret (Service Principal) or the Managed Service Identity (MSI) authentication method.

To create an Azure monitoring domain in GigaVUE-FM,

1. Go to **Inventory > VIRTUAL > Azure**
2. Select **Monitoring Domain**.

The **Monitoring Domain** page appears.

3. In the Monitoring Domain page, select **New**.

The **Azure Monitoring Domain Configuration** wizard appears.

Monitoring Domain Configuration

Monitoring Domain*

Enter a monitoring domain name

Traffic Acquisition Method*

UCT-V (G-vTAP)

Traffic Acquisition Tunnel MTU*

1450

Use FM to Launch Fabric ⓘ

☒ Yes

Connections ⓘ

Name*

Enter a connection name

Credential*

Credential Name...

Subscription ID*

Subscription ID...

Region*

Region Name...

Resource Groups*

☒ Discovered ☐ Regex ⓘ

Resource Groups...

4. Enter or select the appropriate information for the Monitoring Domain:

- **Monitoring Domain:** An alias used to identify the monitoring domain.
- **Traffic Acquisition Method:** Select one of the following Tapping methods:
 - **UCT-V:** If you select UCT-V as the tapping method, the traffic is acquired from the UCT-Vs installed on your standard VMs in the Resource Group or in the Scale Sets. Then, the acquired traffic is forwarded to the GigaVUE V Series nodes. You must configure the UCT-V Controller to monitor the UCT-Vs.
 - **vTAP:** If you select vTAP as the tapping method, traffic tapping is performed by the Azure platform and sent to the GigaVUE V Series Node. GigaVUE-FM creates the necessary configurations in Azure to enable this.
 - **Customer Orchestrated Source:** If you select Customer Orchestrated Source as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series nodes without deploying UCT-Vs or UCT-V Controllers.

NOTE: Select the **Traffic Acquisition Method** as **Customer Orchestrated Source** if you wish to use Application Metadata Exporter (AMX) application.

- **Inline:** If you select this option, you can directly capture the inline traffic from the instances.
- **Traffic Acquisition Tunnel MTU:** The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series node.

The default value is 1450.

- When using IPv4 tunnels, the maximum MTU value is 1450. Ensure that the UCT-V tunnel MTU is 50 bytes less than the UCT-V destination interface MTU size.
- When using IPv6 tunnels, the maximum MTU value is 1430. Ensure that the UCT-V tunnel MTU is 70 bytes less than the UCT-V destination interface MTU size.
- **Use FM to Launch Fabric:** Select **Yes** to [Configure GigaVUE Fabric Components in GigaVUE-FM](#) or select **No** to [Configure GigaVUE Fabric Components in Azure - Integrated Mode](#).

- **Enable IPv6 Preference:** Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes. This option appears only when **Use FM to Launch Fabric** is disabled and Traffic Acquisition Method is UCT-V.
- **Connections:**

Connections

▼

Name*

Enter a connection name

Credential*

Credential Name... | ▼

Subscription ID*

Subscription ID... | ▼

Region*

Region Name... | ▼

Resource Groups*

☒ Discovered ☐ Regex ⓘ

Resource Groups... | ▼

+

-

- A Monitoring Domain can have multiple connections, however only one connection can have **Managed Service Identity** as the **Credential**.
- The connections in a monitoring domain can be a combination of multiple **Application ID with Client Secret** (Service Principal) accounts, or one **Managed Service Identity** and multiple **Application ID with Client Secret** (Service Principal) accounts.
- Each connection can have only one **Subscription ID**.
- **Name:** An alias used to identify the connection.
- **Credential:** Select an Azure credential. For details, refer to [Create Azure Credentials](#).
- **Subscription ID:** A unique alphanumeric string that identifies your Azure subscription.
- **Region:** Azure region for the monitoring domain. For example, West India.

- **Resource Groups:** Select the Resource Groups of the corresponding VMs to monitor.



Notes:

- This field is not applicable if you select **Customer Orchestrated Source** as the **Traffic Acquisition Method**.
- When you remove and re-add a resource group in IAM, it won't appear in GigaVUE-FM automatically. To refresh the list and make the resource group selectable, reselect the Subscription ID from the drop down. This action triggers the UI to reload the resource groups associated with the selected subscription.

5. Select **Save**.

The **Azure Fabric Launch Configuration** wizard appears.



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 only view and delete the existing configuration for GigaVUE V Series Node 1. You cannot perform any other actions on the existing configuration for GigaVUE V Series Node 1 as the features are deprecated from GigaVUE-FM.

Check Permissions while Creating a Monitoring Domain

NOTE: The Check Permissions feature is not available when the **Traffic Acquisition** Method is **vTAP**.

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

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Monitoring Domain**. The **Monitoring Domain** page appears.
3. Select **New**. The **Monitoring Domain Configuration** page appears.
4. Enter the details as mentioned in the [Create Monitoring Domain](#) section.
5. Select **Check Permission**. The **Check Permissions** widget opens.
6. Select the connection for which you wish to check the required permissions and then click **Next**.
7. Select the **Permission Status** tab to view the missing permissions. The **PERMISSIONS** tab lists the permissions required to run GigaVUE Cloud Suite for Azure.
8. Make sure to include all the permissions with Access Status as 'Denied' in the IAM policy.

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

Check Permissions

✓

Connection Selection

2

Permissions

Click on the permission status to view the missing permissions for the selected connection.

CONNECTION	PERMISSION STATUS	CREDENTIAL	REGION
C	✓ Success	sriram-cred	West US

←

<

Go to page: 1 of 1

>

→

1 permissions total

PERMISSIONS

IAM POLICY

Below is the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite.

Copy

Download

①

You must update the AZURE IAM Policy with the missing permissions that are highlighted in the JSON. To recheck the IAM Policy, go to the Permissions tab and click the Recheck button.

```

{
  "properties": {
    "roleName": "GigaVUE-FM-Service-Role",
    "description": "The minimum required permissions for FM to deploy GigaVUE Cloud Suite",
    "assignableScopes": [
      "6447eb55-9d09-481b-89bc-52e96bb52823",
      "d719fcb1-0d1a-43a8-bf8e-7844e293ce1a"
    ]
  },
  "permissions": [
    {
      "actions": [
        "Microsoft.Authorization/roleAssignments/read",
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/images/read",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/powerOff/action",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/restart/action",
        "Microsoft.Compute/virtualMachines/start/action",
        "Microsoft.Compute/virtualMachines/vmSizes/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Resources/subscriptions/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ]
}

```

Back

Close

You can use the **Copy** button to copy the permissions to the clipboard. Also, you can use the **Download** button to download the permission in JSON format.

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

Manage Monitoring Domain

You can view the details of the monitoring domain created in the list view. The list view details is based on:

- [Monitoring Domain](#)
- [Connections Domain](#)
- [Connections Domain](#)
- [UCT-Vs](#)

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

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

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

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

Monitoring Domain

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

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

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

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
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.
Actions	You can select a monitoring domain and then perform the following options: • Edit Monitoring Domain- Select a monitoring domain and then click Edit Monitoring domain to update the configuration. • Delete Monitoring Domain - You can select a monitoring domain or multiple monitoring domains to delete them. • Deploy Fabric - -You can select a monitoring domain to deploy a fabric, you cannot choose multiple monitoring domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific monitoring domain and GigaVUE-FM orchestration is enabled.. You must create a fabric in the monitoring domain, if the option is disabled • Upgrade Fabric-You can select a monitoring domain or multiple monitoring domains to upgrade the fabric. You can upgrade the V Series nodes using this option. • Delete Fabric- You can delete all the fabrics associated with the monitoring domain of the selected Fabric. • Edit SSL Configuration - You can use this option to add Certificate Authority and the SSL Keys. • View Permission Status Report - The View Permission Status Report monitors, audits, and reviews the current status of permissions assigned to users or roles, ensuring proper access control and compliance with security policies.
Filter	Filters the monitoring domain based on the list view options that are configured: • Tunnel MTU • Acquisition Method • Load Balancer • Centralised Connection • Management Subnet You can view the filters applied on the top of the monitoring domain page as a button. You can remove the filters by closing the button.

Connections Domain

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

The list view shows the following details:

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

Fabric

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

The list view shows the following details:

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

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

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

You can use the **Actions** buttons in this page to perform the following actions in the Monitoring domain page:

Buttons	Description
Edit Fabric	Use to edit a GigaVUE V Series Nodes.
Upgrade Fabric	Use to upgrade GigaVUE V Series Nodes. Refer to Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi for more detailed information on how to upgrade.

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

UCT-Vs

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

The list view shows the following details:

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

For details on **Settings**, refer to [Configure Azure Settings](#).

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

Configure GigaVUE Fabric Components in GigaVUE-FM

After configuring the Monitoring Domain, you reach the Azure Fabric Launch Configuration page. In the same page, you can configure all the GigaVUE fabric components.

Enter or select the required information as described in the following table.

Fields	Description
Connections	A connection that you created in the monitoring domain page. For details, refer to Create Monitoring Domain .
Centralized Virtual Network	Alias of the centralized VNet in which the UCT-V Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.
Authentication Type	The authentication method to connect to the Centralized VNet. - SSH Public Key Pair (Azure managed) - SSH Public Keys (manual entry)
SSH Public Key	- When SSH Public Key is selected, you can manually enter your own SSH public key - When SSH Public Key Pair is selected, you can choose an existing SSH key from the list retrieved from your Azure account. This requires an Azure permission that only applies when users want GigaVUE-FM to pull keys from Azure. Refer to Permissions and Privileges (Azure)
Resource Group	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM.
Security Groups	The security group created for the GigaVUE fabric components.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. Note: If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For details, refer to Secure Communication between GigaVUE Fabric Components .
Prefer IPv6	Enables IPv6 to deploy all the Fabric Controllers, and the tunnel between hypervisor to GigaVUE V Series Nodes using IPv6 address. If the IPv6 address is unavailable, it uses an IPv4 address. Note: This option can be enabled only when deploying a new GigaVUE V Series Node. If you wish to enable this option after deploying the GigaVUE V Series Node, then you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.
Select Yes to configure V Series Proxy for the monitoring domain. For details, refer to Configure GigaVUE V Series Proxy	

Azure Fabric Launch Configuration

Check Permissions Save C

Connections Select a Connection

Centralized Virtual Network Select a Virtual Network

Authentication Type sshPublicKey

SSH Public Key Enter your SSH Public Key

Resource Group Select resource group...

Security Groups Select management subnet security group...

Enable Custom Certificates Disabled

Prefer IPv6 No

Configure a V Series Proxy No

UCT-V Controller ①

Controller Version(s) Add

Image Select image...

Size Select instance...

Number of Instances 1

IP Address Type Private Public

Subnet Select management subnet...

Agent CA Select

Additional Subnets Add Subnet

Tags Add

V Series Node

SSL Key Select

Image Select image...

Size Select flavor...

Disk Size (GB) 30

IP Address Type Private Public

Subnet Select management network...

Data Subnets Add Subnet

Tags Add

Min Number of Instances 1

Max Number of Instances 1



To deploy GigaVUE fabric components (GigaVUE V Series Nodes, UCT-V Controller, and GigaVUE V Series Proxies) in GigaVUE-FM, you must accept the terms of the GigaVUE fabric components from the Azure marketplace using the Azure CLI or PowerShell. For details, refer to [Enable Subscription for GigaVUE Cloud Suite for Azure](#).

For details, refer to the following topics:

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

Configure UCT-V Controller

A UCT-V Controller manages multiple UCT-Vs and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes.

NOTE: A single UCT-V Controller can manage up to 500 UCT-Vs. The recommended minimum instance type is Standard_B4ms for UCT-V Controller.

A UCT-V Controller can only manage UCT-Vs that has the same version.

To configure the UCT-V Controllers,

NOTE: You can configure UCT-V Controller only if your **Traffic Acquisition Method** is **UCT-V**.

In the **Azure Fabric Launch Configuration** page, enter or select the appropriate values for the UCT-V Controller as described in the following table.

Controller Version(s)	Add
	Image 1.8.6 Size Standard_B1... Number of Instances 1
Management Subnet	IP Address Type ☒ Private ☐ Public Subnet mgmt
Additional Subnets	Add Subnet
Tags	Add

Fields	Description
Controller Version(s)	Ensure that the UCT-V Controller version you configure is always the same as the UCT-Vs' version number deployed in the VM machines. If multiple versions of UCT-Vs are deployed in the VM machines, then you must configure multiple versions of UCT-V Controllers that matches the version numbers of the UCT-Vs. Note: If the version of UCT-V Controllers doesn't match with UCT-Vs, GigaVUE-FM cannot detect the agents in the instances. To add UCT-V Controllers: - Under Controller Versions, click Add. - From the Image drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. - From the Size drop-down list, select a size for the UCT-V Controller. The default size is Standard_B1s. - In Number of Instances, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.
Management Subnet	IP Address Type: Select one of the following IP address types: - Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller instances and GigaVUE-FM instances in the same network. - Select Public if you want the IP address to be assigned from Azure's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. On selecting Public IP address type, you must select all the required Public IPs. Subnet: Select a Subnet for UCT-V Controller. The subnet that is used for communication between the UCT-V Controllers and the UCT-Vs, as well as to communicate with GigaVUE-FM. Every fabric component (both controllers and the nodes) needs a way to talk to each other and GigaVUE-FM. So, they should share at least one management plane/subnet. Note: Some instance types are supported in Azure platform. For details, refer to Microsoft Azure documentation to learn on supported instance types.
Agent Tunnel Type	The type of tunnel used for sending the traffic from UCT-Vs to GigaVUE V Series Nodes.

Fields	Description
Agent Tunnel CA	The Certificate Authority (CA) that should be used in the UCT-V Controller for connecting the tunnel.
Additional Subnet(s)	(Optional) If UCT-Vs are on subnets that are not IP routable from the management subnet, you must specify additional subnets so that the UCT-V Controller can communicate with all the UCT-Vs. Select Add to specify additional data subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tag(s)	(Optional) The key name and value that helps to identify the UCT-V Controller instances in your Azure environment. For example, you might have UCT-V Controllers deployed in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name that is easy to identify such as us-west-2-uctv-controllers. To add a tag: a. Click Add. b. In the Key field, enter the key. For example, enter Name. c. In the Value field, enter the key value. For example, us-west-2-uctv-controllers.

Configure GigaVUE V Series Proxy

GigaVUE V Series Proxy can manage multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.

NOTE: A single GigaVUE V Series Proxy can manage up to 100 GigaVUE V Series nodes. The recommended minimum instance type is Standard_B1s for V Series Proxy.

To configure the GigaVUE V Series Proxy,

1. In the **Azure Fabric Launch Configuration** page, select **Yes** to **Configure a V Series Proxy**. The GigaVUE V Series Proxy fields appears.
2. Enter or select the appropriate values for the V Series Proxy. For details, refer to the [UCT-V Controller field descriptions](#).

Configure GigaVUE V Series Node

GigaVUE V Series node is a visibility node that aggregates mirrored traffic from multiple UCT-Vs. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite for Azure using the standard VXLAN tunnels.

To launch a GigaVUE V Series node:

In the **Azure Fabric Launch Configuration** page, enter or select the appropriate values for the GigaVUE V Series Node.

