



GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite

Product Version: 6.11

Document Version: 1.0

(See Change Notes for document updates.)

Copyright 2025 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

| Product Version | Document Version | Date Updated | Change Notes |
|-----------------|------------------|--------------|--|
| 6.11 | 1.0 | 06/17/2025 | The original release of this document with 6.11.00 GA. |

Contents

| | |
|---|-----------|
| GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) | 1 |
| Change Notes | 3 |
| Contents | 4 |
| GigaVUE Cloud Suite Deployment Guide - VMware(ESXi) | 7 |
| Overview of GigaVUE Cloud Suite for VMware | 8 |
| Components for GigaVUE Cloud Suite for VMware | 8 |
| Cloud Overview Page (VMware) | 9 |
| Top Menu | 10 |
| Viewing Charts on the Overview Page | 12 |
| Viewing Monitoring Session Details | 13 |
| Architecture for GigaVUE Cloud Suite for VMware ESXi | 14 |
| Points to Note (VMware vCenter) | 15 |
| Volume-Based License | 15 |
| Base Bundles | 16 |
| Bundle Replacement Policy | 16 |
| Add-on Packages | 16 |
| How GigaVUE-FM Tracks Volume-Based License Usage | 17 |
| Default Trial Licenses | 18 |
| Activate Volume-Based Licenses | 19 |
| Manage Volume-Based Licenses | 19 |
| Supported Hypervisors for VMware | 22 |
| Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi | 23 |
| Secure Communication between GigaVUE Fabric Components | 24 |
| GigaVUE-FM acts as the PKI | 25 |
| Bring Your Own CA | 25 |
| Secure Communication in FMHA Mode | 25 |
| Supported Platforms | 25 |
| Supported Components | 26 |
| Rules and Notes | 26 |
| Rediscover | 26 |
| Analytics for Virtual Resources | 27 |
| Sharing the Same Host across Different Monitoring Domains | 27 |

| | |
|---|-----------|
| Cloud Health Monitoring | 28 |
| Selective Source Selection | 28 |
| Customer Orchestrated Source - Use Case | 28 |
| Prerequisites for Integrating V Series Nodes with VMware vCenter | 29 |
| Recommended Form Factor for VMware vCenter (Instance Types) | 30 |
| Minimum Virtual Computing Requirements | 30 |
| Network Firewall Requirements | 31 |
| Required VMware Virtual Center Privileges | 32 |
| Default Login Credentials | 34 |
| Install and Upgrade GigaVUE-FM | 34 |
| Deploy GigaVUE Cloud Suite for VMware (ESXi) | 35 |
| Upload GigaVUE V Series Node Image into GigaVUE-FM | 36 |
| Integrate Private CA | 36 |
| Rules and Notes | 36 |
| Generate CSR | 36 |
| Upload CA Certificate | 37 |
| Create Monitoring Domain for VMware ESXi | 37 |
| Configure GigaVUE V Series Nodes for VMware ESXi | 42 |
| Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi | 49 |
| Configure Secure Communication between Fabric Components in FMHA .. | 54 |
| Configure Monitoring Session | 54 |
| Create a Monitoring Session (VMware) | 55 |
| Monitoring Session Page (VMware) | 56 |
| Configure Monitoring Session Options (VMware ESXi) | 57 |
| Create Ingress and Egress Tunnel (VMware vCenter) | 59 |
| Create Raw Endpoint (VMware vCenter) | 67 |
| Rules and Notes | 67 |
| Configure Raw Endpoint in Monitoring Session | 68 |
| Create a New Map (VMware ESXi) | 69 |
| Example- Create a New Map using Inclusion and Exclusion Maps | 76 |
| Map Library | 76 |
| Add Applications to Monitoring Session | 77 |
| Interface Mapping | 78 |
| Deploy Monitoring Session | 78 |
| View Monitoring Session Statistics | 79 |
| Visualize the Network Topology (VMware ESXi) | 82 |
| Migrate Application Intelligence Session to Monitoring Session | 83 |
| Post Migration Notes for Application Intelligence | 85 |

| | |
|---|------------|
| Monitor Cloud Health | 87 |
| Configuration Health Monitoring | 87 |
| Traffic Health Monitoring | 88 |
| Supported Resources and Metrics | 89 |
| Create Threshold Templates | 91 |
| Apply Threshold Template | 92 |
| Clear Thresholds | 93 |
| View Health Status | 93 |
| Configure VMware Settings | 94 |
| Configure Certificate Settings | 95 |
| Analytics for Virtual Resources | 96 |
| Virtual Inventory Statistics and Cloud Applications Dashboard | 96 |
| Debuggability and Troubleshooting | 101 |
| Sysdumps | 101 |
| Sysdumps—Rules and Notes | 101 |
| Generate a Sysdump File | 102 |
| FAQs - Secure Communication between GigaVUE Fabric | |
| Components | 103 |
| Additional Sources of Information | 107 |
| Documentation | 107 |
| How to Download Software and Release Notes from My Gigamon | 110 |
| Documentation Feedback | 110 |
| Contact Technical Support | 111 |
| Contact Sales | 112 |
| Premium Support | 112 |
| The VUE Community | 112 |
| Glossary | 113 |

GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite for VMware helps you see and manage traffic in your VMware environment. It captures virtual machine (VM) traffic, filters it, and sends only the needed data to your monitoring and security tools.

This solution works with the Gigamon Deep Observability Pipeline to give you complete visibility. It helps you avoid missing traffic in private cloud setups or service provider NFV deployments.

This guide explains how to install, deploy, and manage the GigaVUE V Series Nodes in VMware.

Refer to the sections below for detailed information:

- [Overview of GigaVUE Cloud Suite for VMware](#)
- [Architecture for GigaVUE Cloud Suite for VMware ESXi](#)
- [Points to Note \(VMware vCenter\)](#)
- [Volume-Based License](#)
- [Supported Hypervisors for VMware](#)
- [Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi](#)
- [Prerequisites for Integrating V Series Nodes with VMware vCenter](#)
- [Install and Upgrade GigaVUE-FM](#)
- [Deploy GigaVUE Cloud Suite for VMware \(ESXi\)](#)
- [Configure Monitoring Session](#)
- [Migrate Application Intelligence Session to Monitoring Session](#)
- [Monitor Cloud Health](#)
- [Configure VMware Settings](#)
- [Analytics for Virtual Resources](#)

Overview of GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware enables you to manage and monitor network traffic in virtual environments. It captures, improves, and sends selected network traffic to your security and monitoring tools.

This solution works closely with VMware tools to give you clear visibility into traffic from virtual machines. It helps you understand what's happening in your private cloud.

GigaVUE-FM, a key part of the Cloud Suite, works with VMware vCenter to automatically set up GigaVUE V Series Node to support a growing private cloud infrastructure. It also helps track changes in workloads and keeps traffic policies working properly.

Benefits:

- **Flexible Traffic Acquisition:** Collects traffic using port mirroring in VMware ESXi.
- **Automated Visibility Provisioning:** Automatically sets up and applies traffic rules as new users or groups are added.
- **Improved Tool Efficiency:** Filters and balances traffic to reduce the load on your monitoring tools.
- **Application Intelligence Solution:** Detects thousands of applications and accesses over 7,000 application metadata elements to understand your network better.

Components for GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware comprises includes several key components. These work together to collect, filter, and send network traffic. You can manage everything through a single, easy-to-use web interface.

Main Components

| Component | Description |
|---|--|
| GigaVUE-FM fabric manager (GigaVUE-FM) | Represents a web-based tool that helps you manage physical and virtual network traffic that forms GigaVUE Cloud Suite Cloud Suite for VMware. It gives you complete visibility and control of your entire VMware cloud suite from one dashboard. GigaVUE-FM generates a complete network map to easily see which cloud systems are connected to the deep observability pipeline. It can manage hundreds of visibility nodes across on-premises and cloud environments. It also handles the setup for all other components in your platform. |
| GigaVUE® V Series Node | Represents a node that collects mirrored traffic, applies filters, and processes data using GigaSMART applications. It then sends the optimized traffic to your cloud-based tools or back to on-premises tools. |

Cloud Overview Page (VMware)

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:

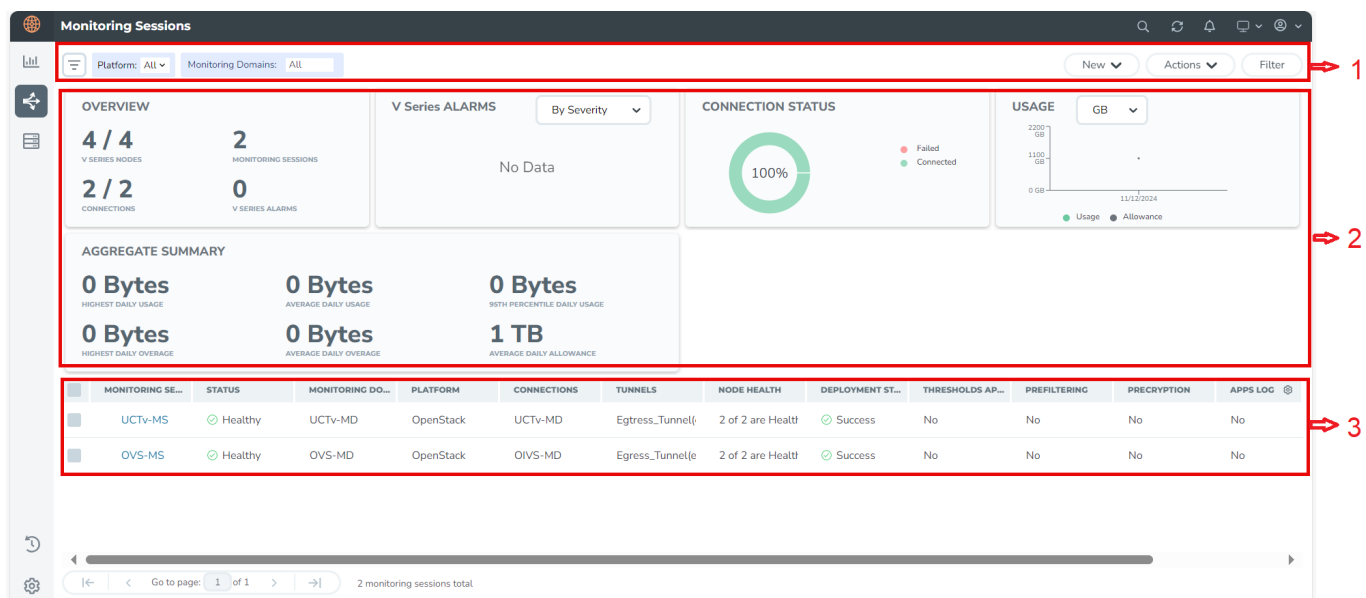
- Basic statistics
- V Series alarms
- Connection status
- Volume usage vs. allowance
- A summary table of active monitoring sessions

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

How to Access the Overview Page

- To view the overall cloud overview page, go to Traffic > Virtual > Overview.