V Series Node

Image	gigavue-gigavue-series-node-3.10-340871
Size	Standard_D4s_v4 8 vCPUs
Disk Size (GB)	>= 30
IP Address Type	☒ Private ☐ Public
Management Subnet	Subnet mgmt
Data Subnets	Add Subnet
Tags	Add

Tool Subnet ☒ Tool Subnet ⓘ

Subnet 1

Security Groups

Fields	Description
Image	From the Image drop-down list, select a GigaVUE V Series Node image.
Size	From the Size down-down list, select a size for the GigaVUE V Series Node. The default size for GigaVUE V Series Node configuration is Standard_D4s_v4 .
Disk Size (GB)	The size of the storage disk. The default disk size is 30GB. Note: When using Application Metadata Exporter, the minimum recommended Disk Size is 80GB.
IP Address Type	Select one of the following IP address types: - Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Node instances and GigaVUE-FM instances in the same network. - Select Public if you want the IP address to be assigned from Azure's pool of public IP address. On selecting Public IP address type, you must select the number of Public IPs defined in the Maximum Instance.
Management Subnet	Subnet: Select a management subnet for GigaVUE V Series. The subnet that is used for communication between the UCT-Vs and the GigaVUE V Series Nodes, as well as to communicate with GigaVUE-FM. Every fabric component (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management

Fields	Description
	plane/subnet.
Data Subnet(s)	The subnet that receives the mirrored VXLAN tunnel traffic from the UCT-Vs. Select a Subnet and the respective Security Groups. Click Add to add additional data subnets. Note: Using the Tool Subnet checkbox you can indicate the subnets to be used by the GigaVUE V Series Node to egress the aggregated/manipulated traffic to the tools.
Tag(s)	(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your Azure environment. For example, you might have GigaVUE V Series Nodes deployed in many regions. To distinguish these GigaVUE V Series Nodes based on the regions, you can provide a name that is easy to identify. To add a tag: - Click Add. - In the Key field, enter the key. For example, enter Name. - In the Value field, enter the key value.
Min Instances	The minimum number of GigaVUE V Series Nodes to be launched in the Azure connection. The minimum number of instances that can be entered is 1. Note: Nodes are launched when a monitoring session is deployed if GigaVUE-FM discovers some targets to monitor. The minimum amount is launched at that time. The GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances	The maximum number of GigaVUE V Series Nodes that can be launched in the Azure connection. When the number of instances per V Series node exceeds the max instances specified in this field, increase the number in the Max Instances to Launch. When additional V Series nodes are launched, GigaVUE-FM re-balances the instances assigned to the nodes. This can result in a brief interruption of traffic.

Click **Save** to complete the Azure Fabric Launch Configuration.

Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM

To check for permissions from the Azure Fabric Launch page, follow these steps:

1. In the Azure Fabric Launch page, enter the details as mentioned in [Configure GigaVUE Fabric Components in GigaVUE-FM](#).
2. Select **Check Permissions**. The **Check Permissions** widget opens. The permission status for Inventory, Security Group, and Fabric Launch are displayed in this widget.
3. Select **INVENTORY > Check Inventory Permissions**. You can view the required inventory permissions. Inventory permissions with the access status **Denied** are either missing in the IAM Policy or have restricted boundary

4. Select **SECURITY GROUPS > Check Security Group Permissions.**

You can view the ports required for the security groups. The ports in the **Denied** State are not open in the security group. The user blocks or restricts ports with the status **Explicit denied**. The ports with status **Partially configured** have incorrect IP address.

5. Select **FABRIC LAUNCH > Check Fabric Launch Permissions.**

You can view the permissions required for deploying the GigaVUE fabric components. The Virtual Machine permissions with the access status **Denied** could be missing in the IAM Policy.

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

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

Check Permissions

INVENTORY

SECURITY GROUPS

FABRIC LAUNCH

IAM POLICY

Below is the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite.

CopyDownload

i You must update the AZURE IAM Policy with the missing permissions that are highlighted in the JSON. To recheck the IAM Policy, go to the Inventory tab or Fabric Launch tab and click the Recheck button.

```

{
  "properties": {
    "roleName": "GigaVUE-FM-Service-Role",
    "description": "The minimum required permissions for FM to deploy GigaVUE Cloud Suite",
    "assignableScopes": [
      "6447eb55-9d09-481b-89bc-52e96bb52823"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/roleAssignments/read",
          "Microsoft.Compute/disks/delete",
          "Microsoft.Compute/images/read",
          "Microsoft.Compute/virtualMachines/delete",
          "Microsoft.Compute/virtualMachines/powerOff/action",
          "Microsoft.Compute/virtualMachines/read",
          "Microsoft.Compute/virtualMachines/restart/action",
          "Microsoft.Compute/virtualMachines/start/action",
          "Microsoft.Compute/virtualMachines/vmSizes/read",
          "Microsoft.Compute/virtualMachines/write",
          "Microsoft.Network/networkInterfaces/delete",
          "Microsoft.Network/networkInterfaces/join/action"
        ]
      }
    ]
  }
}

```

Close

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

Configure GigaVUE Fabric Components in Azure - Integrated Mode

This section provides information on how to register GigaVUE fabric components using Azure Portal or a configuration file.

Overview of Third-Party Orchestration

You can use your own Azure Orchestrator to deploy the GigaVUE fabric components instead of using GigaVUE-FM to deploy your fabric components.

The third-party orchestration feature allows you to deploy GigaVUE fabric components using your own Azure orchestration system. These fabric components register themselves with GigaVUE-FM with user information. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

You can deploy the fabric components using one of the following options:

- Manually using a configuration file.
- Use the Azure portal to launch the instances and deploy the fabric components using Custom data. Using your Custom data, the fabric components register themselves with the GigaVUE-FM. Based on the group name and the subgroup name details provided in the Custom data, GigaVUE-FM groups these fabric components under their respective monitoring domain and connection name.

The heartbeat messages sent from the respective nodes help GigaVUE-FM determine the health status of the registered nodes.

For details, refer to the following sections:

- [Prerequisites](#)
- [Disable GigaVUE-FM Orchestration in Monitoring Domain](#)
- [Configure UCT-V Controller in Azure](#)
- [Configure UCT-V in Azure](#)
- [Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure](#)

Prerequisites

Ensure that GigaVUE V Series Node has at least have two Networks Interfaces (NIC) attached to it:

- A management NIC
- A data NIC with Accelerated Networking enabled.

When creating a virtual machine for GigaVUE V Series Node using CLI, you can attach Management NIC and Data NIC at the time of the virtual machine creation. However, if you are using Azure GUI to create the virtual machine for GigaVUE V Series Node, then you can attach the data NIC only after creating the virtual machine.

For details, refer to the following topics:

- [Create GigaVUE V Series Node with Management and Data NIC Attached using CLI](#)
- [Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI](#)



NOTE:

- Accelerated Networking must be enabled in the Data NIC only when deploying GigaVUE V Series Nodes using Third Party Orchestration.
- Accelerated Networking is not required for Management NIC.

Create GigaVUE V Series Node with Management and Data NIC Attached using CLI

1. Create the management NIC.

```
az network nic create -g <resource group> --vnet-name <VNet Name> --subnet  
<Subnet name> -n <Mangement NIC Name>
```

2. Create data NIC with Accelerated Networking enabled.

```
az network nic create -g <resource group> --vnet-name <VNet> --subnet <Subnet> -  
n <Data NIC> --accelerated-networking true
```

3. Create GigaVUE V Series Node virtual machine using the above NICS.

```
az vm create --resource-group <Resource group> --size <Standard_D4s_  
v4/Standard_D8S_V4> --name <GigaVUE V Series Node> --admin-username gigamon -  
-generate-ssh-keys --image gigamon-inc:gigamon-gigavue-cloud-suite-  
v2:vseries-node-v6.14.00:6.14.00 --plan-name vseries-node-v6.14.00 --plan-  
product gigamon-gigavue-cloud-suite-v2 --plan-publisher gigamon-inc --nics  
<Management NIC and Data NIC>
```

NOTE: You can use the following command to view all the images from Gigamon.

```
az vm image list --all --publisher gigamon-inc
```

Create GigaVUE V Series Node with Management and Data NIC Attached using Azure GUI

Enable Management NIC when creating the GigaVUE V Series Node virtual machine.

For details, refer to the [Create virtual machine](#) topic in Azure Documentation.

Perform the following steps to attach the data NIC:

1. Select the GigaVUE V Series Node virtual machine from the Resources Page.
2. Stop the Virtual Machine using the **Stop** button.
3. Navigate to **Setting > Networking** from the left navigation pane.
The **Networking** page appears.
4. In the **Networking** page, select **Attach network interface**.
5. Select an existing network interface for Data NIC and select **OK**.
To enable accelerated networking, refer to [Manage Accelerated Networking through the portal](#).
6. Start the Virtual Machine.

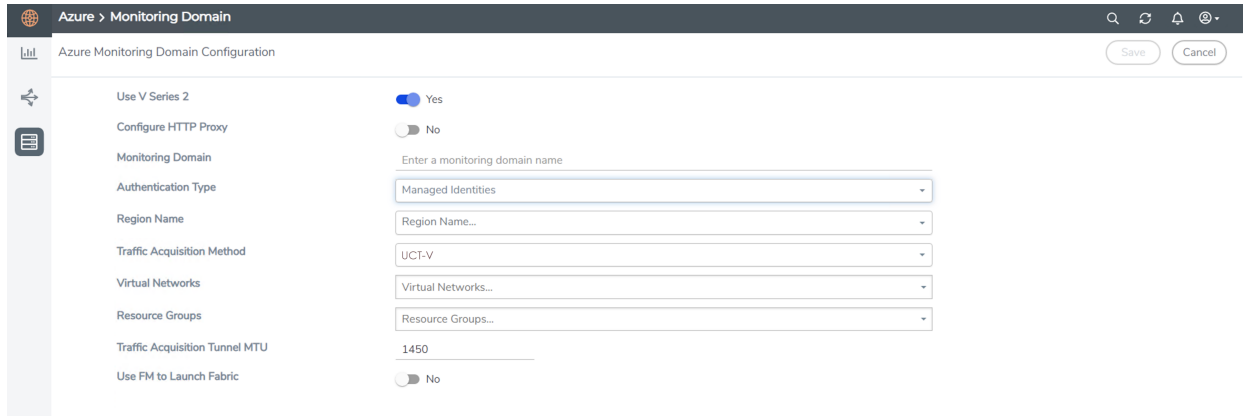
Keep in mind the following when deploying the fabric components using third party orchestration in integrated mode:

- Create tokens in the **User Management** page in GigaVUE-FM. Refer to [Configure Tokens](#) for more detailed information.
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For more details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the 6.9 Documentation.
- When configuring UCT-V Controller, select **UCT-V** as the Traffic Acquisition Method.
- When you select Customer Orchestrated Source as your Traffic Acquisition Method, UCT-V and UCT-V Controller registration are not applicable.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the GigaVUE V Series Nodes or UCT-V Controllers.
- Deployment of UCT-V Controller, GigaVUE V Series Node, and GigaVUE V Series Proxy through a third-party orchestrator is supported only on Linux platform.
- Deployment of UCT-V through a third-party orchestrator is supported on Linux and Windows platforms. Refer to [Linux UCT-V Installation](#) and [Windows UCT-V Installation](#) for detailed information.
- When creating virtual machine for deploying the fabric components in Azure, **SSH public key** must only be used as the **Authentication type** in Azure.

Disable GigaVUE-FM Orchestration in Monitoring Domain

To register fabric components under Azure monitoring domain,

1. Create a monitoring domain in GigaVUE-FM. For details, refer to [Create Monitoring Domain](#).
2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field.
You need to configure the fabric components in Azure Orchestrator.



The screenshot shows the 'Azure Monitoring Domain Configuration' page. The left sidebar contains a navigation menu with icons for 'Azure > Monitoring Domain', 'Azure Monitoring Domain Configuration', and a list icon. The main content area displays the following configuration options:

- Use V Series 2**: Toggle set to **Yes**.
- Configure HTTP Proxy**: Toggle set to **No**.
- Monitoring Domain**: Text input field with placeholder 'Enter a monitoring domain name'.
- Authentication Type**: Dropdown menu set to **Managed Identities**.
- Region Name**: Dropdown menu set to **Region Name...**.
- Traffic Acquisition Method**: Dropdown menu set to **UCT-V**.
- Virtual Networks**: Dropdown menu set to **Virtual Networks...**.
- Resource Groups**: Dropdown menu set to **Resource Groups...**.
- Traffic Acquisition Tunnel MTU**: Text input field set to **1450**.
- Use FM to Launch Fabric**: Toggle set to **No**.

3. Deploy your fabric components through Azure Portal.

In your Azure Portal, you can configure the following GigaVUE fabric components:

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

Configure UCT-V Controller in Azure

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

You can register UCT-V Controller in Azure Portal using one of the following methods:

- [Register UCT-V Controller during Virtual Machine Launch](#)
- [Register UCT-V Controller after Virtual Machine Launch](#)

Register UCT-V Controller during Virtual Machine Launch

In your Azure portal, to launch the UCT-V Controller init virtual machine and register UCT-V Controller using custom data, follow these steps:

1. In the Virtual machines page of the Azure Portal, select **Create > Virtual machine**. The **Create a Virtual Machine** Page appears. For details, refer to the [Create virtual machine](#) topic in Azure Documentation.

2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteIP: <IP address of the GigaVUE-FM>
      sourceIP: <IP address of UCT-V Controller> (Optional Field)
      remotePort: 443
```

- Enter the monitoring domain name and the connection name of the monitoring domain created earlier as the groupName and the subGroupName in the Custom Data.
- The UCT-V Controller uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM

The UCT-V Controller deployed in your Azure portal appears on the Monitoring Domain page of GigaVUE-FM.

☐ Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
☐ MD1					
	pubintapi-vpc				✓ Connected
		G-vTapController	34.219.250.146	1.7-304	✓ Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	✓ Ok
		Gigamon-VSeriesNode-1	172.30.24.188	2.2.0	✓ Ok

Register UCT-V Controller after Virtual Machine Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file,

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

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  token: <Token>
  remoteIP: <IP address of the GigaVUE-FM>
  sourceIP: <IP address of UCT-V Controller> (Optional Field)
  remotePort: 443
```

3. Restart the UCT-V Controller service.
\$ sudo service uctv-cntlr restart

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

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

Example netplan config:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
```

```
dhcp6: no
accept-ra: false
routes:
  - to: 10.114.48.1/32
    scope: link
  - to: default
    via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

```
$ sudo netplan apply
```

Configure UCT-V in Azure



Notes:

- You can deploy UCT-Vs using a third-party orchestrator on Linux and Windows platforms. For details, refer to [Linux UCT-V Installation](#) and [Windows UCT-V Installation](#).
- You can configure more than one UCT-V Controller for a UCT-V. If one UCT-V Controller goes down, the UCT-V registration happens through another active UCT-V Controller.

To register UCT-V after launching a Virtual Machine using a configuration file, follow these steps:

1. Install the UCT-V on the Linux or Windows platform. For detailed instructions, refer to [Linux UCT-V Installation](#) and [Windows UCT-V Installation](#).
2. Log in to the UCT-V. For details, refer to [Default Login Credentials](#).

3. Create a local configuration file and enter the following custom data.



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

Registration:

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



If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:

```
localInterface:<Interface to which UCT-V Controller is connected>
```

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, then GigaVUE-FM unregisters UCT-V and it is removed from GigaVUE-FM.

Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure

It is not mandatory to register GigaVUE V Series Nodes via GigaVUE V Series



- You can register your nodes using GigaVUE V Series Proxy when,
 - A large number of nodes are connected to GigaVUE-FM or
 - The user does not wish to reveal the IP addresses of the nodes.
- In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.



- When deploying GigaVUE V Series Node using GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and provide the IP address of the proxy as the Remote IP of the GigaVUE V Series Node.

Register GigaVUE V Series Node and GigaVUE V Series Proxy in Azure Portal using one of the following methods:

- [Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch](#)
- [Register GigaVUE V Series Node and GigaVUE V Series Proxy after Virtual Machine Launch](#)

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy using the custom data in Azure Portal, follow these steps:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**.
2. On the **Create a Virtual Machine** Page, configure the settings. For detailed information, refer to [Create virtual machine](#) topic in Azure Documentation.
3. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine.

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

- Enter the monitoring domain name and the connection name of the monitoring domain created earlier as the groupName and the subGroupName in the Custom Data.
- The GigaVUE V Series Node and GigaVUE V Series Proxy uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

Register GigaVUE V Series Node and GigaVUE V Series Proxy after Virtual Machine Launch

To register GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow these steps:

1. Log in to the GigaVUE V Series Node or Proxy. For details on UCT-V Controller default login credentials, refer to [Default Login Credentials](#).
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom data.

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



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

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

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

If you are using Azure GUI to create the virtual machine for GigaVUE V Series Node, then you need to attach data NIC to GigaVUE V Series Node after creating the virtual machine.

For details, refer to [Prerequisites](#).

Configure Secure Communication between Fabric Components in FMHA

IMPORTANT: Before upgrading the Fabric Components to version 6.10 or later, complete the following steps after upgrading GigaVUE-FM to version 6.10 or later.

Follow these steps:

1. Access the active GigaVUE-FM via CLI.
2. Archive the stepCA directory using the following commands:

```
sudo su
cd /var/lib
tar -cvf /home/admin/stepca.tar stepca
```
3. Set the permissions of the tar file using the following commands:

```
chmod 666 /home/admin/stepca.tar
```
4. Copy the tar file to all standby instances in the **/home/admin/ directory** using scp:

```
scp /home/admin/stepca.tar <standby-node>:/home/admin/
```
5. Download the **runstepca_fmha** script from the Community Portal.
6. Log in to the standby instance using CLI.
7. Copy the script in the standby instance in the **/home/admin directory** and execute it using the following command:

```
sh /home/admin/runstepca_fmha
```

Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Node. For more detailed information about UCT-V Controller, GigaVUE V Series Proxy and Node Version, refer to the *GigaVUE-FM Version Compatibility* section in the [Prerequisites for GigaVUE Cloud Suite for Azure](#).



IMPORTANT NOTE:

Before upgrading the Fabric Components to version 6.10.00 or above, ensure the following actions are performed:



- Create Token in GigaVUE-FM for UCT-V Installation and update it in the configuration file. For more details, refer to [UCT-V-VSN.html](#).
- Create Tokens for deploying the Fabric Components using Third Party Orchestration. For more details, refer to [Configure Tokens](#).
- Open the required ports in the cloud platform. For more details, refer to [Network Firewall Requirement for GigaVUE Cloud Suite](#).

For more details, refer for more information:

- [Prerequisite](#)
- [Upgrade UCT-V Controller](#)
- [Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy](#)

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node, you must upgrade GigaVUE-FM to software version 5.13.01 or above.

Upgrade UCT-V Controller

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

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

To change UCT-V Controller version between different major versions

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

- a. In the **Azure Fabric Launch Configuration** page, under **Controller Versions**, click **Add**.
- b. From the **Image** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
- c. From the **Size** drop-down list, select a size for the UCT-V Controller. The default size is Standard_B1s.

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

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

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

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

Change UCT-V Controller version with in the same major version

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

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



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

Upgrade GigaVUE V Series Node and GigaVUE V Series Proxy

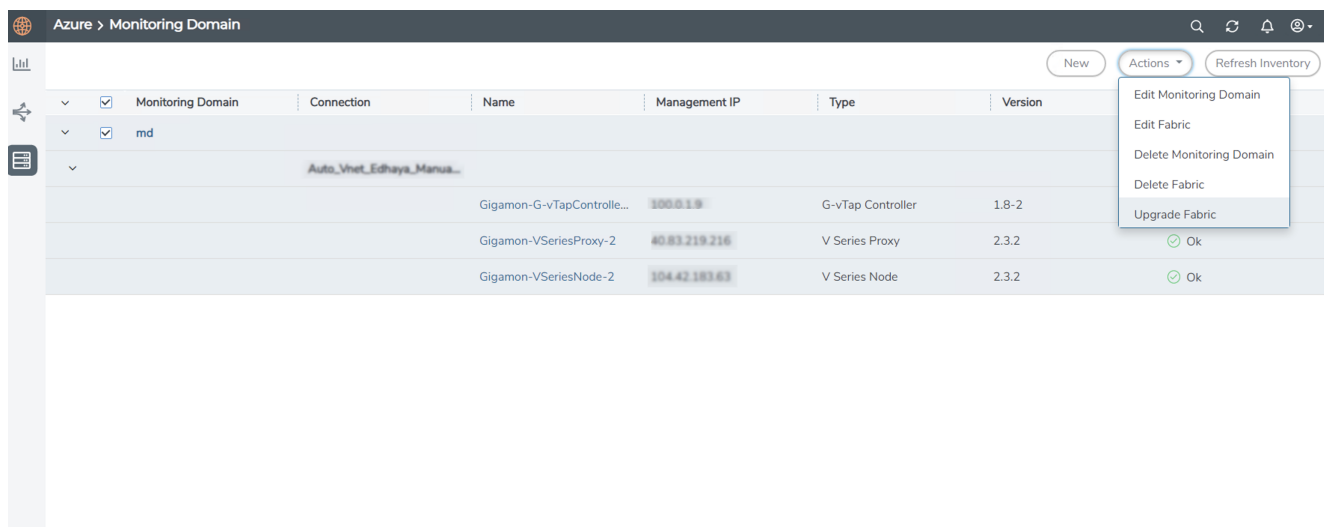
GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Node at a time.

You can upgrade the GigaVUE V Series Proxy and Node using the following options:

- Launch and replace the complete set of nodes and proxys at a time.
For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VNet, you can upgrade all of them at once. First, the new version of GigaVUE V Series controller is launched. Next, the new version of GigaVUE V Series nodes are launched. Then, the old version of V Series controller and nodes are deleted from the VNet.
- NOTES:**
 - When the new version of node and proxy is launched, the old version still exists in the VNet until they are deleted. Make sure the instance type determined during the configuration can accommodate the total number of new and old instances present in the VNet. If the instance type cannot support so many instances, you can choose to upgrade in multiple batches.
 - If an error happens while upgrading the complete set of proxys and nodes present in the VNet, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
 - If you have deployed your nodes using Public IP address while creating the monitoring domain, then select the same number of Public IP addresses defined in your Max Instances when upgrading your nodes. For details, refer to *Create Monitoring Domain* in GigaVUE Cloud Suite Deployment Guide - Azure.
- Launch and replace the nodes and proxy in multiple batches.
For example, if you need to upgrade 18 GigaVUE V Series Nodes, specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node,

- Go to **Inventory > VIRTUAL > Azure**, and then select **Monitoring Domain**. The **Monitoring Domain** page appears.
- On the Monitoring Domain page, select the connection name check box and select **Actions**



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

Fabric Nodes Upgrade

V Series Proxy

Upgrade	☒
Current Version	2.3.0
Image	gigamon-gigavue-vseries-proxy-2.3.2-284364
Change Size	☐
Batch Size	1

V Series Node

Upgrade	☒
Current Version	2.3.0
Image	gigamon-gigavue-vseries-node-2.3.2-284421
Change Size	☐
Batch Size	1
Public IPs	104.42.181.54 104.42.181.63 x

Upgrade

Cancel

4. Select the **Upgrade** check box, upgrade the GigaVUE V Series Node/Proxy.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V SeriesProxy/Nodes.
6. Select the **Change Size** check box to change the flavor of the node/proxy, only if required.
7. Specify the batch size in the **Batch Size** box to upgrade the GigaVUE V Series Node/Proxy.

For example, if you have 7 GigaVUE V Series Nodes, specify 7 as the batch size and upgrade all of them. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series nodes in each batch. In the last batch, the remaining 1 V Series node is launched.

- From the Public IPs drop-down list, select the IP addresses equal to the Max Instances defined when creating a monitoring domain.

NOTE: This is only applicable for nodes deployed using Public IP, when creating a monitoring domain.

- Select **Upgrade**.

The upgrade process takes a while depending on the number of GigaVUE V Series Proxys and Nodes upgrading in your Azure environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. The monitoring session is deployed automatically.

To view the detailed upgrade status, select **Upgrade in progress** or **Upgrade successful**, the **V Series Node Upgrade Status** dialog box appears.

Fabric Nodes Upgrade Status

Monitoring Domain: md

Start Time	2021-10-11 20:58:56
End Time	2021-10-11 21:04:03
Status	Fabric upgrade completed successfully

	Proxies	Nodes
Total	1	1
Upgraded	1	1
Upgrading	0	0
Remaining	0	0
Failures	0	0

Clear

Close

- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.

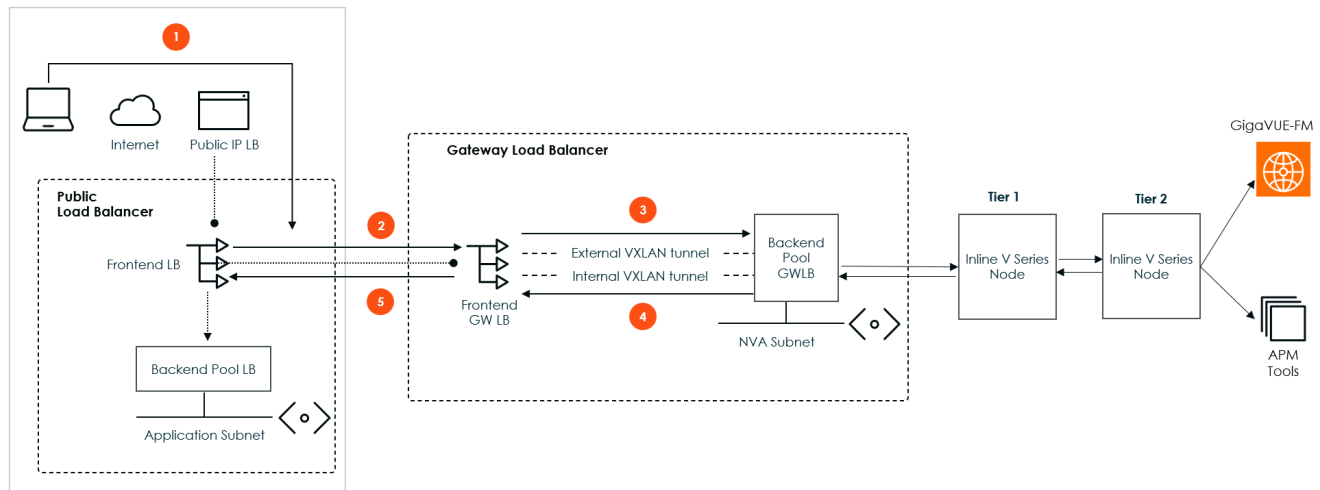
Acquire Traffic using Inline V Series Solution

NOTE: Click the following prompt to generate a quick deployment checklist for this topic.

Create a comprehensive checklist based on the deployment steps outlined in the Deploy Inline V Series Solution in Azure topic.

This section outlines the work flow for acquiring traffic using Inline V Series Node and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides instructions to configure traffic acquisition, processing, and forwarding to your desired destination.

Note: The work flow described in this section is based on the topology shown below. The approach for acquiring traffic depends on your specific requirements. Additionally, you can decide whether to route traffic through public load balancer based on your topology.



Refer to the following topics to deploy Inline V Series in Azure:

- [Create a Resource Group](#)
- [Create Virtual Networks](#)
- [Create a Virtual Network Peering](#)
- [Create a Network Security Group](#)
- [Create a Load Balancer](#)

- [Install GigaVUE-FM on Azure](#)
- [Enable System Assigned Managed Identity](#)
- [Create Gigamon Custom Role](#)
- [Assign Role to Resource Group](#)
- [Assign Role to GigaVUE-FM Instance](#)
- [Create a GigaVUE-FM Token](#)
- [Modify Virtual Machine Scale Set \(VMSS\) Cloud Initialization Template](#)
- [Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node \(Tier 1\)](#)
- [Assign VMSS to GWLB Backend Pools](#)
- [Create Monitoring Domain](#)
- [Deploy GigaVUE V Series Nodes for Inline V Series Solution](#)
- (Optional) [Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node \(Tier 2\)](#)
- [Configure Monitoring session](#)

Create a Resource Group

The resource group is a container that holds all the resources for a solution. Select an existing resource group or create a new resource group. For navigation steps and detailed instructions, refer to [Create a resource group](#) topic in the Azure Documentation.

NOTE: We recommend creating a dedicated Resource Group for GigaVUE Visibility Fabric components such as GigaVUE-FM, V Series Nodes, Gateway Load Balancer, and others.

Create Virtual Networks

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You can choose to:

- **Select an existing VNet:** When you choose an existing VNet, Azure automatically populates the Subnet and Public IP fields.
- **Create a new VNet:** To create a new VNet, follow the steps in the [Create a virtual network](#) topic in the Azure Documentation

NOTE: We recommend setting up two separate virtual networks to support the GigaVUE Visibility Fabric. The first VNet (Viz_VNet) will host the GigaVUE visibility components such as GigaVUE-FM and V Series Nodes. The second VNet (App_VNet) will contain the virtual machines responsible for generating traffic.

Create a Virtual Network Peering

When workload virtual machines are distributed across multiple virtual networks, you must enable Virtual Network Peering between each workload VNet and the VNet hosting the GigaVUE V Series Node. This peering setup allows seamless communication between VNets within Azure.

To set up peering between the two VNets you created, refer to [Manage a virtual network peering](#) topic in Azure documentation.

Create a Network Security Group

Network Security Groups (NSGs) filter inbound and outbound traffic to subnets and network interfaces using security rules. You should configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components. Select an existing network security group or create a new network security group. For navigation steps and detailed instructions, refer to [Create a network security group](#) topic in the Azure Documentation.

Create a Load Balancer

Gigamon deploys its solution as a Network Virtual Appliance positioned behind a Gateway Load Balancer. To ensure traffic flows through the V Series, it must be routed to the GWLB. You can achieve this routing either via a Standard Load Balancer or directly from a virtual machine's public interface. Microsoft recommends using a Standard Load Balancer for optimal integration.

Refer to the following sections for information on creating a Gateway Load Balancer and Standard Load Balancer:

Create a Gateway Load Balancer

Set up a Gateway Load Balancer (GWLB), which will later forward traffic to the Tier 1 V Series Node. Once deployed, the Tier 1 V Series Node will mirror packets from the workload virtual machines, enabling traffic visibility.

The following table lists the specific options you must select when creating a Gateway Load Balancer for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Gateway Load Balancer](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Basics		
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group that you created	Yes
Name	Enter a valid name	Yes
Region	Select the region	Yes
SKU	Select Gateway	Yes
Type	Select Internal	Yes
Tier	Select Regional (default)	Yes
FrontEnd IP Configuration - Add a frontend IP configuration		
Name	Enter a valid name	Yes
IP Version	Select based on the requirement	Yes
Virtual Network	Select your virtual network	Yes
Subnet and IP Assignment	Select your subnet and choose Dynamic for assignment	Yes
Backend Pools - Add a backend pool		
Name	Enter a valid name	Yes
Virtual Network	Default	Yes
Backend Pool Configuration	Select NIC	Yes
Gateway load balancer configuration		
Type	Choose Internal and External.	Yes
Internal and External Ports	Use default values Note: If you change the port values here, update the same ports in the Custom data and cloud-init field when creating the Virtual Machine Scale Set	Yes
NOTE: Add backend pool without IP Configuration (you will attach NICs later in this step Assign VMSS to GWLB Backend Pools).		
Inbound Rules - Add a load balancing rule		Yes
Name	Enter a valid name	Yes
IP Version	Select IPv4 or IPv6	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list	Yes
Backend Pool	Select an existing Backend pool from the drop-down list	Yes

Parameters	Description	Mandatory field
Session Persistence	Select None	Yes
Health Probe	Select Create New and enter the following details: - Protocol - Select HTTP as the protocol - Port - Enter 8888 as the port - Path: /health - Interval - Enter 5 seconds as the approximate amount of time, in seconds	Yes
Idle timeout (minutes)	Leave default or adjust as required	Yes

(Optional) Create a Standard Load Balancer

NOTE: Routing traffic through a public load balancer is optional and applies only to the topology shown at the beginning of this document. Alternatively, you can route traffic to the Gateway Load Balancer from a VM that has an interface with a public IP.

The following table lists the specific options you must select when creating a Standard Load Balancer for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Public Gateway Load Balancer](#) topic in Azure documentation.