- To view platform-specific cloud overview details:
 - Go to Traffic > Virtual > Overview.
 - On the top-left menu, select the name of your cloud from the Platform drop-down option.



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 Top Menu . |
| 2 | Charts | Refer to Viewing Charts on the Overview Page . |
| 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 Viewing Monitoring Session Details 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: |

| Options | Description |
|---------------|--|
| | <ul style="list-style-type: none"> • 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. |
| Filter | You can filter the Monitoring Session details based on a criterion or a combination of criteria. For more information, refer to Filters . |


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. Click  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.
- Hover over a bar to 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.

Architecture for GigaVUE Cloud Suite for VMware ESXi

This document highlights how to deploy GigaVUE V Series Node on the VMware ESXi platforms and set up traffic monitoring sessions using these nodes.

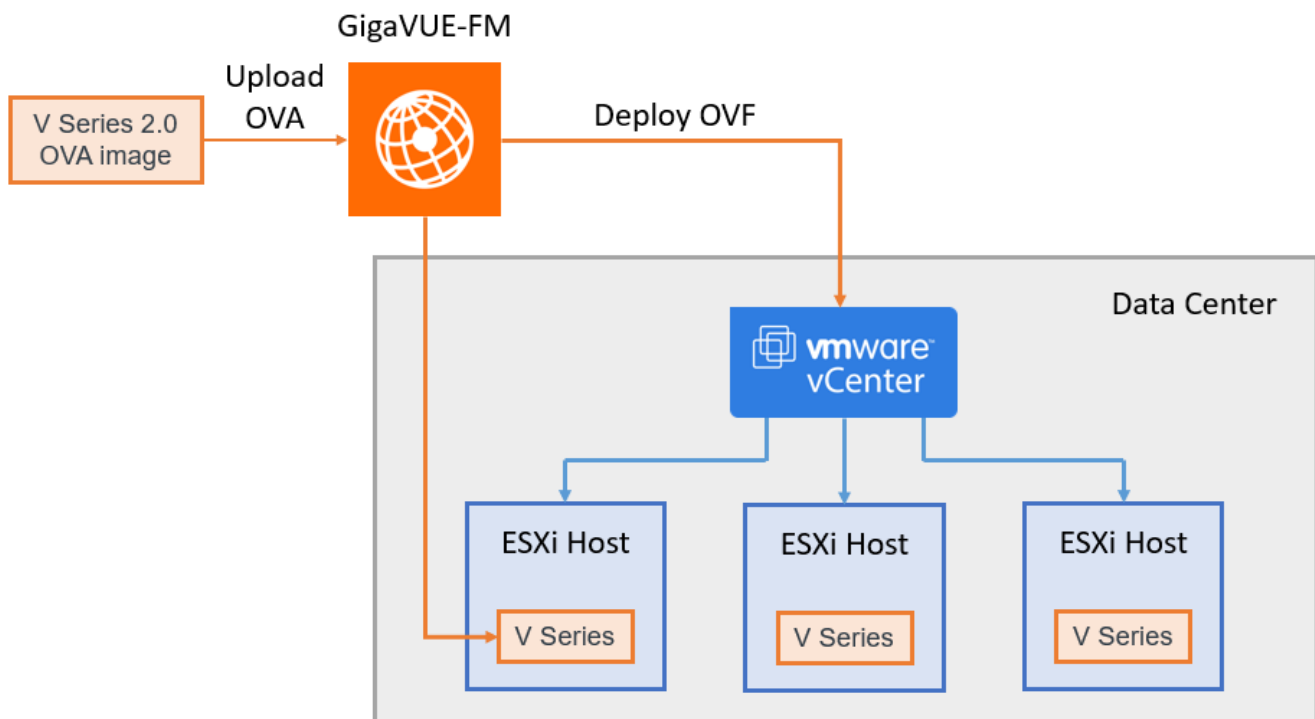
The GigaVUE V Series Nodes provide traffic visibility on the following VMware network types:

- vSphere Standard Switch
- vSphere Distributed Switch

Based on your setup, GigaVUE-FM creates, updates, and deletes the GigaVUE V Series Nodes on the ESXi hosts. Each GigaVUE V Series must run on the same ESXi host as the virtual machines (VMs) it monitors. It receives mirrored traffic directly from those VMs.

You can deploy only one GigaVUE V Series Node on a single ESXi host. GigaVUE-FM communicates directly with the GigaVUE V Series Nodes.

The following diagram displays a high-level overview of the deployment:



Points to Note (VMware vCenter)

1. **VMware vCenter Setup:** These steps assume that VMware vCenter is installed and configured. For details, refer to [VMware Documentation](#).
2. **Virtual Switch Configuration:** Ensure the source virtual machine and the monitoring tool are connected to different virtual standard switches. If both are on the same switch, traffic may loop back, causing issues.
3. **Handling Latency from NGFW with DPI:** If NextGen Firewall (NGFW) with Deep Packet Inspection (DPI) is enabled to inspect your east-west traffic, expect an increase in latency due to mirrored traffic. To avoid increased latency, perform one of the following:
 - Create an exception rule for the tunneled traffic (mirrored traffic from the GigaVUE V Series Nodes to the tool).
 - Configure a private VDS that can bypass the NGFW rules for this traffic.
4. **NSX N-VDS Support:** NSX Virtual Distributed Switch (N-VDS) based segments are not supported in **VMware vCenter** Monitoring Domain. N-VDS is supported only on NSX versions less than or equal to 3.0. For more information, refer to [VMware Documentation](#).

Volume-Based License

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

- For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales team.
- For more information, refer to the Data Sheet for the required GigaVUE Cloud Suite.

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

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

Bundle Replacement Policy

Refer to the following notes:

- You can only upgrade to a higher bundle.

You cannot have two different base bundles at the same time. However, you can have multiple base bundles of the same type.

As soon as you upgrade to a higher bundle, the existing lower bundles are automatically deactivated.

Add-on Packages

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

The following add-on SKUs are available:

Rules for add-on packages:

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

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

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

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

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

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

Default Trial Licenses

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

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

This license includes the following applications:

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


- Inline SSL
- SSL Decrypt
- Precryption

NOTE: If you do not have any other volume-based licenses installed, the deployed monitoring sessions are undeployed from the existing GigaVUE V Series Nodes after 30 days at the expiration of the trial license.

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

Activate Volume-Based Licenses

To activate Volume-Based Licenses:


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

Manage Volume-Based Licenses

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

Manage active Volume-Based License

To manage active Volume-Based License (VBL):

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

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


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

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

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

Manage Inactive Volume-Based License

To manage inactive Volume-Based License (VBL):

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

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

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

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

Use the following buttons to manage your VBL.

| Button | Description |
|---------------------------|---|
| Activate Licenses | Use this button to activate a Volume-Based License. For more information, refer to the topic Manage Volume-Based Licenses of the GigaVUE Licensing Guide . |
| Email Volume Usage | Use this button to send the volume usage details to the email recipients. Refer to Add Email Notification Recipients for more details on how to add email recipients. |
| Filter | Use this button to narrow down the list of active Volume-Based Licenses that are displayed on the VBL active page. |
| Export | Use this button to export the details in the VBL active page to a CSV or XLSX file. |
| Deactivate | Use this button to deactivate the licenses. You can only deactivate licenses that have expired. |

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

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

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

Supported Hypervisors for VMware

The following table lists the supported hypervisor versions for vCenter, VMware ESXi and VMware NSX-T.