For details regarding traffic flow from Gateway Load Balancer to Standard Load Balancer, refer to [Gateway Load Balancer](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Basics		
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group that you created	Yes
Name	Enter a valid name	Yes
Region	Select the region	Yes
SKU	Select Standard	Yes
Type	Select Public (validated type)	Yes
Tier	Select Regional	Yes
FrontEnd IP Configuration - Add a frontend IP configuration		
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
IP Type	Select IP Address as the IP type	Yes
Public IP address	Select the public IP address from the drop-down list. If	Yes

Parameters	Description	Mandatory field
	required, you can create a new IP address	
Gateway Load Balancer	Select the Gateway Load Balancer you created in the previous step to associate it with the frontend IP configuration	Yes
Backend Pools - Add a backend pool		
Name	Enter a valid name	Yes
Virtual Network	Select the same virtual network as the Standard Load Balancer —typically the App VNet—to ensure communication with the workloads.	Yes
Backend Pool Configuration	Select IP Address	Yes
IP Address	Specify the private IP address of the source/customer VM	
Inbound Rules - Add a load balancing rule		Yes
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list	Yes
Backend Pool	Select an existing Backend pool from the drop-down list	Yes
Protocol	Select TCP as the protocol	Yes
Port	Enter 80 as the port	Yes
Backend Port	You can configure the backend port to match the frontend port. Enter a value based on your traffic requirements	Yes
Health Probe	Select Create new and create a new Health Probe with TCP Protocol, Port 80, and 5-second attempt interval	Yes
Session Persistence	Select None	Yes
Idle timeout (minutes)	Enter or select 4	Yes
Outbound Rules -		
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list.	Yes
Protocol	All	Yes
Idle timeout (minutes)	Enter or select 4	Yes
TCP Reset	Enabled	Yes
Backend Pool	Select an existing Backend pool from the drop-down list.	Yes
Port Allocation	Use the default number of outbound ports	Yes

Install GigaVUE-FM on Azure

To install GigaVUE-FM using the Azure Marketplace:

1. Go to Azure Marketplace and search for Gigamon. The latest version of Gigamon GigaVUE Cloud Suite for Azure appears. Click **Get it Now**.
2. In the pop-up window, select the **GigaVUE-FM (Fabric Manager) vX.XX - BYOL** option and click Continue.
3. Select the "**Want to deploy programmatically? Get started**" link.
4. Review the terms of service and the subscription name, and then select Enable. Click **Save**.
5. Verify the selected **Subscription** and **Plan**, then click **Create**.

6. Configure the GigaVUE-FM VM details. Most fields are pre-populated, but some require manual input. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#). For detailed instructions, refer to [Create a Linux virtual machine in the Azure](#) in Azure Documentation.

Table 1: GigaVUE-FM Installation Steps

Field	Description
Basics	
Subscription	Select your subscription.
Resource Group	Select the Inline V Series Resource Group that you created.
System-assigned managed identity	Use a system-assigned managed identity when a resource needs to authenticate to other services, and you want the identity to be created and deleted with the resource. Note: If you update any role it would take more than an hour to reflect in GigaVUE-FM, however, if you use APP registration it would take between 5-10 minutes to update in GigaVUE-FM.
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Availability Zone	Choose your availability zone
Security Type	To enable UEFI secure boot, select Trusted launch virtual machines from the drop-down list. Click Configure security features and ensure that the Enable secure boot check box is enabled.
Image	Select the latest GigaVUE-FM images. NOTE: You cannot select multiple images for a VM.
Size	Select the recommended instance type: GigaVUE-FM - Standard_D4s_v3
Authentication Type	We support only SSH public key authentication type - SSH public key - Enter the administrator username for the VM. - Enter the SSH public key pair name. - Password - Enter the administrator username for the VM. - Enter the administrator password. NOTE: The username "gigamon" is reserved for internal usage. Do not create a user with the name "gigamon"
Disks	

Field	Description
Disk Size	The required disk size for GigaVUE-FM is 2 x 40GB .
Networking	
Virtual Network	Select the virtual network that you created.
Configure network security group	Select the network security group that you created.

NOTE: Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in Azure, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

Enable System Assigned Managed Identity

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.

To enable MSI on the VM running in GigaVUE-FM using the Azure portal, refer to [Configure managed identities using the Azure portal](#) in the Azure documentation.

Create Gigamon Custom Role

When you first connect GigaVUE-FM to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for GigaVUE-FM to integrate with Azure APIs and to automate the fabric deployment and management.

IMPORTANT: "Microsoft.Authorization/roleAssignments/read" permission is required for validating the required permissions. Ensure to include "Microsoft.Authorization/roleAssignments/read" permission in your IAM policy.

The 'built-in' roles provided by Microsoft are open to all resources. Refer to [Create or update Azure custom roles](#) topic in the Azure documentation to update the policy with the relevant IAM service.

After completing the configuration in the Basics, Permissions, and Assignable Scopes sections, copy the permissions listed below and paste them into the JSON code to create a custom role.

NOTE: Ensure to assign the roles for the permissions listed below at the subscription level.

```
{
  "Name": "CustomRoleForInline",
  "description": "Minimum requirements for FM in inline tapping",
  "assignableScopes": [
    "/subscriptions/<Subscription ID>"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.Resources/subscriptions/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/backendPoolAddresses/read",
        "Microsoft.Compute/virtualMachineScaleSets/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigurations/read",
        "Microsoft.Compute/virtualMachines/read"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ]
}
```

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.

Assign Role to Resource Group

You can specify where the custom role is available for assignment such as a management group, subscription, or resource group and assign the created role to the resource group you created. In Azure, locate your newly created Role by navigating to

“Management Groups” and selecting your subscription Id.

For further navigation and instructions to assign a role to your resource group, refer to the steps listed in **Update a custom role** and **Assignable scopes** sections of the [Create or update Azure custom roles](#) topic in the Azure documentation.

Assign Role to GigaVUE-FM Instance

You can assign the custom role you have created to GigaVUE-FM instance in Azure. For navigation path and detailed instructions, follow the steps listed in **Open the Add role assignment page**, **Select the appropriate role**, and **Select who needs access** sections of the [Assign Azure roles using the Azure portal](#) topic in the Azure documentation.

Create a GigaVUE-FM Token

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can create multiple tokens if required.

To create a token in GigaVUE-FM, follow these steps:

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

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

3. Select **New Token**.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access GigaVUE-FM from the **User Group** drop-down list.
7. Select **OK** to generate a new token. The generated token appears on the **Tokens** page.
8. Select the token to copy and use it to authenticate the GigaVUE-FM REST APIs.
 - a. Go to **Actions > Copy Token**.
 - b. Paste the copied token in the required fields to complete authentication.

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

Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template

The script given below will be essential for creating the VMSS, which uses this data to deploy the V Series node. This information is also required when configuring the Monitoring Domain in GigaVUE-FM.

Ensure you save these values in a secure location for reference in the upcoming steps. You can modify only the following parameters in the template:

- groupName
- subGroupName
- remoteIP
- Token

Custom Template:

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.

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

- path: /etc/vseries-inline.conf
  owner: root:root
  permissions: '0644'
  content: ""
```

Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)

V Series Nodes are created as part of a Virtual Machine Scale Set (VMSS) to allow scaling based on demand. This setup enables you to scale out or scale in the number of V Series Nodes as needed for each tier. Therefore, each tier will have a dedicated VMSS. The inline V Series solution does not support standalone V Series Nodes that are not part of a scale set.

The following table lists the specific options you must select when creating a Virtual Machine Scale Set for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Virtual Machine Scale Set](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group	Yes
Virtual Machine Scale Set Name	Enter a valid name	
Region	Select a desired region	
Availability Zones	Choose if you want to use zones for high availability.	No
Orchestration		
Orchestration Mode	Select Uniform as the orchestration mode.	Yes
Security Type	Select Standard mode.	Yes
Scaling		
Scaling Mode	Choose Autoscaling .	Yes
Scaling Configuration	Click Configure to edit the scaling conditions.	Yes
Default Condition	Enter the Initial Instance Count as 0. NOTE: Once the Monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that you need to deploy in this Monitoring Domain.	Yes
Condition	Choose a metric-based scaling condition (For example, CPU usage, network traffic).	Yes
Metric Source	Select the metric (For example, Average CPU Percentage).	Yes
Scale out	Set conditions like greater than 70% for scaling up.	Yes
Scale in	Set conditions like less than 20%.	
Cooldown Period	Set a cooldown period to prevent rapid scaling.	Yes
Instance Details		
Instance Type	Choose Standard_D4S_v4 as the VM size.	

Parameters	Description	Mandatory field
Image	Select the GigaVUE V Series Node image.	
Authentication Type	Choose SSH public key.	
Username	Enter a user name. Do not use admin or gigamon.	
Networking		
Virtual Network	Select the required VNet.	Yes
Subnet Selection	Choose the appropriate subnet for Inline V Series Node.	Yes
NIC Configuration	GigaVUE V Series Node requires two NICs—one for management and one for mirrored data traffic. To configure the Data NIC, add a second network interface, select the appropriate subnet and network security group (NSG), and enable Accelerated Networking.	Yes
Management		

Parameters	Description	Mandatory field
Upgrade Mode	Choose Automatic .	Yes
Advanced		
Custom data and cloud init	Enter the Custom Template modified in step Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config files (/etc/gigamon-cloud.conf and /etc/vseries-inline.conf) and register with GigaVUE-FM using Third Party Orchestration. 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. <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token> - path: /etc/vseries-inline.conf owner: root:root permissions: '0644' content: ""</pre> Custom Data with Internal and External Ports If you have modified the internal and external port values in the Gateway Load Balancer, use the following custom data: <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: </pre>	Yes

Parameters	Description	Mandatory field
	<pre> Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token> - path: /etc/vseries-inline.conf owner: root:root permissions: '0644' content: tunnel: vxlan external_port : <Enter the port value> external_vni : <Enter the port value> internal_port : <Enter the port value> internal_vni : <Enter the port value> </pre>	

Assign VMSS to GWLB Backend Pools

Identify the Gateway Load Balancer you created in [Create a Load Balancer](#) step. To attach the Data NIC of the VMSS to the Gateway Load Balancer:

1. In the Azure portal, navigate to the Gateway Load Balancer you created earlier.
2. From the main page, go to **Settings** and select **Backend Pool**.
3. Locate the Virtual Network (VNet) where your VMSS is deployed.
4. Click **+ Add** under **IP Configuration**.
5. In the pop-up window, search for the Data NIC associated with your VMSS.
6. Select the NIC and click **Add**.
7. Click Save to apply the changes.

Create Monitoring Domain

Azure Load Balancer launches and manages GigaVUE V Series Node that is registered with GigaVUE-FM.

To deploy GigaVUE V Series Node with Gateway Load Balancing in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Monitoring Domain**.
3. On the Monitoring Domain page, select **New**.

4. On the **Monitoring Domain Configuration** page, select **Inline** as the Traffic Acquisition method.
5. Enter the **Monitoring Domain** Name and the **Connection** Name as mentioned in the user data provided during the template launch in Azure. Refer to Advanced section in [Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node \(Tier 1\)](#).
6. (Optional) Turn on the **Use FM to launch Proxy** toggle to launch the GigaVUE V Series Proxy using GigaVUE-FM.

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

- a. From the **Image** drop-down list, select the required image.
 - b. From the **Size** drop-down list, select the instance size.
 - c. For **Number of Instances**, specify the required number of instances.
 - d. For **Management Subnet**:
 - a. Select the **IP Address Type** as Private or Public.
 - b. From the **Subnet** drop-down list, select the management subnet.
 - c. Select **Add Subnet** under **Additional Subnets** to add additional subnets.
 - e. Select **Add** under **Tags** to assign tags for resource identification.
7. Select **Save**.

Deploy GigaVUE V Series Nodes for Inline V Series Solution

When the Monitoring Domain is created successfully you will be navigated to the **Azure Fabric Launch Configuration** page in GigaVUE-FM automatically.

1. From the **Connections** drop-down list, select the required connection that you have configured.



Note:

After configuring the Monitoring Domain and establishing the connection, update the **Default Condition** count in the following steps based on the number of GigaVUE V Series Nodes you want to deploy within the Monitoring Domain:

- [Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node \(Tier 1\)](#)
- (Optional) [Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node \(Tier 2\)](#)



Adjust the instance count in the scale set to match the required number of nodes for your deployment.

2. Select the required resource group from the **Resource Group** drop-down list.
3. From the **Gateway Load Balancer** drop-down list, select the Load Balancer configured in Azure.
4. Under **Node Groups**, you can configure multiple node groups based on the deployment use case.
 - o **Inline Node Group:** This node group is used for the Inline V Series Node that is used for traffic acquisition.
 - a. In the **Inline Node Group Name** field, enter a name for the node group.
 - b. From the **Inline Auto Scaling Group** drop-down list, select the auto scaling group where you deploy the Inline V Series Node.
 - o **(Optional) Node Group:** You can configure this section if you wish to process the traffic using GigaVUE V Series Node. You can add or delete node groups using the + and - buttons.
 - a. In the **Node Group Name** field, enter a name for the node group.
 - b. From the **Auto Scaling Group** drop-down list, select the VMSS created in Azure.
5. Select **Save**.

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

(Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)

The Tier 2 V Series Node (Out-of-Band) processes mirrored traffic using GigaSMART operations to enrich and optimize data before forwarding it to the tool set. If only filtering is required, the Tier 1 V Series Node can handle it and send the traffic directly to the tool—eliminating the need for a Tier 2 node.

The following table lists the specific options you must select when creating a Virtual Machine Scale Set for Out-of-Band for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Virtual Machine Scale Set](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Availability Zones	Choose if you want to use zones for high availability.	No
Orchestration		
Orchestration Mode	Select Uniform as the orchestration mode.	Yes
Security Type	Select Standard mode.	Yes
Scaling		
Scaling Mode	Choose Autoscaling .	Yes
Scaling Configuration	Click Configure to edit the scaling conditions.	Yes
Default Condition	Enter the Initial Instance Count as 0. NOTE: Once the Monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that you need to deploy in this Monitoring Domain.	Yes
Condition	Choose a metric-based scaling condition (For example, CPU usage, network traffic).	Yes
Metric Source	Select the metric (For example, Average CPU Percentage).	Yes
Scale out	Set conditions like greater than 70% for scaling up.	Yes
Scale in	Set conditions like less than 20%.	
Cooldown Period	Set a cooldown period to prevent rapid scaling.	Yes
Instance Details		
Instance Type	Choose Standard_D4S_v4 as the VM size.	Yes
Image	Select the GigaVUE V Series Node image.	Yes
Authentication Type	Choose SSH public key.	Yes
Username	Enter a user name. Do not use admin or gigamon.	Yes
Networking		
Virtual Network	Select the required VNet.	Yes
Subnet Selection	Choose the appropriate subnet for V Series Node.	Yes
NIC Configuration	GigaVUE V Series Node requires two NICs—one for management and one for mirrored data traffic. To configure the Data NIC, add a second network interface, select the appropriate subnet and network security group (NSG), and enable Accelerated Networking.	Yes
Management		

Parameters	Description	Mandatory field
Upgrade Mode	Choose Automatic .	
Advanced		
Custom data and cloud init	Enter the Custom data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config files (/etc/gigamon-cloud.conf) and register with GigaVUE-FM using Third Party Orchestration. 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. <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token></pre>	Yes

Configure Monitoring session

When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default. You can configure up to three tiers in a Monitoring Session and define multiple Sub Policies. Each Sub Policy can have its own ingress and egress tunnels and traffic processing applications.



Notes:

- You can configure a maximum of three tiers in a Monitoring Session.
- Tier 1 supports only Maps. Inline traffic is disabled and reserved for future use.
- You can configure a maximum of 8 Sub Policies in a Monitoring Session.
- Each Sub Policy can have its own Ingress Tunnels, Egress Tunnels, and Applications.
- Traffic from an out-of-band endpoint can either:



- Pass through a Map and send to a tool using an Egress Tunnel.
- (Optional) Send to the GigaVUE V Series Node of the next tier for further processing.

To configure the Monitoring Session for Inline V Series Solution:

Tier 1 Monitoring Session:

1. Perform one of the following options:

- Create a new Monitoring Session. Refer to [Create a Monitoring Session \(Azure\)](#) for details.
- On an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.

The GigaVUE-FM Monitoring Session canvas page appears.

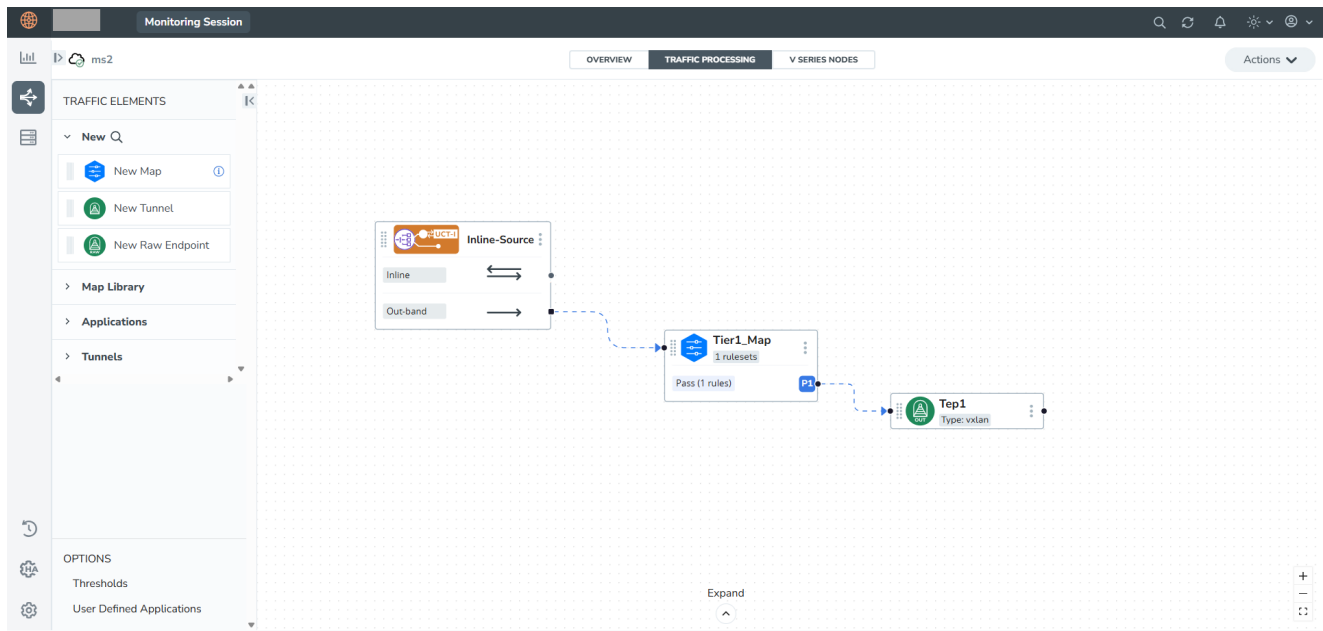
When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default.

2. Drag and drop the following items to the canvas as required for Tier 1 or Sub Policy 1:

- Maps from the **new map** section. Refer to [Create a New Map \(Azure\)](#) for details.
- Egress tunnels from the **new tunnel** section. When configuring Egress Tunnel, configure the **Remote Tunnel IP** if you intend to send the traffic directly from Tier 1 to the tool. Refer to [Create Ingress and Egress Tunnels \(Azure\)](#) for details.

NOTE: If sending traffic to Tier 2, Remote IP is optional. GigaVUE-FM will automatically add the remote IPs internally.

3. Now create a connection between the three tiles by dragging a line from the Inline-Source tile labeled “Out-Band” to the newly created Map and from Map to Egress tunnel.



Deploy Monitoring Session (Tier 1)

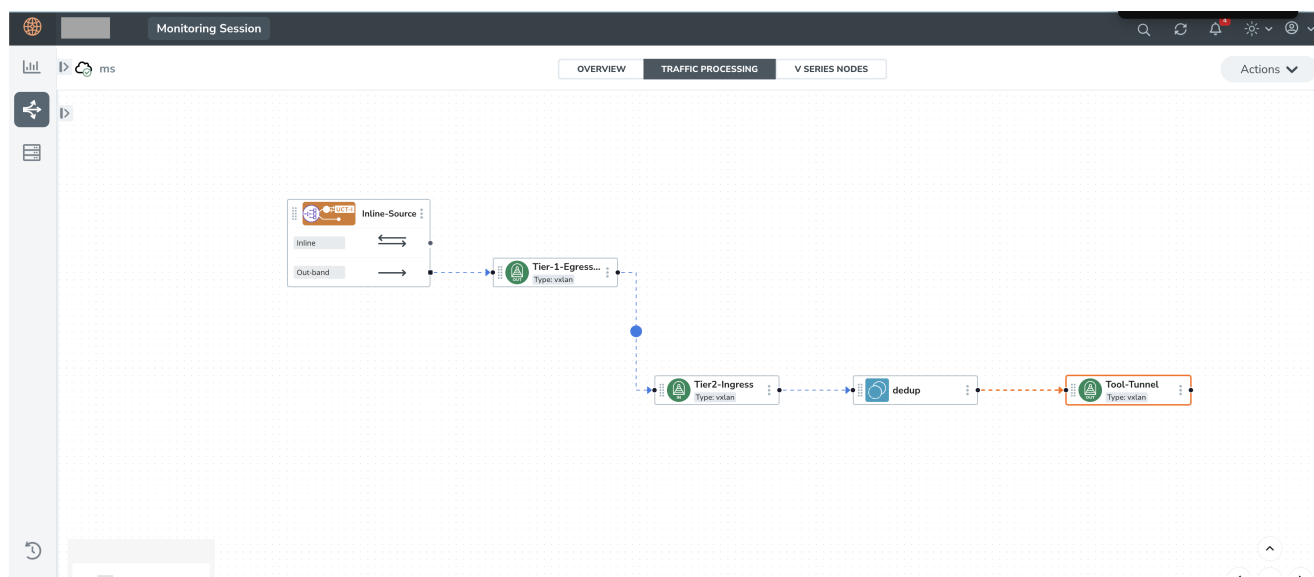
1. From the Actions drop-down list, select **Deploy**. The Deploy Monitoring Session pop-up appears.
2. Enter the following details:
 - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
 - From the **Node Group** drop-down list, select the appropriate node group associated with this policy.
 - Under **Interface Mapping**, configure the interfaces:
 - i. From the **Ingress - <Tunnel>** drop-down list, select the input interface.
 - ii. From the **Egress - <Tunnel>** drop-down list, select the output interface.
3. Select **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

Tier 2 Monitoring Session (Optional):

You can send the filtered traffic to a Tier 2 V Series node, where GigaVUE-FM enriches and optimizes the data further.

1. In the same Monitoring Session canvas, drag and drop the following items to the canvas as required for Tier 2 or Sub Policy 2:
 - Ingress tunnel (as a source) from the **New** section. Refer to [Create Ingress and Egress Tunnels \(Azure\)](#) for details.
 - Maps from the **New Map** section. Refer to [Create a New Map \(Azure\)](#) for details.
 - GigaSMART apps from the Applications section. Refer to [Add Applications to Monitoring Session \(Azure\)](#).
 - Egress tunnels from the **new tunnel** section. Enter the **Remote Tunnel IP** address.
2. Create a link from the Ingress Tunnel to the Map or Application, and then connect it to the Egress Tunnel.
3. Create a direct link between the Egress Tunnel of Tier 1 and the Ingress Tunnel of Tier 2. The Blue Dot serves as an identifier to differentiate between tiers.
4. Repeat the above steps to configure a third tier, if required.



Deploy Monitoring Session Tier 1 to Tier 2

1. From the Actions drop-down list, select **Deploy**.

The Deploy Monitoring Session pop-up appears.

2. For each Policy (Tier) configured in the Monitoring Session, enter the following details:
 - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
 - From the **Node Group** drop-down list, select the appropriate node group associated with this policy.
 - Under **Interface Mapping**, configure the interfaces:
 - i. From the **Ingress - <Tunnel>** drop-down list, select the input interface.
 - ii. From the **Egress - <Tunnel>** drop-down list, select the output interface.
3. Select **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

What to do Next:

To view Monitoring Session Statistics and Dashboards for Inline V Series Solution, refer to:

- [View Monitoring Session Statistics \(Azure\)](#)
- [Analytics for Inline V Series Solution \(Azure\)](#)

Configure Secure Tunnel (Azure)

You can configure secure tunnels for:

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

Precrypted Traffic

You can send the precrypted traffic through a secure tunnel. When secure tunnels for Precryption is enabled,

- Packets are framed and sent to the TLS socket.
- The packets are sent in PCAPng format.
- When you enable the secure tunnel option for regular and precrypted packets, two TLS secure tunnel sessions are created.

We recommend to enable secure tunnels for precrypted traffic to securely transfer the sensitive information.

Mirrored Traffic

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

Refer to the following sections for Secure Tunnel Configuration:

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

Prerequisites

- Enable Port 11443 in security group settings. For details, refer to [Network Security Groups](#).
- While creating Secure Tunnel, you must provide the following details:
 - SSH key pair
 - CA Certificate chain

Notes

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

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

To configure a secure tunnel in UCT-V, you must configure one end of the tunnel to the UCT-V and the other end to GigaVUE V Series Node. You must configure the CA Certificate chain 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 CA Certificate chain in a single file	You must upload a CA Certificate chain to UCT-V Controller to establish a connection with the GigaVUE V Series Node. To upload the CA Certificate chain using GigaVUE-FM, follow the steps given below: 1. Go to Inventory > Resources > Security > CA List. 2. Select New to add a new 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. NOTE: Ensure that the Intermediate CA Certificate(s) are included in the CA certificate chain file in the correct signing order, followed by the Root CA Certificate at the end. For more information, refer to the section Adding Certificate Authority
2	Upload an SSL Key Pair	You must add an SSL key pair to the GigaVUE V Series Node. Follow the steps in the section SSL Decrypt.

S. No	Task	Refer to
3	Select the SSL Key Pair while creating a monitoring domain and configuring the fabric components in GigaVUE-FM.	You must select the added SSL Key Pair in the GigaVUE V Series Node while creating a monitoring domain configuring the fabric components in GigaVUE-FM. To select the SSL key pair, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM. If the existing monitoring domain does not have a SSL key pair, you can add it by following the given steps: 1. Select the monitoring domain for which you want to add the SSL key pair. 2. Select Actions> Edit SSL Configuration. An Edit SSL Configuration window appears. 3. Select the CA Certificate chain in the UCT-V Agent Tunnel CA drop down list. 4. Select the SSL key pair in the V Series Node SSL key drop down list. 5. Select Save.
4	Select CA Certificate chain while creating the monitoring domain configuring the fabric components in GigaVUE-FM.	You should select the added CA Certificate chain in UCT-V Controller. To select the CA Certificate chain, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM .
5	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, follow these steps: 1. In the Edit Monitoring Session page, click Options. The Apply template page appears. 2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic. Note: When GigaVUE V Series Node is upgraded or deployed to 6.5, all the existing monitoring sessions will be redeployed, and individual TLS TEPs are created for each UCT-V.

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 CA Certificate chain in a single file	You must upload a CA Certificate chain to UCT-V Controller to establish a connection between the GigaVUE V Series Node. To upload the CA Certificate chain using GigaVUE-FM follow the steps given below: 1. Go to Inventory > Resources > Security > CA List. 2. Select Add, to add a new CA Certificate chain. The Add Certificate 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. 5. Select Deploy All. NOTE: Ensure that the Intermediate CA Certificate(s) are included in the CA certificate chain file in the correct signing order, followed by the Root CA Certificate at the end. For more information, refer to the section Adding Certificate Authority
2.	Upload an SSL Key Pair	You must add an SSL key pair to GigaVUE V Series Node. Follow the steps in the section Upload SSL Keys.
3	Select the added SSL Key Pair while creating a Monitoring Domain.	Select the added SSL Key Pair while creating a Monitoring Domain and configuring the fabric components in GigaVUE-FM in the first GigaVUE V Series Node . You must select the added SSL Key Pair for the first GigaVUE V Series Node. To select the SSL key pair, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM
4	Select the added CA Certificate chain while creating the Monitoring Domain	You should select the added CA Certificate chain in UCT-V Controller. To select the CA Certificate chain, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM

S. No	Task	Refer to
5	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 Apply template page appears. 2. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and precrypted traffic.
6	Create an Egress tunnel from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG in 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 in the Monitoring Session. For details, refer to Create Ingress and Egress Tunnels (Azure). To create the egress tunnel, follow these steps: 1. After creating a new monitoring session, or click Actions > Edit on an existing monitoring session, the GigaVUE-FM canvas appears. 2. In the canvas, select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears. 3. On the New Tunnel quick view, enter or select the required information as described in the following table: • Alias - The name of the tunnel endpoint. • Description -The description of the tunnel endpoint. • Type - Select TLS-PCAPNG for creating egress secure tunnel

S. No	Task	Refer to