| GigaVUE V Series Node Supported Hypervisors | | Tested Platforms | | |
|---|------|------------------|----------------|--|
| | | vCenter Server | ESXi | GigaVUE-FM |
| vSphere ESXi | v6.7 | v6.7U3 | v6.7U3 | v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01 |
| | v7.0 | v7.0 | v7.0 | v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01, v5.14.00, v5.15.00, v5.16.00, v6.0.00, v6.1.00 |
| | v7.0 | v7.0U3 | v7.0U3 | v5.15.00, v5.16.00, v6.0.00, v6.1.00, v6.2.00, v6.3.00, v6.4.00, v6.5.00, v6.6.00, v6.7.00, v6.8.00, v6.9.00, v6.10.00, v6.11.00 |
| | v8.0 | v7.0U3 | v8.0U2 | v6.9.00 |
| | v8.0 | v8.0 | v8.0 | v6.3.00, v6.4.00, v6.5.00, v6.6.00, v6.7.00, v6.8.00, v6.9.00 |
| | v8.0 | v8.0U2, v8.0U3 | v8.0U2, v8.0U3 | v6.8.00, v6.9.00, v6.10.00, v6.11.00 |

| GigaVUE V Series Node Supported Hypervisors | | Tested Platforms | | |
|---|--------|------------------|------------------------|---|
| | | vCenter Server | ESXi | GigaVUE-FM |
| vSphere NSX-T | v3.1.0 | v7.0 | v7.0 | v5.11.01, v5.12.00 |
| | v3.1.2 | v7.0 | v6.7U3, v7.0U1 | v5.12.00, v5.13.00, v5.13.01 |
| | v3.1.3 | v7.0 | v6.7U3, v7.0U1 | v5.13.01, v5.14.00, v6.0.00 |
| | v3.2.0 | v7.0, v7.0U3 | v6.7U3, v7.0U1, v7.0U3 | v5.14.01, v5.15.00, v5.16.00, v6.0.00 |
| | v3.2.1 | v7.0U3 | v6.7U3, v7.0U1, v7.0U3 | v6.0.00, v6.1.00, v6.2.00 |
| | v3.2.2 | v7.0U3 | v7.0U3 | v6.3.00, v6.4.00 |
| | v3.2.3 | v7.0U3 | v7.0U3 | v6.5.00, v6.6.00, v6.7.00, v6.8.00, v6.9.00, v6.10.00, v6.11.00 |
| | v4.0.0 | v7.0U3 | v7.0U3 | v6.0.00, v6.1.00, v6.2.00, v6.3.00 |
| | v4.1.0 | v7.0U3 | v7.0U3 | v6.3.00, v6.4.00, v6.5.00 |
| | | v8.0U2 | v8.0U2 | v6.5.00, v6.6.00, v6.7.00 |
| | v4.1.2 | v8.0U2, v8.0U3 | v8.0U2, v8.0U3 | v6.8.00, v6.9.00 |
| | v4.2 | v8.0U2 | v8.0U2, v8.0U3 | v6.9.00, v6.10.00, v6.11.00 |

Introduction to Supported Features for GigaVUE Cloud Suite for VMware ESXi

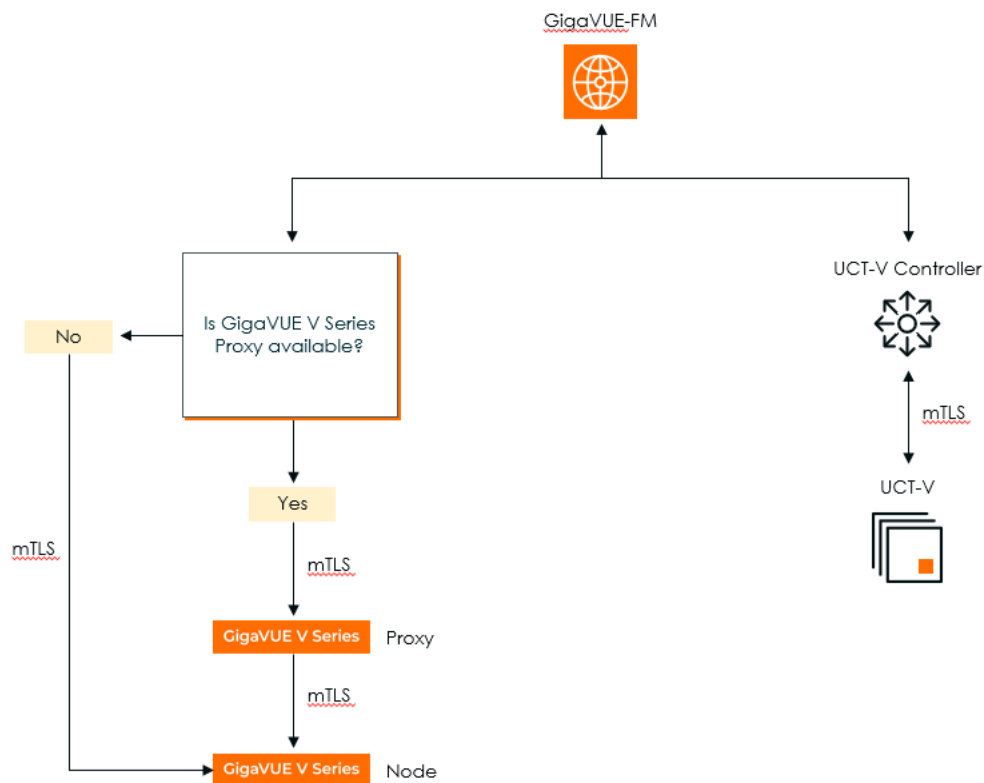
GigaVUE Cloud Suite for VMware (ESXi) supports the following features:

- [Rediscover](#)
- [Analytics for Virtual Resources](#)
- [Sharing the Same Host across Different Monitoring Domains](#)
- [Cloud Health Monitoring](#)
- [Selective Source Selection](#)

Secure Communication between GigaVUE Fabric Components

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

How it Works!



In this setup:

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

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

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

GigaVUE-FM acts as the PKI

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

Bring Your Own CA

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

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

Secure Communication in FMHA Mode

In FMHA (Fabric Manager High Availability) mode:

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

Supported Platforms

- AWS
- Azure
- OpenStack
- Nutanix
- Third Party Orchestration

- VMware ESXi
- VMware NSX-T

Supported Components

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

Rules and Notes

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

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

Rediscover

Sometimes, changes made to a GigaVUE V Series Node in VMware vCenter can cause its settings to go out of sync with what's shown in GigaVUE-FM. When this happens, you can use the Rediscover button in GigaVUE-FM to fix the mismatch:

Rediscovery updates the following settings:

- GigaVUE V Series Node name
- Datastore
- Management IP address
- Tunnel IP address
- Network name for Management Interface
- Network name for Tunnel Interface

NOTE: Note: GigaVUE-FM automatically performs rediscovery every 24 hours to keep settings in sync.

To manually rediscover a node:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and select **Monitoring Domain**.
The **Monitoring Domain** page appears.
2. Select **Actions > Rediscover**.

NOTE: You can only rediscover GigaVUE V Series Nodes that are in **OK** state.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a separate tool that helps you see your data through visual charts.

With Analytics, you can:

- Create charts and turn them into visualizations.
- Group visualizations into dashboards.
- Build search objects to find specific data.

These items, Dashboards, Visualizations, and Search Objects, are called Analytics objects.

For details, refer to [Analytics for Virtual Resources](#).

Sharing the Same Host across Different Monitoring Domains

GigaVUE-FM enables you to share a host between VMware ESXi and VMware NSX-T monitoring domains. You can deploy multiple V Series nodes from VMware NSX-T monitoring domain and one V Series Node from VMware ESXi monitoring domain on the same host.

As a result, you can monitor the workload of virtual machines using the following two options:

- Connected to NSX segments using the V Series nodes deployed in NSX-T monitoring domain.
- Connected to regular VSS / VDS networks using the V Series node deployed in the ESXi monitoring domain.

NOTE: Note: GigaVUE-FM cannot provide visibility in the ESXi platform to a Virtual Machine with NICs attached to both VMware NSX-T segments and ESXi VDS or VSS port groups.

Cloud Health Monitoring

GigaVUE-FM helps you track the health of your monitoring sessions. You can check traffic flow and configuration status for each session and its parts.

This section explains how to:

- View the health of your monitoring sessions.
- Verify the status of each component.

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

Selective Source Selection

This feature enables you to select an individual network adapter of a virtual machine as a target while creating a map.

For details, refer to [Create a New Map \(VMware ESXi\)](#).

Customer Orchestrated Source - Use Case

Customer Orchestrated Source is a traffic capture method that allows to tunnel traffic directly to the GigaVUE V Series Nodes. This method is practical when some restrictions or a firewall prevent the setting up of UCT-V or VPC Mirroring. You can tunnel the traffic to a GigaVUE V Series Node to filter and process.

When using this method, you can:

- Set up tunnels or raw endpoints directly in the monitoring session.
- Apply tools like Slicing, Masking, Application Metadata, and Application Filtering to process the tunneled traffic.

To learn how to configure tunnels and endpoints, see:

- [Create Ingress and Egress Tunnel \(VMware vCenter\)](#)
- [Create Raw Endpoint \(VMware vCenter\)](#)

To set up,

1. Configure an Ingress tunnel in the Monitoring Session.
2. Use the GigaVUE V Series Node IP address as the destination IP address,

The traffic is directly tunneled to that GigaVUE V Series Node.

Prerequisites for Integrating V Series Nodes with VMware vCenter

- Learn about supported VMware vCenter, VMware ESXi and VMware NSX-T versions. For details, refer to [Supported Hypervisors for VMware](#).
- Ensure the ESXi hosts have the minimum vCPU and memory resources to host the GigaVUE V Series Nodes. For details, refer to [Recommended Form Factor for VMware vCenter \(Instance Types\)](#).
- Set the vCenter character encoding to UTF-8 to support internationalized characters in the VMware vCenter environment.
- Access to GigaVUE V Series Node device OVA image file. You can download from [Gigamon Customer Portal](#).
- Verify that all the target VMs have VMware guest tools or Open VM tools if you use IP-based filtering.
- Ensure that Port 8889 is available for GigaVUE-FM to access GigaVUE V Series Nodes.
- Ensure that TCP Port 443 is open between the GigaVUE-FM instance and the ESXi host to upload the OVA files. For details, refer to [Network Firewall Requirements](#)
- Ensure a minimum of **Intel Sandy Bridge** CPU compatibility for proper operation and optimal performance to enable **VMware EVC** in VMware vCenter. Recommended option: **Skylake** and above.