		- Traffic Direction- Choose Out (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: - MTU- The default value is 1500 for Azure. Note: - Time to Live: Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64. - DSCP: Enter the Differentiated Services Code Point (DSCP) value. - Flow Label: Enter the Flow Label value. - Source L4 Port: Enter the Source L4 Port value - Destination L4 Port: Enter the Destination L4 Port value. - Flow Label - Cipher: Only SHA 256 is supported. - TLS Version: Select TLS Version1.3. - Selective Acknowledgments: Choose Enable to turn on the TCP selective acknowledgments. - SYN Retries: Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6. - Delay Acknowledgments: Choose Enable to turn on delayed acknowledgments. - 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 Cloud Suite V Series Node (Destination IP). 4. Select Save.
7.	Select the added SSL Key Pair while creating a Monitoring Domain and configuring the fabric components in GigaVUE-FM in second GigaVUE V Series Node	You must select the added SSL Key Pair in second GigaVUE V Series Node. To select the SSL key pair, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM
8	Create an ingress tunnel for the second GigaVUE V Series Node with tunnel type as TLS-PCAPNG in the Monitoring Session	You must create a ingress tunnel for traffic to flow in from the GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the monitoring session. For details, refer to Create a Monitoring Session (Azure). To create the ingress tunnel, follow these steps:

S. No	Task	Refer to
		1. After creating a new monitoring session, or select 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. Note: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above. • Traffic Direction - Choose In (Decapsulation) for creating an ingress tunnel that receives traffic from 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 Cloud Suite 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 >** , and then select **Monitoring Domain**.
2. In the **Monitoring Domain** page, view the status.

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

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

Create Prefiltering Policy Template

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, refer to [Configure Monitoring Session Options \(Azure\)](#).

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 \(Azure\)](#) section.

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

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

Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnels, maps, and applications in a Monitoring Session to receive and send traffic to the GigaVUE Cloud Suite V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools.

Refer to the following sections for details:

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

Create a Monitoring Session (Azure)

You must create a Monitoring Domain before creating a Monitoring Session. Refer to [Create Monitoring Domain](#).

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 (Azure)

The following table outlines the functional tabs available on the Azure Monitoring Session page, each designed to support specific aspects of network monitoring and 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 (Azure) .
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view

Tab	Description
	and filter the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. In the Selection Status section, you can view the VM status. The status indicates whether the VM is supported, not supported, selected, or not selected. When you hover over the status, a tooltip displays the reason for that status. NOTE: In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Acquisition	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create a Prefiltering and Precryption templates and apply them to the Monitoring Session. Refer to Configure Monitoring Session Options (Azure) . Note: Traffic Acquisition is only applicable for Monitoring Domain created with UCT-V as Acquisition method.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold templates, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options (Azure).
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 Node name, Health status (Configuration health + Traffic health), Host VPC, Management IP and Deployment Failure Message (if applicable). You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping (Azure).
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 (Azure).

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

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

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

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

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

Configure Monitoring Session Options (Azure)

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

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

TRAFFIC ACQUISITION

To navigate to **TRAFFIC ACQUISITION** tab,

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

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

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

Enable Prefiltering

To enable Prefiltering:

1. In the **TRAFFIC ACQUISITION** page, go to **Mirroring > Edit Mirroring**.
2. Enable the **Mirroring** toggle button.
3. Enable **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.

4. Select an existing Prefiltering template from the **Template** drop-down menu, or create a new template using **Add Rule** option and apply it. For details, refer to [Create Prefiltering Policy Template](#).
5. Select the **Save as Template** to save the newly created template.
6. Select **Save** to apply the template to the Monitoring Session.

Enable Precryption

Consideration before you enable Precryption:

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

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

To enable Precryption:

1. In the **TRAFFIC ACQUISITION** page, select **Precryption** tab and click **Edit Precryption**.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic in the respective cloud guides for details.

3. Apply Precryption to a few selective components based on the traffic:

NOTE: If you wish to use Selective Precryption, ensure that the versions of GigaVUE-FM and the fabric components are 6.8.00 or above.

Applications:

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

L3-L4

You can select an existing Precryption template from the **Template** drop-down list, or you can create a new template and apply it. For details, refer to [Create Precryption Template for UCT-V](#).

4. Enable the **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.

Validate Precryption connection

To validate the Precryption connection, follow the steps:

- To confirm it is active, navigate to the Monitoring Session **Overview** tab and check the Traffic Acquisition Options.
- Select **Precryption**, to view the rules configured.

Limitations

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

TRAFFIC PROCESSING

To navigate to **TRAFFIC PROCESSING** tab:

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

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

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

Apply Threshold Template

To apply threshold:

1. In the **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. You can select an existing threshold template from the **Select Template** drop-down list, or you can create a new template using **New Threshold Template** option and apply it.
For more details on Threshold Template, refer to the [Traffic Health Monitoring](#) section.
3. Select **Save** to save the newly created template.
4. Select **Apply** to apply the template to the Monitoring Session.

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

You can also view the related details of the applied thresholds, such as Traffic Element, Metric, Type, Trigger Values, and Time Interval in the **Threshold** window. Select **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

To enable user defined application:

1. In the **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.

3. Add from the existing applications or create new User-Defined Application from the **Actions** drop-down. Refer to [User Defined Application](#).

Enable Distributed De-duplication

In the TRAFFIC PROCESSING page, click **Distributed De-duplication** under **Options** menu. Enabling the Distributed De-duplication option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Refer to [Distributed De-duplication](#).



Notes:

- Distributed De-duplication is only supported on V Series version 6.5.00 and later.
- From version 6.9.00, Traffic Distribution option is renamed to Distributed De-duplication.

Tool Exclusion

Tool Exclusion helps prevent traffic loops by ensuring monitoring tools are not mistakenly selected as traffic targets during Automatic Target Selection (ATS). This feature is available only when the traffic acquisition method is VPC Traffic Mirroring.

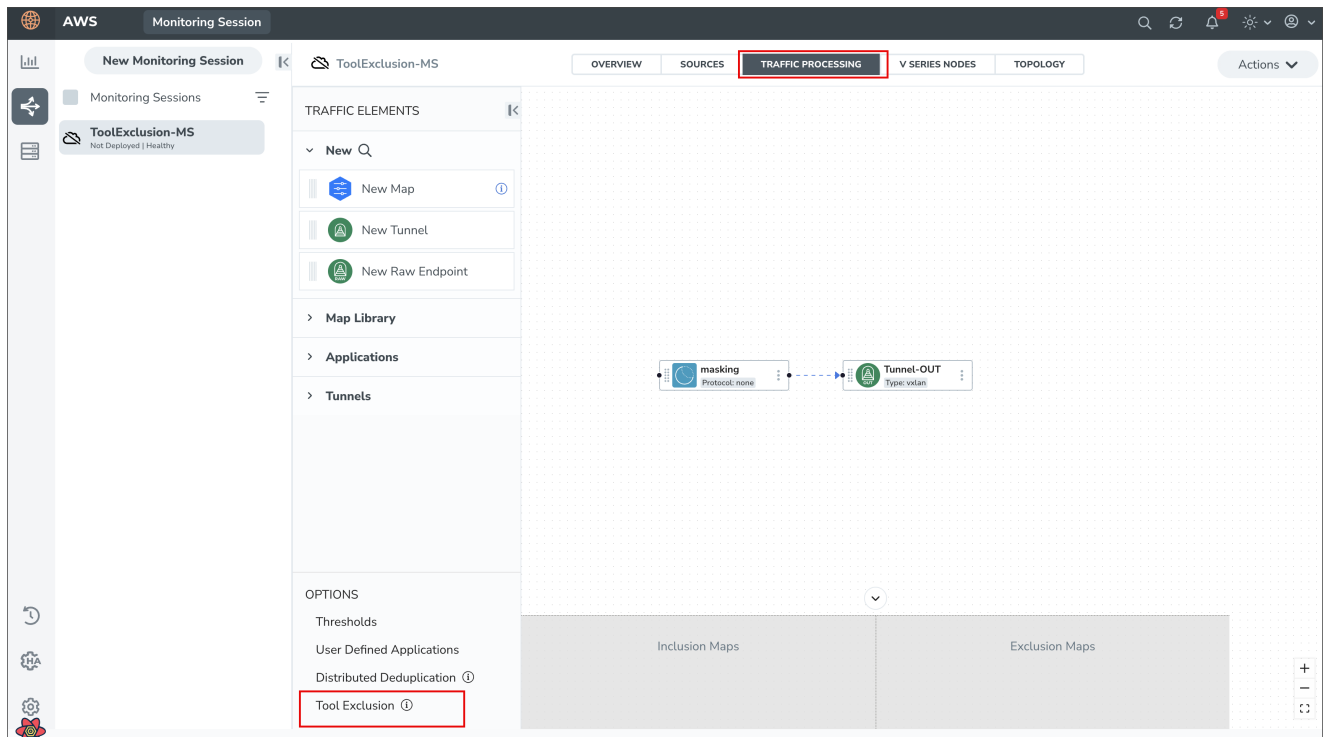
You can exclude tool instances using either of the following methods:

1. Using AWS Tag Key

During deployment, apply the AWS tag key **GigamonExclude:Value** (Any Value) to any instance that acts as a monitoring tool. This tag ensures the system automatically excludes these instances from ATS.

2. Using the Tool Exclusion Feature in UI

During deployment, if the same instance IP is configured as both source (ingress) and tool (egress), the system prompts you to manually identify and exclude tools. Also, you can use the **Tool Exclusion** option to include or exclude tools and targets manually.



Create Ingress and Egress Tunnels (Azure)

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

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**.

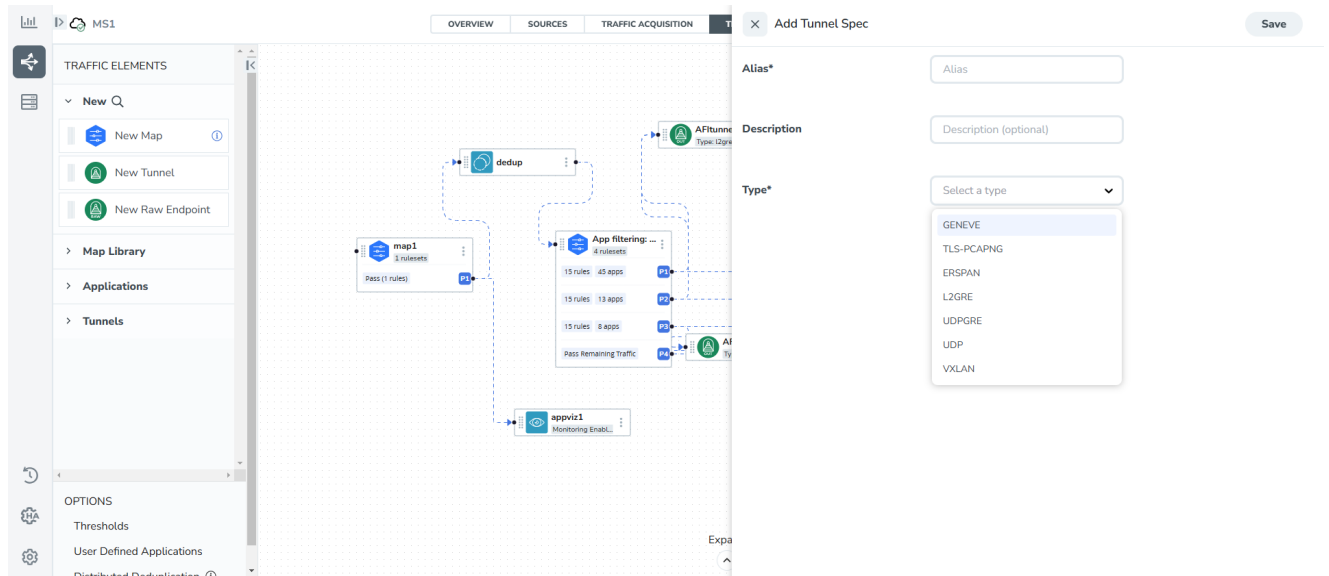


Table 1: Details - Add Tunnel Specifications

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

Field	Description	
	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.
	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. Applicable Platforms: OpenStack, Third Party Orchestration, VMware ESXi  Notes: You can configure either a single-tap or multi-tap setup for the egress tunnel. Switching between these configurations is

Field	Description	
		 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. 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

Field	Description	
		target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to the Secure Tunnels .		
In	Choose In (decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP/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.
	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

Field	Description	
		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 (Azure)

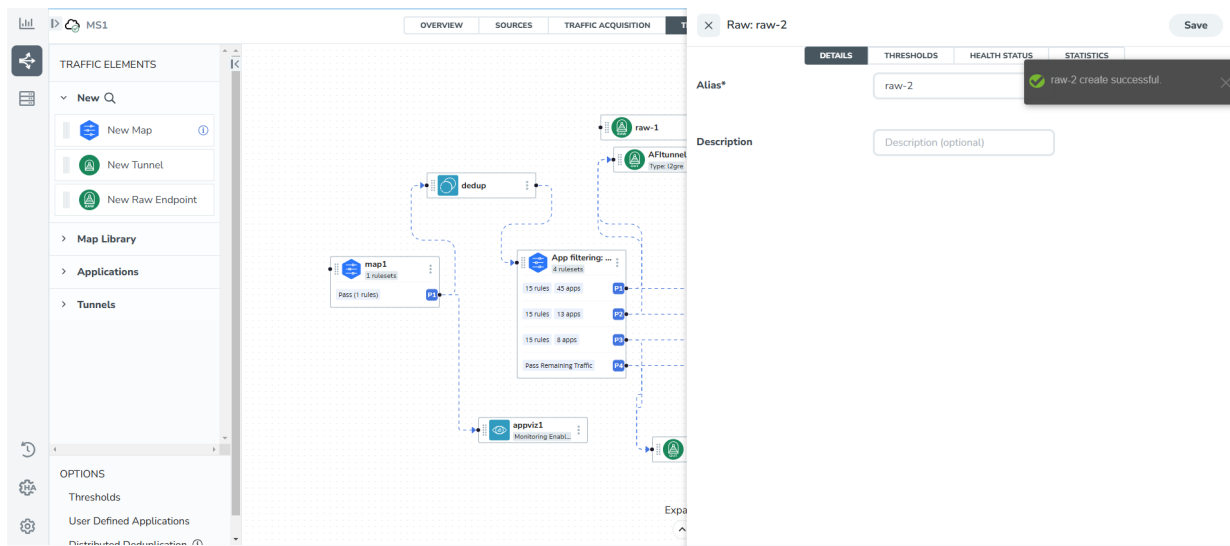
Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the Monitoring Session.

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.

- Enter the Alias and Description details for the Raw End Point and click **Save**.



- To deploy the Monitoring Session after adding the Raw Endpoint:
 - Select **Deploy** from the **Actions** drop-down list on the **TRAFFIC PROCESSING** page. The **Deploy Monitoring Session** dialog box appears.
 - Select the V Series Nodes for which you wish to deploy the Monitoring Session.
 - 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.
 - Select **Deploy**.
- Select **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map (Azure)

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 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.

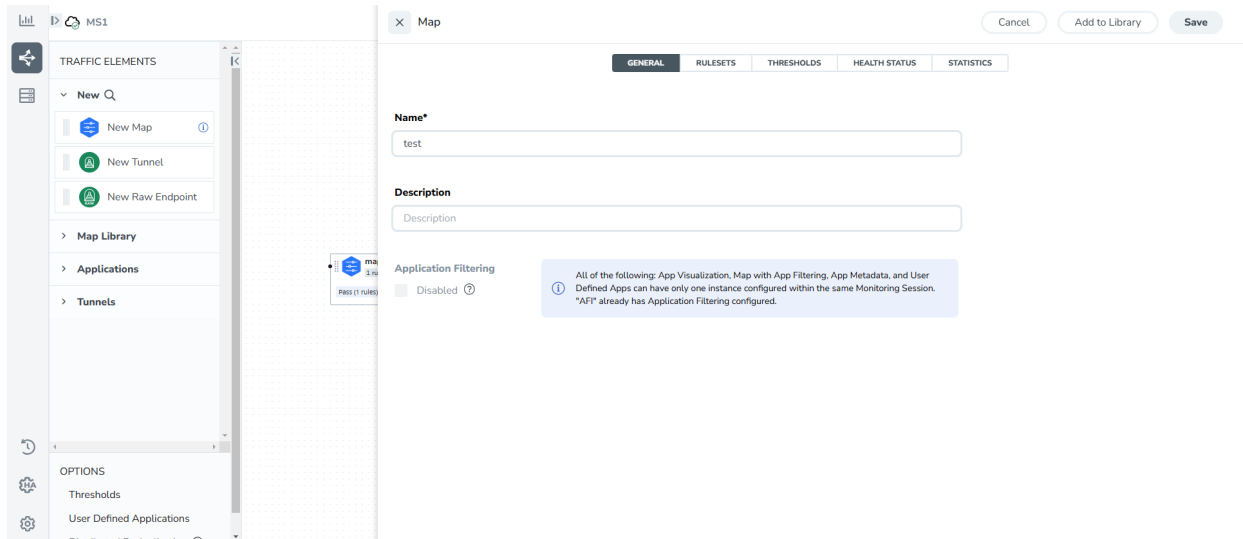
Rules and Notes:

- 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 (Azure)

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

Interface Mapping (Azure)

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.

Deploy Monitoring Session (Azure)

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

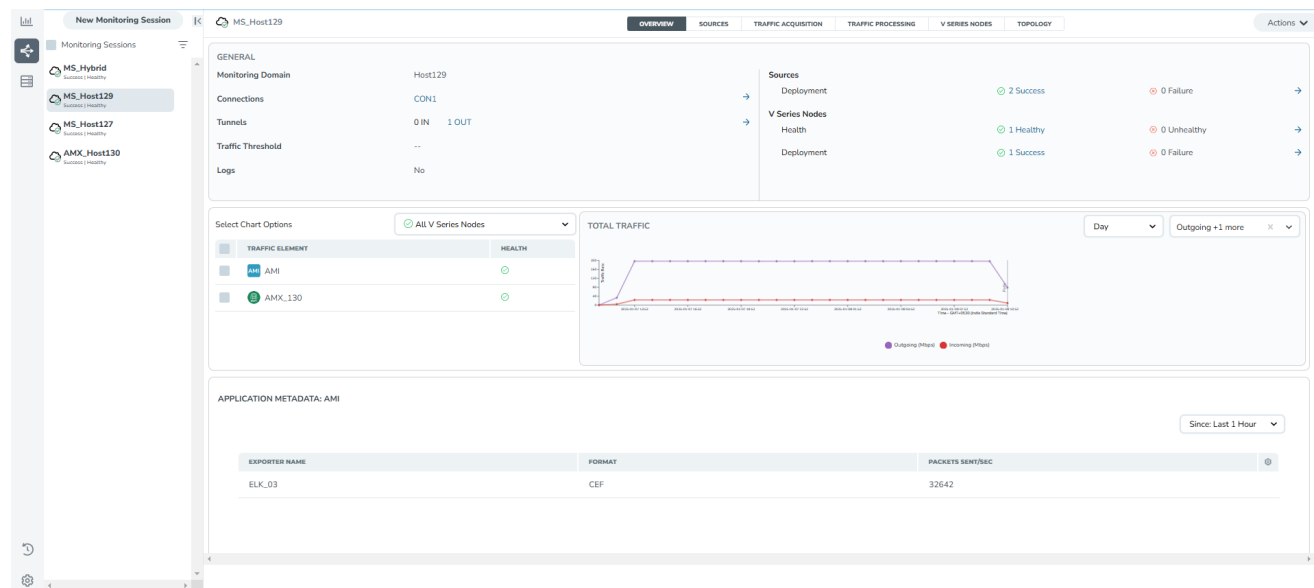
Cancel Deploy

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

View Monitoring Session Statistics (Azure)

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.

View FQDN resolution details

Use the **FQDN tab** under the **V SERIES NODES tab** to view the FQDNs configured for supported egress tunnel destinations in the monitoring session. This tab displays the configured FQDN, the current resolution status, and the IP address to which the FQDN currently resolves.

- Use this tab to verify that the system resolved the configured FQDN and to identify DNS resolution issues.
- If the system resolves the FQDN successfully, the status shows OK and the Resolve IP field displays the mapped IP address.
- If the system cannot resolve the FQDN, the status shows Failed and the Resolve IP field displays 0.0.0.0.

The screenshot displays the 'V SERIES NODES' tab in the GigaVUE Cloud Suite interface. A red box highlights the 'FQDN' sub-tab within the 'Details' section for a specific V Series Node. Below this, a table lists the configured FQDNs and their resolution status.

FQDN	STATUS	RESOLVE IP	NOTE
sslqa1.com	Resolved	22.0.3.110	—
sslqa2.com	Resolved	2600:1f14:388a:9c01:b477:c431...	—
sslqa3.com	Resolved	22.0.3.250	—

Visualize the Network Topology (Azure)

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.

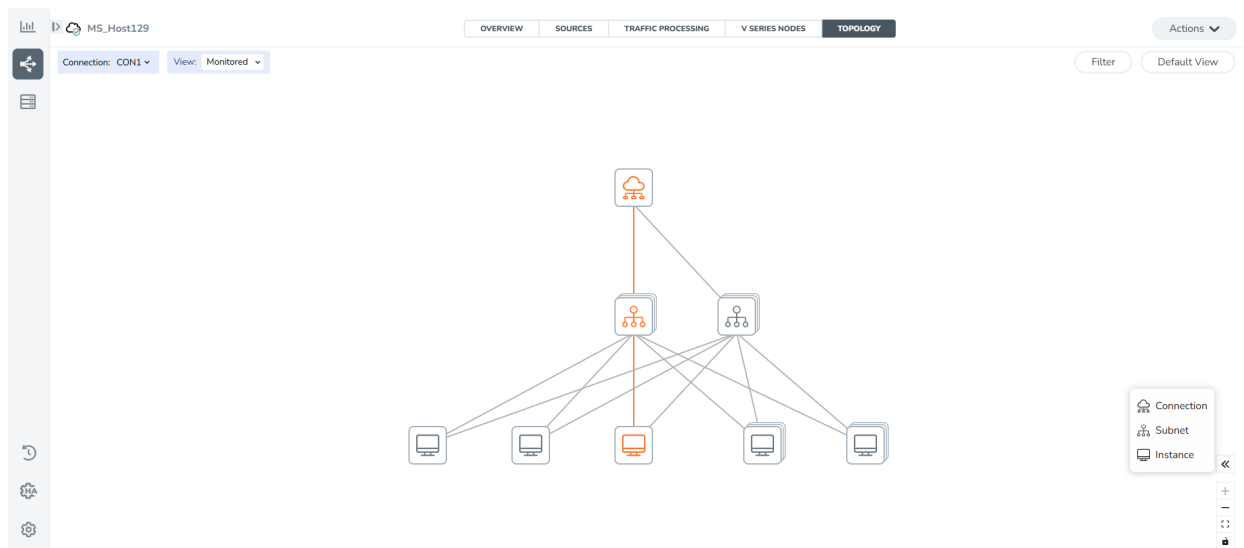
To view the topology in GigaVUE-FM:

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.

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.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, you must configure the Application Intelligence solution from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for a virtual environment from the **Application Intelligence** page.

The following actions are available only when using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

We recommend to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM seamlessly migrates all your virtual Application Intelligence sessions and their connections. If migration fails, all sessions return to their original states.



Points to Note:

- You must have write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. For details, refer to Create Roles section In GigaVUE Administration Guide



- The migration does not proceed:
 - If any of the existing Application Intelligence Session is in PENDING or SUSPENDED. Resolve the issue and start the migration process.
 - If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration. Resolve the issue and start the migration process.
 - If an existing Monitoring Session has the same name as the Application Intelligence Session. Change the existing Monitoring Session name to continue with the migration process.
- You cannot continue the session if any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set. In the Monitoring Session, the fifth Rule Set supports either Pass All or Advanced Rules as Drop. Delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for assistance.

Migrate your existing Application Intelligence Session to Monitoring Session Page

Follow these steps:

1. In the left navigation pane, select **Traffic > Solutions > Application Intelligence**. You cannot create a new Application Intelligence Session from this page. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
2. Review the message and select **Migrate**. The **Confirm Migration** dialog box appears with the list of Application Intelligence Session that you need to migrate.
3. Review the list and select **Migrate**. GigaVUE-FM verifies the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
4. Select **Go to Monitoring Session Page**.

You can view that all the virtual Application Intelligence Sessions in the Application Intelligence page are migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

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

1. **Secure Tunnels in the Options page** If you wish to enable Secure tunnels after migrating the Session, follow these steps:
 - a. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
 - b. Select a Monitoring Session from the Monitoring Sessions list view on the left pane and select the **TRAFFIC ACQUISITION** tab.
 - c. Enable **Secure tunnels**. For information about how to enable secure tunnel for a Monitoring Session, refer to the *Configure Monitoring Session Options* topic in the respective GigaVUE Cloud Suite Deployment Guide.
 - d. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
 - e. From the **Monitoring Sessions** page, select the Monitoring Session for which you enabled Secure Tunnels.
 - f. Select **Actions > Undeploy**. The Monitoring Session is undeployed.
 - g. Select the Monitoring Session for which you enabled Secure Tunnels and edit the Monitoring Session.
 - h. Add the Application Intelligence applications.
 - i. Modify the Number of Flows as per the below table.

Cloud Platform	Instance Size	Maximum Number of Flows
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k

- Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k..
 - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.
- j. Select **Deploy**. For details on how to deploy, refer to Application Intelligence section in the GigaVUE V Series Applications Guide.

2. Temporary Loss of Statistics with Version Mismatch

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

3. Configuration Changes Post-Migration

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

Monitor Cloud Health

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

- [Configuration Health Monitoring](#)
- [Traffic Health Monitoring](#)
- [View Health Status](#)

Configuration Health Monitoring

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

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

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

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

Traffic Health Monitoring

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

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

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. 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*.

This feature supports GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Third Party Orchestration

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

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

Consideration to configure a threshold template

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

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

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring. 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 9. Workload - Records Dropped 10. Workload - Req Auth Errors 11. Workload - Req Timedout Errors 12. Workload - Req Errors 13. Exporter - Avg File Size	1. Difference 2. Derivative	1. Over 2. Under

	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 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
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
EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED	The exporter health-monitor probe or upload to the tool timed out. Example: CLOUDEXPORTER_EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED KAFKA_EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED
EXPORTER_ERR_EVENT_CONTEXT_CANCELED	The exporter health-monitor probe or upload was canceled before completion, typically due to shutdown or reconfiguration. Example: CLOUDEXPORTER_EXPORTER_ERR_EVENT_CONTEXT_CANCELED KAFKA_EXPORTER_ERR_EVENT_CONTEXT_CANCELED

Message	Description
EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL	The hostname of the configured Kafka broker or Cloud Exporter endpoint could not be resolved due to a DNS failure. Example: CLOUDEXPORTER_EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL KAFKA_EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL
EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE	The exporter probe failed at the network layer, for example, due to no route to the host or an unreachable network. Example: CLOUDEXPORTER_EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE KAFKA_EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE
EXPORTER_ERR_EVENT_TRANSPORT_LAYER_ERR	The exporter probe failed at the transport layer, such as connection refusal, TCP reset, or TLS handshake failure. Example: CLOUDEXPORTER_EXPORTER_ERR_EVENT_TRANSPORT_LAYER_ERR KAFKA_EXPORTER_ERR_EVENT_TRANSPORT_LAYER_ERR

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.

Administer GigaVUE Cloud Suite for Azure

You can perform the following administrative tasks:

- [Configure Certificate Settings](#)
- [Set Up Email Notifications](#)
- [Configure Proxy Server](#)
- [Configure Azure Settings](#)
- [Role Based Access Control](#)
- [About Events](#)
- [About Audit Logs](#)

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**.

Set Up Email Notifications