Refer to the following topics for more information:

- [Recommended Form Factor for VMware vCenter \(Instance Types\)](#)
- [Network Firewall Requirements](#)
- [Required VMware Virtual Center Privileges](#)
- [Default Login Credentials](#)

Recommended Form Factor for VMware vCenter (Instance Types)

The form factor (instance type) of the GigaVUE V Series Node is configured on the OVF file and packaged as part of the OVA image file.

Note: Instance types can differ for GigaVUE V Series Nodes in different ESXi hosts. Small is the default type.

The table below lists the available form factors (instance types) based on memory and the number of vCPUs for a single GigaVUE V.

| Type | Memory | vCPU | Disk space | vNIC |
|--------|--------|--------|------------|---|
| Small | 4GB | 2 vCPU | 8GB | 1 Management interface, 1 Tunnel interface, and 8 vTAP interfaces |
| Medium | 8GB | 4 vCPU | | |
| Large | 16GB | 8 vCPU | | |

NOTE: Note: You can contact your account manager or Gigamon Technical Support to identify a suitable form factor.

Minimum Virtual Computing Requirements

When deploying GigaVUE V Series Nodes, your Virtual Distributed Switch (VDS) must have a minimum number of ports available in its port groups. The required number of ports depends on how many port groups you use in each deployment.

If Using a Single Port Group:

- Each GigaVUE V Series Node needs 10 ports from that port group.
- So, the port group must support: $10 \times (\text{Number of GigaVUE V Series Nodes})$

If Using Two Port Groups:

When using two port groups in one deployment (typically one for Management and one for Tunnel traffic):

- Management Port Group
Needs: 1 port per GigaVUE V Series Node

- Tunnel Port Group

Needs: 9 ports per GigaVUE V Series Node

Use these calculations to ensure your port groups are sized correctly before deploying.

Network Firewall Requirements

Network Firewall Requirements for GigaVUE V Series Node deployment

| Source | Destination | Source Port | Destination Port | Protocol | Service | Purpose |
|---------------|------------------------|------------------|------------------|----------|------------|--|
| GigaVUE-FM | ESXi hosts | Any (1024-65535) | 443 | TCP | https | Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files. OVA files require access to the host IP/URL for bulk deployment |
| | vCenter | | | | | |
| GigaVUE-FM | GigaVUE V Series Nodes | Any (1024-65535) | 8889 | TCP | Custom API | Allows GigaVUE-FM to communicate with GigaVUE V Series Node |
| GigaVUE-FM | GigaVUE V Series Nodes | Any (1024-65535) | 5671 | TCP | Custom TCP | Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node |
| GigaVUE-FM | GigaVUE V Series Nodes | Any (1024-65535) | 80 | TCP | Custom TCP | Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Node. |
| Administrator | GigaVUE-FM | Any (1024-65535) | 443 | TCP | https | Facilitates Management connection to GigaVUE-FM . |
| | | | 22 | | ssh | |
| Administrator | GigaVUE V | Not | 22 | | ssh | Facilitates |

| | Series Nodes | Applicable | | | | troubleshooting GigaVUE V Series Nodes. |
|---------------------------|--|---|----------------------|-------|------------------|---|
| Remote Source | GigaVUE V Series Nodes | Custom Port (VXLAN and UDPGRE),N/A for GRE | 4789 | UDP | VXLAN | Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable to the Tunnel Ingress option only) |
| | | | N/A | IP 47 | GRE | |
| | | | 4754 | UDP | UDPGRE | |
| GigaVUE V Series Nodes | Tool/ GigaVUE HC Series instance | Custom Port (VXLAN),N/A for GRE | 4789 | UDP | VXLAN | Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool |
| | | | Not Applicable | IP 47 | GRE | |
| GigaVUE V Series Nodes | Tool/ GigaVUE HC Series instance | Not Applicable | Not Applicable | ICMP | Echo Request | (Optional) Allows GigaVUE V Series Node to health check tunnel destination traffic |
| | | | | | Echo Response | |
| GigaVUE V Series Nodes | GigaVUE-FM | Any (1024- 65535) | Any (1024- 65535) | TCP | Custom TCP | Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM |
| GigaVUE V Series Nodes | GigaVUE-FM | Any (1024- 65535) | 9600 | TCP | Custom TCP | Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node. |

Required VMware Virtual Center Privileges

This topic lists the minimum privileges required for the GigaVUE-FM user in Virtual Center.

You assign privileges to Virtual Center users. To assign privileges, from the left pane, select **Administration** and go to **Access Control > Roles**.

Important! You must apply the roles at the vSphere Virtual Center level, not at the data center or Host levels.

The following table lists the minimum permissions required for GigaVUE-FM to manage the virtual center user with the specified roles:

| Category | Required Privilege | Purpose |
|---------------------------|---|--|
| Datastore | Allocate space | V Series Node Deployment |
| Distributed Switch | VSPAN Operation | VDS Tapping |
| Folder | Create Folder | V Series Node Deployment |
| Host | Configuration <ul style="list-style-type: none"> Network Configuration | VSS Tapping |
| | Inventory <ul style="list-style-type: none"> Modify Cluster | Pin V Series Node to the host in cluster configurations to prevent automatic migration. |
| Network | <ul style="list-style-type: none"> Assign network Configure | <ul style="list-style-type: none"> V Series Node Deployment/VSS Tapping V Series Node Deployment |
| Resource | Assign virtual machine to resource pool | V Series Node Deployment |
| vApp | <ul style="list-style-type: none"> Import vApp instance configuration vApp application configuration | V Series Node Deployment |
| Virtual machine | Configuration <ul style="list-style-type: none"> Add new disk Add or remove device Modify device settings Rename | V Series Node Deployment V Series Node Deployment/VSS Tapping |

| Category | Required Privilege | Purpose |
|----------|--|--------------------------|
| | Interaction <ul style="list-style-type: none"> • Connect devices • Power on • Power Off • Reset | V Series Node Deployment |
| | Inventory <ul style="list-style-type: none"> ▪ Create from existing ▪ Remove | V Series Node Deployment |
| | Provisioning <ul style="list-style-type: none"> ▪ Clone virtual machine | V Series Node Deployment |

Default Login Credentials

You can login to the GigaVUE V Series Node by using the default credentials.

| Product | Login credentials |
|-----------------------|--|
| GigaVUE V Series Node | <p>You can login to the GigaVUE V Series Node by using ssh. The default username and password is:</p> <p>Username: gigamon</p> <p>Password: Enter the password provided during the fabric launch configuration. Refer Configure GigaVUE V Series Nodes for VMware ESXi for more detailed information on fabric launch configuration.</p> |

Install and Upgrade GigaVUE-FM

You have the flexibility of installing GigaVUE-FM on various supported platforms, including both cloud and on-premises environments.

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

Reference links

- **Installation:** Refer to GigaVUE-FM Installation and Upgrade Guide in the [Gigamon Documentation Library](#).

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

Deploy GigaVUE Cloud Suite for VMware (ESXi)

To integrate GigaVUE V Series Nodes with VMware vCenter, perform the following steps:

- [Upload GigaVUE V Series Node Image into GigaVUE-FM](#)
- [Create Monitoring Domain for VMware ESXi](#)
- [Configure GigaVUE V Series Nodes for VMware ESXi](#)
- [Rediscover](#)

The table below outlines each step to deploy GigaVUE Cloud Suite for VMware, helping you gain visibility into both physical and virtual network traffic.

Note: Review the VMware ESXi System Requirements and [Prerequisites for Integrating V Series Nodes with VMware vCenter](#) sections for prerequisites.

| Step No | Task | Refer the following topics |
|---------|---|---|
| 1 | Upload the GigaVUE V Series Node Image (OVA File) into GigaVUE-FM | Upload GigaVUE V Series Node Image into GigaVUE-FM |
| 2 | Create a Monitoring Domain | Create Monitoring Domain for VMware ESXi |
| 3 | Deploy GigaVUE V Series Node using GigaVUE-FM | Configure GigaVUE V Series Nodes for VMware ESXi Refer to <i>Deploy GigaVUE V Series Nodes using GigaVUE-FM</i> section. |
| 4 | Create Monitoring session | Create a Monitoring Session (VMware) |
| 5 | Create an Ingress and Egress Tunnels to tunnel traffic | Create Ingress and Egress Tunnel (VMware vCenter) |
| 6 | Add Applications to the Monitoring Session | Add Applications to Monitoring Session |
| 7 | Deploy Monitoring Session | Deploy Monitoring Session |
| 8 | View Monitoring Session Statistics | View Monitoring Session Statistics |

Upload GigaVUE V Series Node Image into GigaVUE-FM

This step is optional. You can upload the GigaVUE V Series Node image to GigaVUE-FM even while deploying the GigaVUE V Series Node. For details, refer to [Configure GigaVUE V Series Nodes for VMware ESXi](#).

To upload the V Series image into GigaVUE-FM,

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and select **Settings > OVA Files**.
2. In the **OVA Files** page, select **Browse**, and then select the image file. For example, *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova*. **Note:** You can upload three OVA files to GigaVUE-FM for VMware vCenter.
3. Select **Upload to Server**
You have uploaded the OVA image file to the GigaVUE-FM server.

NOTE:

Integrate Private CA

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


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

Rules and Notes

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

Generate CSR

To create an intermediate CA certificate:


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

The CSR is downloaded successfully.

Upload CA Certificate

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

To upload the signed CA certificate to GigaVUE-FM:

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

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

Create Monitoring Domain for VMware ESXi

This chapter describes how to create a monitoring domain for deploying GigaVUE V Series Nodes in VMware vCenter environment through GigaVUE-FM. You must establish a connection between GigaVUE-FM and VMware vCenter. Creating a monitoring domain in GigaVUE-FM allows you to establish a connection between vCenter and GigaVUE-FM.

To create a monitoring domain in GigaVUE-FM for VMware vCenter,

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, and select **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, select **New**. The **VMware Configuration** page appears.

The screenshot shows the 'VMware Configuration' page in the GigaVUE Cloud Suite interface. The page has a dark header with 'VMware vCenter', 'Monitoring Domain', and 'Settings' tabs. Below the header, there's a 'VMware Configuration' section with a 'Save' and 'Cancel' button. The configuration fields are as follows:

- Monitoring Domain***: Text input field.
- Connection Alias***: Text input field.
- Virtual Center***: Text input field.
- Username***: Text input field.
- Password***: Text input field with a toggle for visibility.
- Traffic Acquisition Method**: Dropdown menu set to 'Platform Tapping'.
- Resource Allocation ⓘ**: Dropdown menu set to 'Target VM Based'.
- Maximum number of V Series nodes per Host**: Text input field set to '10'.

A help box on the right side of the page provides information about the 'Resource Allocation' options:

- **Target VM Based (Default)** - Preferable for environments when there are workload VMs attached to less than or equal to 8 virtual switches on the same ESXi Host.
- **Switch Based** - Preferable for environments when there are workload VMs attached to more than 8 virtual switches on the same ESXi Host.

At the bottom left, the text 'FM Instance:GigaVUE-FM - 6.7.00' is visible.

3. In the **VMware Configuration** page, enter or select the following details:

| Field | Description |
|--------------------------|---|
| Monitoring Domain | Name of the monitoring domain |
| Connection Alias | Name of the connection |
| Virtual Center | <p>IP address or FQDN of the vCenter</p> <div> NOTE: To ensure the validity of VMware virtual central certificates issued by a trusted Certificate Authority (CA), you must enable the Trust Store. For details, refer to Cloud solution in Trust Store section in the GigaVUE Administration Guide. </div> |
| Username | <p>Username of the vCenter user with minimum privileges as described in the Prerequisites for Integrating V Series Nodes with VMware vCenter section.</p> <div> NOTE: Whenever you change the vCenter credentials in VMware vCenter, edit the Monitoring Domain to update that in GigaVUE-FM. Otherwise, the connection status reaches an authentication failure state. </div> |
| Password | vCenter password to connect to the vCenter |

| Field | Description |
|---|--|
| Traffic Acquisition Method | <p>Select a Traffic Acquisition Method.</p> <p>Platform Tapping: Platform tapping is performed in two ways.</p> <ul style="list-style-type: none"> • VSS: Used when a workload Virtual Machine is connected to a Virtual Standard Switch network. GigaVUE-FM creates a promiscuous network on the VSS switch for tapping traffic. • VDS: Used when a workload Virtual Machine is connected to a Virtual Distributed Switch portgroup. Port Mirroring is created on the VDS switch by GigaVUE-FM for tapping the traffic <p>Customer Orchestrated Source: If you select Customer Orchestrated Source as the tapping method, you can use a tunnel or raw endpoint where traffic is directly tunneled to GigaVUE V Series Nodes.</p> <p>NOTE: Select the Traffic Acquisition Method as Customer Orchestrated Source if you want to deploy an AMX application in the Monitoring Session for this Monitoring Domain.</p> |
| Resource Allocation <p>NOTE: This field is applicable only when using Platform Tapping as the Traffic Acquisition Method.</p> | <p>When deploying multiple GigaVUE V Series Node in a single host, select any one of the following options:</p> <p>Target VM Based: Choose this option if your deployment workload VMs attached to less than or equal to 8 vSwitches on the same ESXi host. This resource allocation type distributes the workload VMs across multiple GigaVUE V Series Nodes on the same ESXi host.</p> <p>Switch Based: A single GigaVUE V Series Node can tap a maximum of 8 vSwitches. Choose this option if you have traffic monitoring VMs running on ESXi hosts connected to more than 8 vSwitches in a single host. The vSwitches are mapped to the GigaVUE V Series Node in a round-robin manner. In this model, vSwitches are evenly distributed across the available GigaVUE V Series Nodes on the same host.</p> <p>NOTE: Ensure to undeploy all the Monitoring Session associated with the connection before changing the Resource Allocation type.</p> |
| Maximum Number of V Series Nodes per Host | Enter the maximum number of GigaVUE V Series Nodes possible to deploy in a single host. The default value is 10. |

4. Select **Save**. The **VMware Fabric Launch Configuration** page appears. For details on how to deploy GigaVUE V Series Nodes in the **VMware Fabric Launch Configuration** page, refer to [Configure GigaVUE V Series Nodes for VMware ESXi](#)

**Notes:**

- Ensure that all V Series Nodes within a Monitoring Domain run 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.

The Monitoring Domain created in this section is listed on the **Monitoring Domain** page.



Points to Note:

- Whenever you change the vCenter credentials in VMware vCenter, edit the Monitoring Domain to update that in GigaVUE-FM. Otherwise, the connection status reaches an authentication failure state.
- When the Monitoring Domain is in a "Not Connected" state, updating the vCenter credentials will only refresh the information stored in the GigaVUE-FM database.

To establish the connection:

1. Navigate to the **Monitoring Domain** page.
2. Select **Actions** and select **Connect**.

By following these steps, you can ensure that your vCenter credentials are updated and the connection is established correctly.

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

| Actions | Description |
|---------------------------------|--|
| Edit | Use to edit a monitoring domain. |
| Deploy Fabric | Use to deploy GigaVUE V Series Nodes. |
| Upgrade Fabric | Use to upgrade GigaVUE V Series Nodes. For details, refer to Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi |
| Delete Monitoring Domain | Use to delete a Monitoring Domain. |
| Delete Fabric Nodes | Use to delete a GigaVUE V Series Node. |
| Connect / Disconnect | <p>Disconnect: This option appears when the Monitoring Domain is Connected. Use it to stop communication between GigaVUE-FM and the VMware vCenter.</p> <p>Connect: This option appears when the Monitoring Domain is disconnected. Use it to start communication between GigaVUE-FM and the VMware vCenter.</p> |
| Rediscover | The changes made in vCenter for the GigaVUE V Series is reflected in GigaVUE-FM. Refer to Rediscover topic for more detailed information. |
| Power On | You can select an individual GigaVUE V Series Node and power it on. The status of the GigaVUE V Series Node is changed to Ok . |
| Power Off | You can select an individual GigaVUE V Series Node and power it off. If the GigaVUE V Series Node is turned off from GigaVUE-FM, then it is not considered as part of Cloud Health Monitoring and GigaVUE-FM does not try to turn it on. The status of the GigaVUE V Series Node is changed to Down . |

| Actions | Description |
|-------------------------------|---|
| Reboot | You can select an individual GigaVUE V Series Node and reboot it. |
| Edit SSL Configuration | You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels. |
| Generate Sysdump | <p>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.</p> <p>For more information, refer to Debuggability and Troubleshooting.</p> |
| Manage Certificates | <p>You can use this button to perform the following actions:</p> <ul style="list-style-type: none"> • Re-issue: Required to address security compromises, key changes, or configuration updates, like validity period adjustments. • Renew: Extends the 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. For details, refer to Configure Certificate Settings |

- To view and manage the generated sysdump files, select the GigaVUE V SeriesNode and select the **Sysdump** tab in the lower pane.
- To view the certificates associated with the fabric, select the fabric nodes and select the **Certificates** tab in the lower pane.

Configure GigaVUE V Series Nodes for VMware ESXi

This section provides step-by-step instructions on how to deploy GigaVUE V Series Nodes in VMware vCenter Monitoring Domain.

To deploy GigaVUE V SeriesNodes using GigaVUE-FM, follow these steps:

1. Go to the **VMware Fabric Launch Configuration** page using one of the following options:
 - **Automatic Option:** Create a monitoring domain, and the page opens automatically.
 - **Manual Option:** Open **VMware Fabric Launch Configuration** page from the **Monitoring Domain** page.
 - To launch the **VMware Fabric Launch Configuration** from the Monitoring Domain, go to **Inventory > VIRTUAL > VMware vCenter (V Series)**.
 - Select **Actions > Deploy Fabric**.

The **VMware Fabric Launch Configuration** page appears.

VMware Fabric Launch Configuration

Datacenter*

Cluster*

V Series Node Image*

Form Factor*

Enable Custom Certificates ☐

Host* ☐ Import Host Info from File ☒ Add Host Info Manually

Common Configuration

☒ Datastores ☐ Datastore Clusters

Datastore

V Series Node Name Prefix

V Series Node Name Suffix

Name Server

SSL Key

No. of V Series Nodes Per Host

Management

Network*

IP Type

MTU

Tunnel

Network*

IP Type

Gateway IP

MTU

Use IPv6 ☐


Virtual Disk Format


Deployment Folder

User Password* (gigamon)