A range of events such as Azure license expiry and VM instance terminated trigger Notifications. You can set up the email notification for a particular event or a number of events and the recipient or recipients to whom the email should be sent.

Gigamon recommends to enable email notifications. It provides immediate visibility of the events affecting node health.

You can setup the email notifications the following events:

- Azure License Expire
- Fabric Node Down
- Fabric Node Reboot Failed
- Fabric Node Rebooted
- Fabric Node Replacement Launch Failed
- Fabric Node Replacement Launched
- Fabric Node Restart Failed
- Fabric Node Restarted
- Fabric Node Unreachable
- Fabric Node Up

Configure Email Notifications

To configure the automatic email notifications,

1. On the left pane, select **System > Event Notifications > Email Servers**.

2. On the **Email Servers** page, select **Configure**.
The **Configure Email Server** wizard appears. For field information, refer to "Email Servers" section in the *GigaVUE Administration Guide*.

Configure Email Server

Save

Cancel

Enable SMTP Authentication

☐

Email Host

10.10.1.125

Username

Username

Password

Password

From Email

no-reply@gigavue-fm

Port

25

3. Select **Save**.

Configure Proxy Server

GigaVUE-FM cannot reach Azure API endpoints If the virtual network (VNet) hosting GigaVUE-FM does not have internet access. To enable connectivity, you must configure a proxy server.

To create a proxy server,

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Proxy Server Configuration**.
3. In the **Proxy Server Configuration** page, select **Add**.

The **Configure Proxy Server** page appears.

Configure Proxy Server

SaveCancel

Alias	Alias
Host	IP Address
Port	0 - 65535
Username	Username
Password	Password

☐ NTLM

4. Select or enter the appropriate information for the following fields.
 - a. **Alias:** The name of the proxy server.
 - b. **Host:** The host name or the IP address of the proxy server.
 - c. **Port:** The port number that the proxy server uses for Internet connection.
 - d. **Username:** (Optional) The username of the proxy server.
 - e. **Password:** The password of the proxy server.
 - f. **NTLM:** (Optional) The type of the proxy server used to connect to the VNet.
 - g. **Domain:** The domain name of the client accessing the proxy server.
 - h. **Workstation:** (Optional) The name of the workstation or the computer accessing the proxy server.
5. Select **Save**.

GigaVUE-FM adds the new proxy server configuration to the Proxy Server Configuration page. The proxy server is also listed in the Azure Connection page.

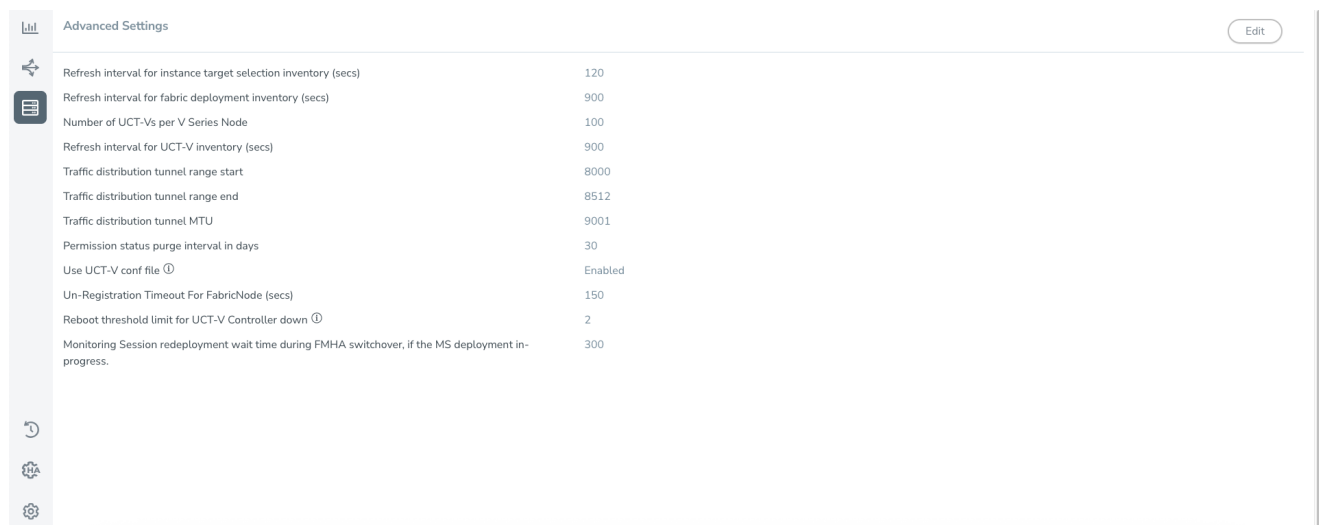
NOTE: If you change any of the fields in the Proxy Server Configuration page after the initial connection is established between the GigaVUE-FM and Azure, then you must also edit the connection and select the proxy server again and save (in the Azure Connection Page). Otherwise, GigaVUE-FM does not use the new saved configuration that was saved, and may lose connectivity to the Azure platform.

Configure Azure Settings

This section provides information on how to customize Azure-related settings in GigaVUE-FM to control refresh intervals, connection limits, tunnel ranges, and UCT-V behavior.

Access Advanced Azure Settings

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Advanced Settings**.



Advanced Settings		Edit
Refresh interval for instance target selection inventory (secs)	120	
Refresh interval for fabric deployment inventory (secs)	900	
Number of UCT-Vs per V Series Node	100	
Refresh interval for UCT-V inventory (secs)	900	
Traffic distribution tunnel range start	8000	
Traffic distribution tunnel range end	8512	
Traffic distribution tunnel MTU	9001	
Permission status purge interval in days	30	
Use UCT-V conf file ⓘ	Enabled	
Un-Registration Timeout For FabricNode (secs)	150	
Reboot threshold limit for UCT-V Controller down ⓘ	2	
Monitoring Session redeployment wait time during FMHA switchover, if the MS deployment in-progress.	300	

The page displays the configuration listed below.

Settings	Description
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the state of Virtual Machines target selection in Azure.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the state of fabric deployment information such as subnets, security groups, images, and VNets.
Number of UCT-Vs	Specifies the maximum number of instances that you can assign to the GigaVUE V

Settings	Description
per GigaVUE V Series Node	Series node.
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available in the VNet. 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.
Traffic distribution tunnel MTU	Specifies the MTU value for the traffic distribution tunnel.
Permissions status purge interval in days	Specifies the number of days GigaVUE-FM retains permissions report before auto purging.
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, create a new Monitoring Domain and configure the Monitoring Session. - When changing the UCT-V conf file option from disabled to enabled, perform 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
Un-Registration Timeout For FabricNode (secs)	Specify the unregistration wait time between 150 to 900 seconds to control how long GigaVUE-FM waits before removing an unhealthy node; the default is 150 seconds.
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 the down state. GigaVUE-FM retries every 60 seconds.

Role Based Access Control

The Role Based Access Control (RBAC) feature controls the access privileges of users and restricts users from either modifying or viewing unauthorized data. Access privileges in GigaVUE Cloud Suite works on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depends on the following:

- **User role:** A user role defines permission for users to perform any task or operation
- **User group:** A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more groups.

To access the resources and to perform a specific operation in GigaVUE Cloud Suite you must be a user with **fm_super_admin** role or a user with write access to the following resource category depending on the task you need to perform.

Resource Category	Cloud Configuration Task
Physical Device Infrastructure Management: This includes the following cloud infrastructure resources: • Cloud Connections • Cloud Proxy Server • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory	• Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric • Configure Proxy Server
Traffic Control Management: This includes the following traffic control resources: • Monitoring session • Threshold Template • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Create and Apply Threshold Template • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points
Third Party Orchestration: This includes the following resource: • Cloud Orchestration	Deploy the fabric components using Third Party Orchestration. Refer to Configure Role-Based Access for Third Party Orchestration for more details on how to create users, roles, and user groups for Third Party Orchestration.

NOTE: Cloud APIs are also RBAC enabled.

Refer to the *GigaVUE Administration Guide* for detailed information about Roles, Tags, User Groups.

About Events

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

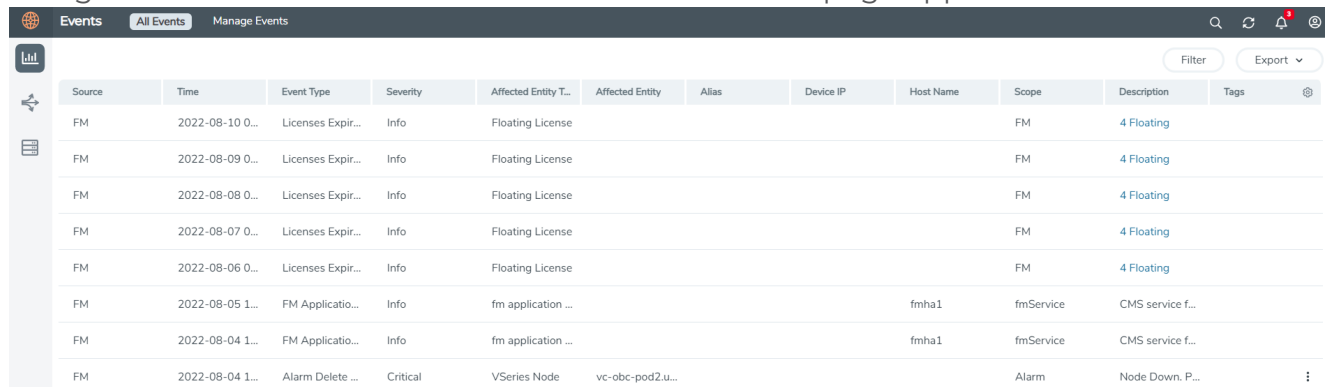
- Cloud provider License Expiry
- UCT-V Inventory Update Completed
- Cloud provider Connection Status Changed

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

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

Access Event

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



Source	Time	Event Type	Severity	Affected Entity T...	Affected Entity	Alias	Device IP	Host Name	Scope	Description	Tags	
FM	2022-08-10 0...	Licenses Expir...	Info	Floating License					FM	4 Floating		
FM	2022-08-09 0...	Licenses Expir...	Info	Floating License					FM	4 Floating		
FM	2022-08-08 0...	Licenses Expir...	Info	Floating License					FM	4 Floating		
FM	2022-08-07 0...	Licenses Expir...	Info	Floating License					FM	4 Floating		
FM	2022-08-06 0...	Licenses Expir...	Info	Floating License					FM	4 Floating		
FM	2022-08-05 1...	FM Applicatio...	Info	fm application ...				fmha1	fmService	CMS service f...		
FM	2022-08-04 1...	FM Applicatio...	Info	fm application ...				fmha1	fmService	CMS service f...		
FM	2022-08-04 1...	Alarm Delete ...	Critical	VSeries Node	vc-obc-pod2.u...				Alarm	Node Down. P...		

The following table describes the parameters recording for each alarm or event. You can also use filters to narrow down the results.

Controls/ Parameters	Description
Source	The source from where the events are generated. The criteria are: ■ FM - indicates the event that the GigaVUE-FM fabric manager flagged. ■ VMM - indicates the event that the Virtual Machine Manager flagged. ■ FM Health - indicates the event that the health status change of GigaVUE-FM flagged.
Duration	The timestamp when the event occurred or the duration of the event. IMPORTANT: Timestamps or the duration appear in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
Scope	The category to which the events belong. Events can belong to the following categories: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if an event generates a notification for port utilization low threshold, the scope is displayed as Physical Node.
Alarm Type	The type of events that generates the alarms. The types of alarms are Abnormal Fan Operation, Card Unhealthy, Circuit Tunnel Unhealthy, CPU Over Loaded, Device Upgrade Failed.
Event Severity	The severity is one of Critical, Major, Minor, Warning, or Info. Info is informational messages. For example, when a power status change notification is displayed, the message is Info.
Event Status	The status of the event. The status is either Acknowledged or Unacknowledged.
Event Type	The type of event that generated the events. The types of events are CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow generation statistics, and so on.
Affected Entity Type	The resource type associated with the event. For example, when a low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Cluster ID	Enter the Cluster ID.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Device IP	The IP address of the device.
Host Name	The host name of the device.
Alias	Event Alias
Monitoring Domain	The name of the Monitoring Domain.
Connection	The name of the Connection.
Show Non-taggable Entities	Enable to display the events for entities that you cannot tag. For example, Policies, GigaVUE-FM instance, and other such entities.
Tags	Select the Key and the Value from the drop-down list.

To filter the alarms and events,

1. Select **Filter**.

The Filter quick view is displayed.

2. Select the filtering criteria, and then select **Apply Filter**.

The result appears on the Events page.

About Audit Logs

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

Access Audit Logs

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

All Audit Logs Filter Manage

Filter : none

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

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics¹, you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You

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

can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. For details, refer to the [Analytics](#) section in *GigaVUE Fabric Management Guide*.

Rules and Notes:

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations.

For details, refer to the [Clone Dashboard](#) section in GigaVUE-FM Installation and Upgrade Guide

- Use the Time Filter option to select the required time interval for which you need to view the visualization.

Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. For details on dashboard and visualization about the Discover page and Reports page. refer to the [Analytics](#) section in *GigaVUE Fabric Management Guide*.

To access the dashboards,

- Go to  -> **Analytics -> Dashboards.**
- Select the required dashboard to view the visualizations.

The following table lists the various virtual dashboards:

Dashboard	Displays	Visualizations	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: - Number of Monitoring Sessions - Number of V Series Nodes - Number of Connections - Number of GCB Nodes You can filter the visualizations based on the following control filters: - Platform - Health Status	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy GigaVUE V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms

Dashboard	Displays	Visualizations	Displays
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: - Platform - Connection - V Series Node	<i>V Series Node Maximum CPU Usage Trend</i>	Line chart that displays maximum CPU usage trend of the GigaVUE V Series Node in 5 minutes interval, for the past one hour. NOTE: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	Line chart that displays Maximum CPU usage of the GigaVUE V Series Node for the past 5 minutes. NOTE: You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Rx Trend</i>	Receiving trend of the GigaVUE V Series Node in 5 minutes interval, for the past one hour.
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	Total packets received by each of the GigaVUE V Series Node

Dashboard	Displays	Visualizations	Displays
			network interface for the past 5 minutes. NOTE: You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Tunnel Rx Packets/Errors</i>	Displays the reception of packet at the Tunnel RX. This is the input to GigaVUE V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, GigaVUE V Series Node, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from GigaVUE V Series Node. GigaVUE V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: - Platform - Connection - V Series Node	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the de-duplicated packets received against the de-duplication application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following	<i>Tunnel Bytes</i>	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.

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

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

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

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

Analytics for Inline V Series Solution (Azure)

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

Analytics support is available for the following cloud platforms:

- AWS
- Azure

To access the dashboards:

1. From the left navigation pane, go to  -> **Analytics -> Dashboards.**
2. Navigate to **System Dashboards -> Inline.**
3. From the **Load Balancer** drop-down list, select the Gateway load Balancer configured in AWS.
4. From the **Monitoring Session** drop-down list, select the Monitoring Session in which Inline V Series solution is configured.
5. From the **Node Name** drop-down list, select the GigaVUE V Series Node.

The following tables lists the various visualizations for Inline V Series solution:

Table 2: Overall 5G Apps Dashboard

Dashboard	Description	Visualizations	Details
Inline Source (Packets)	Displays the overall visualization details of Inline V Series Solution	LoadBalancer to Inline Source Average Packets	Displays the Inline traffic received from the Load balancer to the Inline V Series Node interface in packets.
		Inline Source to Load Balancer Average Packets	Displays the Inline traffic sent back from the Inline V Series Node interface to the Load balancer in packets.
		LoadBalancer to Inline Source App Average Packets	Displays the Inline traffic received from the Inline V Series Node interface to the IVTAP application in packets.
		Inline Source to LoadBalancer App Average Packets	Displays the Inline traffic sent back from the IVTAP application to the Inline V Series Node interface in packets.
		Average IVTAP App Total Packets Drop	Displays the IVTAP application total packet drops while processing the Inline traffic received from Inline V Series Node interface.
		Average Inline Source IVTAP Errors	Displays the IVTAP application errors while processing the Inline traffic received from Inline V Series Node interface
		Average Out-of-band Ingress Tunnel rx Packets	Displays the Out-of-Band traffic (Mirrored traffic) received from Inline V Series Node interface.
		Average Tool Tunnel tx Packets	Displays the bytes transmitted to the tool from GigaVUE V Series Node of the last tier.
		Average Out-of-band Ingress Tunnel Packets Drop	Displays the Out-of-Band traffic packet drops while receiving traffic (Mirrored traffic) from Inline V Series Node interface.
		Average Out-of-band Ingress Tunnel Errors	Displays the Out-of-Band errors while receiving traffic (Mirrored traffic) from Inline V Series Node interface.
Inline Source (Bytes)	Displays the overall	Load Balancer to	Displays the Inline traffic

Dashboard	Description	Visualizations	Details
	visualization details of Inline V Series Solution	Inline Source Average Bytes	received from the Load balancer to the Inline V Series Node interface in bytes.
		Inline Source to Load Balancer Average Bytes	Displays the Inline traffic sent back from the Inline V Series Node interface to the Load balancer in bytes.
		LoadBalancer to Inline Source App Average Bytes	Displays the Inline traffic received from the Inline V Series Node interface to the ITAP application in bytes.
		Inline Source to LoadBalancer App Average Bytes	Displays the Inline traffic sent back from the ITAP application to the Inline V Series Node interface in bytes.
		Average Out-of-band Ingress Tunnel rx Bytes	Displays the Out-of-Band traffic (Mirrored traffic) received from Inline V Series Node interface in bytes.
		Average Tool Tunnel tx Bytes	Displays the bytes transmitted to the tool from GigaVUE V Series Node of the last tier in bytes.
Heart Beat Analytics		Average LoadBalancer To Inline Source Heart Beat Packets	Displays the Health Check request packets (Heart beat packets) received by Inline V Series Node from Load balancer
		Average Inline Source To LoadBalancer Heart Beat Packets	Displays the Health Check response packets (Heart beat packets) sent by Inline V Series Node to Load balancer.

Debuggability and Troubleshooting

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

Sysdumps

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

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 shows the Azure Fabric Manager interface. At the top, there are tabs for Monitoring Domains, Connections, Fabric, UCT-V, and UCT-V Upgrade. Below the tabs, there are filters for Monitoring Domains (All) and Connections (All). A table lists Fabric Nodes with columns: FABRIC NODES, MONITORING DOMAIN, CONNECTIONS, TYPE, and MANAGEMENT IP. The table contains three rows: vamsi-inline-vmss_0, vamsi-inline-vmss_1, and vamsi-oob-vmss_0. An Actions menu is open over the first row, showing options: Edit Fabric, Delete Fabric, Upgrade Fabric, and Generate Sysdump.

FABRIC NODES	MONITORING DOMAIN	CONNECTIONS	TYPE	MANAGEMENT IP
☒ vamsi-inline-vmss_0	MD	CN	V Series Node	10.0.0.10
☐ vamsi-inline-vmss_1	MD	CN	V Series Node	10.0.0.12
☐ vamsi-oob-vmss_0	MD	CN	V Series Node	10.0.0.4

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**.

FAQs - Secure Communication between GigaVUE Fabric Components (Azure)

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?

No. The upgrade process remains unchanged across all supported upgrade paths. You can upgrade your nodes without any additional steps. The upgrade results in the automatic deployment of the appropriate certificates based on the node versions

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self-Signed Certificate

2. What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?

Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions:

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. What are the new ports that must be added to the security groups?

The following table lists the port numbers that must be opened for the respective fabric components:

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80, 8892
GigaVUE V Series Proxy	8300, 80, 8892
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to Prerequisites for GigaVUE Cloud Suite for Azure .

4. Is the registration process different for deploying the fabric components using Third-Party Orchestration?

Yes. Beginning with version 6.10, you must use tokens in the gigamon-cloud.conf file instead of the username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. For more details, refer to [Configure Tokens](#).

Example Registration Data for UCT-V:

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      token: <Token>
      remoteIP: <IP address of the UCT-V Controller 1, <IP address of the UCT-V
Controller 2>
      sourceIP: <IP address of UCT-V> (Optional Field)
```