Confirm User Password*

2. On the **VMware Fabric Launch Configuration** page, enter or select the following details:

| Field | Description |
|--|---|
| Datacenter | vCenter Data Center with the ESXi hosts to be provisioned with GigaVUE V Series Nodes. |
| Cluster | Cluster where you want to deploy the GigaVUE V Series Nodes. |
| V Series Node Image | <p>Select the OVA file uploaded in the Upload GigaVUE V Series Node Image into GigaVUE-FM, from the drop-down menu.</p> <p>You can also add OVA files when launching the fabric. To add OVA files:</p> <ol style="list-style-type: none"> Click on the Add button. The Upload Image dialog box opens. In the Upload Image dialog box, click Browse to select the <i>gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova</i> file. Select Upload to Server to upload the selected OVA image file to GigaVUE-FM server. |
| Form Factor | <p>Instance size of the GigaVUE V Series Node. For details, refer to Prerequisites for Integrating V Series Nodes with VMware vCenter.</p> <div>  <ul style="list-style-type: none"> Small Form Factor is not supported when using applications like Application Visualization, Application Metadata, Application Filtering. Select 80GB Disk Space, when using AMX Application. </div> |
| Enable Custom Certificates | <p>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 unavailable in Trust Store, communication does not happen, and a handshake error occurs.</p> <div> <p>NOTE: If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state.</p> </div> |
| Certificate <div> <p>NOTE: This field appears only when Enable Custom Certificates field is enabled.</p> </div> | <p>Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes. For more information, refer to Secure Communication between GigaVUE Fabric Components.</p> |
| Hosts | <p>Select the ESXi hosts for GigaVUE V Series Node deployment.</p> <div> <p>NOTE: You can select up to 250 hosts manually.</p> </div> <p>Select Import Host Info from file or Add Host Info Manually.</p> <p>Import Host Info from file:</p> <p>To import host details from a .csv file:</p> <ol style="list-style-type: none"> Download the .csv template file. |

| Field | Description | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|----------------------|--|------------------|--|----------------------------------|---|----------------------------------|--|--------------------|--|---------------------------------------|---|------------|--|---------|--|---------|--|------------|---|---|--|----------------|---|
| | <p>b. Enter the required values in the Excel sheet and save the file.</p> <p>c. Select Browse and select the .csv file saved in the previous step.</p> <div>  <ul style="list-style-type: none"> To deploy more than one GigaVUE V SeriesNode on the same host, add more rows in the Excel sheet with the same host value for each extra GigaVUE V SeriesNode you want to deploy. If your GigaVUE-FM version is above 6.5 and GigaVUE V Series Nodes are on a version below 6.5, Name Server and MTU are not supported. Therefore, these fields in the .csv file must be empty. </div> <p>Add Host Info Manually:</p> <p>Select the ESXi hosts for GigaVUE V Series Node deployment.</p> <p>The Common Configuration drop-down wizard appears. Expand the Common Configuration drop-down wizard and update the following details to apply the configuration to all the selected hosts.</p> <p>You can expand the individual hosts and add or delete GigaVUE V Series Node. You can expand the individual GigaVUE V Series Node and modify the configurations applied in the Common Configuration.</p> <table border="1"> <thead> <tr> <th colspan="2">Common Configuration</th></tr> </thead> <tbody> <tr> <td>Datastore</td><td>Network datastore shared among all ESXi hosts.</td></tr> <tr> <td>V Series Node Name Prefix</td><td>Enter a prefix for the GigaVUE V SeriesNode name.</td></tr> <tr> <td>V Series Node Name Suffix</td><td>Enter a suffix for the GigaVUE V Series Node name.</td></tr> <tr> <td>Name Server</td><td>The server that stores the mapping between the domain names and the IP addresses. The maximum number of name servers that can be entered is three. Enter valid IPv4 addresses, separated by a comma.</td></tr> <tr> <td>No. of V Series Nodes per Host</td><td>Enter the number of GigaVUE V Series Nodes to be deployed in each host.</td></tr> <tr> <th colspan="2">Management</th></tr> <tr> <td>Network</td><td>Management network for GigaVUE V Series Nodes.</td></tr> <tr> <td>IP Type</td><td>Select the management network IP type as Static or DHCP.</td></tr> <tr> <td>Gateway IP</td><td>Gateway IP address of the Management Network.</td></tr> <tr> <td colspan="2"> <div> NOTE: This field appears only when the Management IP type is Static. </div> </td></tr> <tr> <td>Netmask Length</td><td>Management network's subnet mask value in CIDR format. For example, 21 for /21.</td></tr> </tbody> </table> | Common Configuration | | Datastore | Network datastore shared among all ESXi hosts. | V Series Node Name Prefix | Enter a prefix for the GigaVUE V SeriesNode name. | V Series Node Name Suffix | Enter a suffix for the GigaVUE V Series Node name. | Name Server | The server that stores the mapping between the domain names and the IP addresses. The maximum number of name servers that can be entered is three. Enter valid IPv4 addresses, separated by a comma. | No. of V Series Nodes per Host | Enter the number of GigaVUE V Series Nodes to be deployed in each host. | Management | | Network | Management network for GigaVUE V Series Nodes. | IP Type | Select the management network IP type as Static or DHCP. | Gateway IP | Gateway IP address of the Management Network. | <div> NOTE: This field appears only when the Management IP type is Static. </div> | | Netmask Length | Management network's subnet mask value in CIDR format. For example, 21 for /21. |
| Common Configuration | | | | | | | | | | | | | | | | | | | | | | | | | |
| Datastore | Network datastore shared among all ESXi hosts. | | | | | | | | | | | | | | | | | | | | | | | | |
| V Series Node Name Prefix | Enter a prefix for the GigaVUE V SeriesNode name. | | | | | | | | | | | | | | | | | | | | | | | | |
| V Series Node Name Suffix | Enter a suffix for the GigaVUE V Series Node name. | | | | | | | | | | | | | | | | | | | | | | | | |
| Name Server | The server that stores the mapping between the domain names and the IP addresses. The maximum number of name servers that can be entered is three. Enter valid IPv4 addresses, separated by a comma. | | | | | | | | | | | | | | | | | | | | | | | | |
| No. of V Series Nodes per Host | Enter the number of GigaVUE V Series Nodes to be deployed in each host. | | | | | | | | | | | | | | | | | | | | | | | | |
| Management | | | | | | | | | | | | | | | | | | | | | | | | | |
| Network | Management network for GigaVUE V Series Nodes. | | | | | | | | | | | | | | | | | | | | | | | | |
| IP Type | Select the management network IP type as Static or DHCP. | | | | | | | | | | | | | | | | | | | | | | | | |
| Gateway IP | Gateway IP address of the Management Network. | | | | | | | | | | | | | | | | | | | | | | | | |
| <div> NOTE: This field appears only when the Management IP type is Static. </div> | | | | | | | | | | | | | | | | | | | | | | | | | |
| Netmask Length | Management network's subnet mask value in CIDR format. For example, 21 for /21. | | | | | | | | | | | | | | | | | | | | | | | | |

| Field | Description | |
|-------|--|--|
| | NOTE: This field appears only when the Management IP type is Static. | |
| | MTU | The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000. |
| | Data Interfaces - When using Customer Orchestrated Source as the Traffic Acquisition Method, you must configure two data interfaces. | |
| | Use IPv6 | Enable to use IPv6. |
| | NOTE: This field appears only when Customer Orchestrated Source as the Traffic Acquisition Method. | |
| | Network | Tunnel Network for the GigaVUE V Series Nodes. |
| | IP Type | Select the tunnel network IP address type as Static or DHCP. |
| | Gateway IP (optional) | Gateway IP address of the Tunnel Network. |
| | Netmask Length | Tunnel network's subnet mask value in CIDR format. For example, 21 for /21. |
| | NOTE: This field appears only when the Tunnel IP type is Static. | |
| | MTU | The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000. |
| | IPv6 Prefix Length | Enter the IPv6 prefix length as 64. |
| | NOTE: This field appears only when the Use IPv6 toggle button is enabled. | |
| | Virtual Disk Format | Select the Virtual Disk Format from the drop-down menu |
| | Deployment Folder | Enter the folder name in vCenter, under which the GigaVUE V SeriesNodes must be deployed. |
| | Password | Enter the password you wish to use for the GigaVUE V Series Node. |

3. Select **Deploy**. After deployment in vCenter, it appears on the **Monitoring Domain** page under the Monitoring Domain, where the GigaVUE V Series Node is deployed.

NOTE: GigaVUE-FM can process a maximum of ten GigaVUE V Series Nodes deployment requests in parallel on VMware vCenter. Each deployment request can have multiple GigaVUE V Series Nodes for deployment.

Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi

This section explains the available methods to upgrade the GigaVUE V Series Nodes and provides instructions on how to upgrade GigaVUE V Series Nodes.



IMPORTANT NOTE:

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

- Open the required ports in the cloud platform. For details, refer to .
- When using FMHA configuration, follow the steps provided in the [Configure Secure Communication between Fabric Components in FMHA](#) section.

Update GigaVUE V Series Nodes

Use one the following two options:

1. Upgrade all the GigaVUE V Series Node in a monitoring Domain:
 - a. Select the Monitoring Domain.
 - b. Select **Actions > Upgrade Fabric**.
2. Upgrade a single or a group of GigaVUE V Series Node. When upgrading a group of GigaVUE V Series Nodes, ensure all the GigaVUE V Series Nodes deployed on the same ESXi hosts are selected.

Upgrade Considerations

- You can select an entire monitoring domain and upgrade all the GigaVUE V Series Nodes in that particular monitoring domain, or you can select an entire host and upgrade all the GigaVUE V Series Node deployed in that particular host.
- When multiple GigaVUE V Series Nodes are deployed on the same ESXi host and only if a part of GigaVUE V Series Nodes are selected in that particular host, then the **Upgrade Fabric** button is disabled.

- When upgrading GigaVUE V Series Nodes, if a host of a particular GigaVUE V Series Node is under maintenance mode, then the **Upgrade Fabric** button is disabled.
- Unselect the GigaVUE V Series Node whose host is under maintenance mode, and upgrade that GigaVUE V Series Node when the host is out of the maintenance mode.
- **NOTE:** GigaVUE-FM supports only (n, n-1, n-2) GigaVUE V Series Node versions.

Upgrade the GigaVUE V Series Node in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**, then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select an entire monitoring domain or an entire host and select **Actions**.
3. From the drop-down list, select **Upgrade Fabric**. The **V Series Node Upgrade Task** dialog box appears.

V Series Nodes Upgrade Task

Name*

Image*

Name Server

Change Form Factors ☒

Default Form Factor ⓘ

| V Series Node | Form Factor | Version |
|------------------|--------------------------------|---------|
| VSeries.vp-esxi- | Small, 2vCPU, 4GB RAM, 8GB ... | 6.4.00 |
| VSeries.vp-esxi- | Small, 2vCPU, 4GB RAM, 8GB ... | 6.4.00 |

4. Enter a name for the V Series Node upgrade task.
5. Select the latest GigaVUE V Series Node OVA image from the **Image** drop-down list. **Note:** When upgrading the GigaVUE V Series Nodes to any version equal to or greater than 6.5.00, the **Name Server** field is displayed. This field is optional. Name Server is a server that stores the mapping between the domain names and the IP address. The maximum number of name servers that can be entered is three. Enter valid IPv4 address, separated by comma.

6. (Optional) If you want to modify the form factor (instance) size, select the **Change Form Factors** check box.
7. Select the form factor from the Default Form Factor drop-down menu to change the form factor of all the selected V Series Nodes. You can use the **Use Current** option to use the existing form factor of the individual GigaVUE V Series Node. You can also change the form factor of a individual GigaVUE V Series Node from the **Form Factor** drop-down menu of the respective GigaVUE V Series Node. The form factor selected here overwrites the form factor selected in the **Default Form Factor**.

NOTE: All the GigaVUE V Series Node with Static IP address retain their old IP address even after the upgrade.

8. Select **Upgrade** to launch the GigaVUE V Series Node upgrade.

NOTE: Both the new and the current GigaVUE V Series Nodes appear in the same Monitoring Domain until the new nodes replaces the current and the status changes to **Ok**.

You can view the status of the upgrade in the Status column of the **Monitoring Domain** page.

New

Actions

Refresh Inventory

| | | Monitoring Domain | Connections | Host | Name | Management IP | Tunnel IP | Type | Version | Status | |
|--|--|-------------------|-------------|---------------|----------------------------|---------------|---------------|---------------|---------|-----------|----------------|
| | | md1 | | | | | | | | | Upgrade Status |
| | | | con1 | | | | | | | Connected | |
| | | | | 10.115.81.184 | | | | | | | |
| | | | | | VSeries.127310.115.81.184 | 10.114.82.69 | 10.114.84.3 | V Series Node | 6.6.00 | upgrading | |
| | | | | | VSeries.new10.115.81.184-1 | 10.114.84.86 | 10.114.84.93 | V Series Node | 6.6.00 | upgrading | |
| | | | | 10.115.81.185 | | | | | | | |
| | | | | | VSeries.new10.115.81.185-1 | 10.114.82.143 | 10.114.84.86 | V Series Node | 6.6.00 | upgrad | |
| | | | | | VSeries.sl10.115.81.185-1 | 10.115.80.190 | 10.115.80.191 | V Series Node | 6.6.00 | upgrading | |

To view the detailed upgrade status click **Upgrade Status**, the **V Series Node Upgrade Status** dialog box appears.

V Series Node Upgrade Status

Monitoring Domain Name: esxi-md-202-13

Upgrade Tasks



▼ Upgrade_GigaVUE_VSERIES_Node | SUCCESS

Clear

Summary

■ Success: 2
■ Failed: 0
■ In Progress: 0
Total: 2

Node Statuses


| Node | Status |
|--|--------|
| VSeries.vp-redscvr-  | OK |
| VSeries.vp-redscvr-  renamed2 | OK |

▼ Upgrade | IN_PROGRESS

Summary

■ Success: 0
■ Failed: 0
■ In Progress: 1
Total: 1

Node Statuses

| Node | Status |
|---|-----------|
| VSeries.vp-redscvr-  upgrade | launching |

- Select **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.
- If the GigaVUE V Series Node upgrade fails or is interrupted for any reason, select **Retry** on the **V Series Node Upgrade Status** dialog box.

NOTE: You cannot modify the node configurations when you are using **Retry** option. GigaVUE-FM uses the same values defined in the initial fabric upgrade configuration.