5. Are there any changes to the UCT-V manual installation and upgrade process?

Starting from version 6.10, you must add tokens during manual installation and upgrades.

- Create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation
- After installing UCT-V, you can add the configuration file in the /etc directory.

Important! Without this token, UCT-V cannot register with GigaVUE-FM.

6. Can I use my PKI infrastructure to issue certificates for the Fabric Components?

Direct integration of your PKI with GigaVUE-FM is not supported. However, you can provide your Intermediate Certificate Authority (CA) to sign the node certificate.

7. **What happens to the existing custom certificates introduced in the 6.3 release?**

The custom certificate feature is not supported for the fabric components with version 6.10 or higher, even if a custom certificate is selected in the Monitoring Domain. However, this feature remains available for older versions.

- When upgrading from version 6.9 or earlier with custom certificates upgrades to version 6.10, the system automatically generates and deploys certificates signed by GigaVUE-FM.
- If deploying version 6.9 or earlier components from a 6.10 GigaVUE-FM, custom certificates are still applied.

8. **How to issue certificates after upgrading the fabric components to 6.10?**

When the upgrade process begins, GigaVUE-FM transmits the certificate specifications to the new fabric components using the launch script. The fabric components utilize these specifications to generate their own certificates.

9. **Is secure communication supported in FMHA deployment?**

Yes, it is supported. However, you must follow a few manual steps before upgrading the fabric components to 6.10. For details, refer to [Configure Secure Communication between Fabric Components in FMHA](#).

NOTE: This step is essential if you are using cloud deployments in FMHA mode and would like to deploy or upgrade the fabric components to version 6.10 or later.

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 Cloud Suite 6.14 Hardware and Software Guides	
GigaVUE-TA200 Hardware Installation Guide	
GigaVUE-TA200E Hardware Installation Guide	
GigaVUE-TA400 Hardware Installation Guide	
GigaVUE-TA400E Hardware Installation Guide	
GigaVUE-OS Installation Guide for DELL S4112F-ON	
G-TAP A Series 2 Installation Guide	
GigaVUE M Series Hardware Installation Guide	
GigaVUE-FM Hardware Appliances Guide	
Software Installation and Upgrade Guides	
GigaVUE-FM Installation, Migration, and Upgrade Guide	
GigaVUE-OS Upgrade Guide	
GigaVUE V Series Migration Guide	
Fabric Management and Administration Guides	
GigaVUE Administration Guide	covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide	
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)