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
```

Configure Monitoring Session

GigaVUE-FM collects inventory data on all V Series nodes deployed in your environment through vCenter connections. You can design your monitoring session to include or exclude the target VMs you want to monitor. You can also choose to monitor egress, ingress, or all traffic.

When a new target VM is added to your environment, GigaVUE-FM automatically detects it. If the detected VM matches the defined selection criteria, your monitoring session displays it.

Similarly, when a traffic monitoring target VM is removed, the monitoring sessions are updated to show the removed instance.

Important! Before deploying a monitoring session, you need to deploy a V Series node on each host where you want to monitor traffic.

Limitations:

- **NOTE:** Pre-filtering is not supported on VMware ESXi running with V Series nodes.

Refer to the following topics for details:

- [Create a Monitoring Session \(VMware\)](#)
- [Monitoring Session Page \(VMware\)](#)
- [Create Raw Endpoint \(VMware vCenter\)](#)
- [Create a New Map \(VMware ESXi\)](#)
- [Add Applications to Monitoring Session](#)
- [Interface Mapping](#)
- [Deploy Monitoring Session](#)
- [View Monitoring Session Statistics](#)
- [Visualize the Network Topology \(VMware ESXi\)](#)
- [Configure VMware Settings](#)

Create a Monitoring Session (VMware)

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

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

Target Instance

- When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds it to your Monitoring Session based on your selection criteria. Similarly, when an instance is removed, it updates the Monitoring Sessions.
- For the VPCs without UCT-Vs, targets are not automatically selected. In those cases, you can use Customer Orchestrated Source in the Monitoring Session to accept a tunnel from anywhere.

You can create multiple Monitoring Sessions within one Monitoring Domain.

To create a new Monitoring Session:

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

NOTE: Note: Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.

4. Select **Save**.
The Monitoring Session Overview page appears.

Monitoring Session Page (VMware)

The Monitoring Session page provides a comprehensive view of each monitoring session in your VMware environment. This topic includes descriptions of Tabs, Actions, and Sidebar Controls.

Tabs Menu



| Tab | Description |
|-----------------|---|
| Overview | Displays key information about the selected monitoring session, such as connections, tunnel and health status, deployment state, and information related to Application Intelligence statistics. You can view traffic trends (ingress/egress) hourly, daily, weekly, or monthly. You can filter statistics by associated elements. For more information, refer to View Monitoring Session Statistics |
| Sources | Lists all monitored sources and targets. You can view/edit connection details, check deployment status, number of targets, and source health. For OVS Mirroring, the source tab also displays hypervisor and instance details. |

| Tab | Description |
|---------------------------|---|
| Traffic Processing | Allows you to add and configure applications, tunnel endpoints, raw endpoints, and maps. View stats for each application, apply threshold templates, enable user-defined apps, and toggle distributed de-duplication. For more information, refer to Configure Monitoring Session Options (VMware ESXi) |
| V Series Nodes | Shows the V Series Nodes tied to the session. In the split view, you can view the node name, health, deployment status, host VPC, version, and management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. For more information, refer to the Interface Mapping |
| Topology | Visualizes the monitored network fabric, showing connections, subnets, and instances. You can explore topology by selecting specific connections, offering a clear visualization of the monitored network elements. For more information, refer to Visualize the Network Topology (VMware ESXi) . |

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 (VMware ESXi)

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

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

Access the TRAFFIC PROCESSING tab

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

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

Apply Threshold Template

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

To apply a threshold,

1. In the **TRAFFIC PROCESSING** page, select **Options > Thresholds**.
2. Select an existing threshold template from the **Select Template** drop-down list.
Note: You can create a template using **New Threshold Template** option and apply it. For more information, refer to the [Traffic Health Monitoring](#) section.
3. Select **Apply**.

NOTE: The template is added to the Monitoring Session.

NOTE: Notes:

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

Enable User-Defined Applications

To enable a defined application,

1. In the Monitoring Session **TRAFFIC PROCESSING** page, select **Options > User Defined Applications**.
2. Enable the **User-defined Applications** toggle button.
3. From the **Actions** drop-down, add one of the existing applications or create a User-Defined Application.
For more information, refer to [User Defined Application](#).

Enable Distributed De-duplication

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

To enable,

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



Notes:

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

Create Ingress and Egress Tunnel (VMware vCenter)

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, TLS-PCAPNG, UDP, or ERSPAN tunnel.


NOTE: GigaVUE-FM lets you configure ingress tunnels in a Monitoring Session when you use the Traffic Acquisition Method UCT-V.

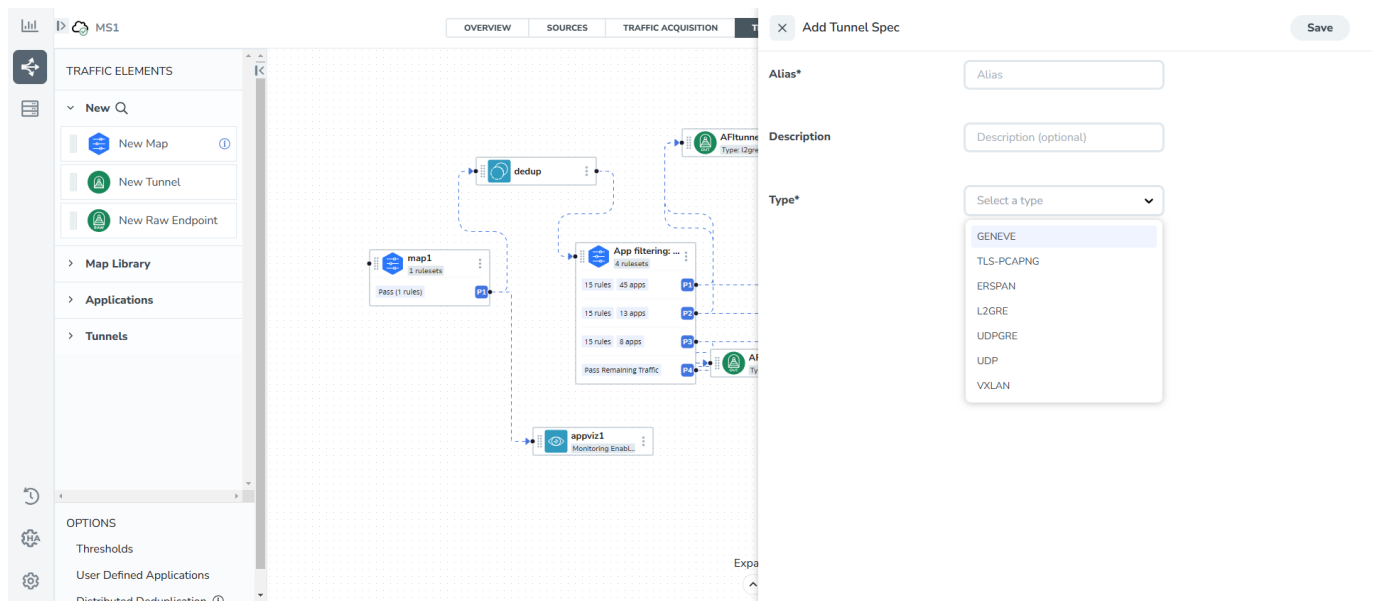
Create a new tunnel endpoint

To create,

1. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.


The GigaVUE-FM Monitoring Session canvas page appears.

2. 1. In the canvas, select the  icon on the left side of the page to view the traffic processing elements.
3. 2. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.
3. 3. The **Add Tunnel Spec** quick view appears.
4. 4. Enter the **Alias**, **Description**, and **Type** details.
5. 5. For details, refer to [Details - Add Tunnel Specifications](#) table.
5. Select **Save**.



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

Apply a threshold template to Tunnel End Points

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

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

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

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

Table 1: Details - Add Tunnel Specifications

| Field | Description |
|--|---|
| Alias | The name of the tunnel endpoint. |
| Description | The description of the tunnel endpoint. |
| Admin State <div> NOTE: This option appears only after the Monitoring session deployment. </div> | 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 Series Node has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. GigaVUE-FM only disable the tunnels when it receives a notification via REST API indicating that a tool or group of tools is down. <div> NOTE: This option is not supported for TLS-PCAPNG tunnels. </div> |
| Type | The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE. |
| VXLAN | |
| Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. <div> 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 </div> | |

| Field | Description | |
|--|--|--|
| details, refer to Secure Tunnels . | | |
| In | Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node. | |
| | IP Version | The version of the Internet Protocol. Select IPv4 or IPv6. |
| | Remote Tunnel IP | For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source. |
| | VXLAN Network Identifier | Unique value that is used to identify the VXLAN. The value ranges from 1 to 16777215. |
| | Source L4 Port | The port used to establish the connection to the target. For example, if A is the source and B is the destination, this port value belongs to A. |
| | Destination L4 Port | The port used to establish the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B. |
| Out | Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination endpoint. | |
| | Remote Tunnel IP | For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint. |
| | 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 |

| Field | Description | |
|--|--|---|
| | | NOTE: You can configure either a single-step or multi-step setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session. |
| | Source L4 Port | The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A. |
| | Destination L4 Port | The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B. |
| UDPGRE | | |
| Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. | | |
| In | Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node. | |
| | IP Version | The version of the Internet Protocol. Select IPv4 or IPv6. |
| | Remote Tunnel IP | For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source. |
| | Key | Identifier used to differentiate different UDPGRE/L2GRE tunnels. It routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295. |
| | Source L4 Port | The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A. |
| | Destination L4 Port | The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B. |
| L2GRE | | |
| Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. | | |
| NOTE: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device. For details, refer to the Secure Tunnels . | | |
| In | Choose In (Decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node. | |

| 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. |
| | Key | Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295. |
| Out | Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint. | |
| | Remote Tunnel IP | For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint. |
| | MTU | The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500. |
| | Time to Live | Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64. |
| | DSCP | Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority. |
| | Flow Label | Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575. |
| | Key | Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295. |
| ERSPAN | | |
| Traffic Direction | | |
| The direction of the traffic flowing through the GigaVUE V Series Node. | | |
| In | IP Version | The version of the Internet Protocol. Select IPv4 or IPv6. |
| | Remote Tunnel IP | For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source. |
| | Flow ID | The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023. |

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

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

| Field | Description | |
|-------|----------------------------------|---|
| Out | L4 Destination IP Address | Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter . |
| | Source L4 Port | The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A. |
| | Destination L4 Port | The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B. |

Create Raw Endpoint (VMware vCenter)

This topic provides instructions on configuring a RAW Endpoint (REP) in the Monitoring Session.

Rules and Notes

Ingress REP works only when you select the Traffic Acquisition Method as **Customer Orchestrated Source** while configuring the Monitoring Domain.

For details, refer to [Create Monitoring Domain for VMware ESXi](#)

Consideration

When deploying GigaVUE V Series Nodes in the Monitoring Domain, the number of interfaces varies based on the Traffic Acquisition Method. See the table below for details.


| Traffic Acquisition Method | Display Name | Interface Name | Role | Comments |
|------------------------------|-------------------|----------------|------------|--|
| Customer Orchestrated Source | Network Adapter 1 | ens160 | Management | |
| | Network Adapter 2 | ens192 | Data | Supports Tunnel and RAW endpoint. Available for Ingress and Egress REP |
| | Network Adapter 3 | ens224 | Data | Supports Tunnel and RAW endpoint. Available for |

| Traffic Acquisition Method | Display Name | Interface Name | Role | Comments |
|----------------------------|------------------------|----------------|------------|---|
| | | | | Ingress and Egress REP |
| Platform Tapping | Network Adapter 1 | ens160 | Management | |
| | Network Adapter 2 | ens192 | Data | Supports Tunnel and Egress RAW endpoint. |
| | Network Adapter 3 - 10 | - | Data | Reserved and used for platform tapping (Port Mirroring) |

Configure Raw Endpoint in Monitoring Session

Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the monitoring session.

To configure,

1. From the New expand menu, drag and drop **New Raw Endpoint** to the graphical workspace.
2. On the new raw endpoint icon, select the  menu button and select **Details**. The **Raw** quick view page appears.
3. Enter the Alias and Description details for the Raw End Point and select **Save**.
4. Perform the following steps to deploy the Monitoring Session after adding the Raw Endpoint:
 - a. From the **Actions** drop-down list on the **TRAFFIC PROCESSING** page, select **Deploy**. The **Deploy Monitoring Session** dialog box appears.
 - b. Select the V Series Nodes to deploy the Monitoring Session.
 - c. From the drop-down menu of the selected individual V Series Nodes, select the interfaces for each REPs and the TEPs deployed in the Monitoring Session.
 - d. Select **Deploy**.
5. Select **Export** to download all or selected V Series Nodes in the CSV and XLSX formats.


Create a New Map (VMware ESXi)

If you're a new user, the free trial lasts for 30 days. After that, GigaVUE-FM asks you to buy a license. For details,, refer to [GigaVUE Licensing Guide](#).

A map filters traffic that flows through GigaVUE V Series Nodes. It includes one or more rules, each defining what traffic to match. Traffic can match one or more rules in the map.

Parameters to create a map

| Parameter | Description |
|----------------------------|---|
| Rules | A rule (R) includes filtering conditions that traffic must match. It also defines traffic direction (ingress or egress) and target. |
| Priority | Sets the rule execution order. Use values from 1 (highest) to 5 (lowest). |
| Pass | Sends traffic from the VM to the destination. |
| Drop | Drops the traffic from the virtual machine when passing through the map. |
| Traffic Filter Maps | A set of maps to match traffic and perform various actions on the matched traffic. |
| Inclusion Map | An inclusion map determines the instances to be included for monitoring. This map is used only for target selection. |

| | |
|---|--|
| Exclusion Map | An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection. |
| Automatic Target Selection (ATS) | <p>A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session.</p> <p>The below formula describes how ATS works:</p> <p>Selected Targets = Traffic Filter Maps \cap Inclusion Maps - Exclusion Maps</p> <p>Below are the filter rule types that work in ATS:</p> <ul style="list-style-type: none"> • • mac Source • • mac Destination • • ipv4 Source • • ipv4 Destination • • ipv6 Source • • ipv6 Destination • • VM Name Destination • • VM Name Source • • VM Tag Destination - Not applicable to Nutanix. • • VM Tag Source - Not applicable to Nutanix. • • VM Category Source - Applicable only to Nutanix. • • VM Category Destination - Applicable only to Nutanix. • • Host Name -Applicable only to Nutanix and VMware. <p>The traffic direction is as follows:</p> <ul style="list-style-type: none"> • • For any rule type as Source - the traffic direction is egress. • • For Destination rule type - the traffic direction is ingress. • • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. <div> <p> Notes:</p> <ul style="list-style-type: none"> • For OpenStack environment, Subnet Name Source and Subnet Name Destination are the exclusion filters available as part of Exclusion Maps with Traffic Acquisition method as OVS Mirroring in the Monitoring Domain. • If no ATS rule filters listed above are used, all VMs and vNICs are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC. </div> |
| Group | A group is a collection of pre-defined maps saved in the map library for reuse. |

Rules and Notes:

- Directional rules do not work on single NIC VMs running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.
- If you are running GigaVUE Cloud Suite on OpenStack, you can add a subnet to the exclusion map. To do this, create an exclusion map and select the Subnet name in the ruleset.
- 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*.

Create a Map

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.

- **Name:** Name of the new map
- **Description:** Details of the map
- **Application Filtering:** Enable this option if you wish to use Application Filtering Intelligence. Enabling this option allows you to filter traffic based on Application name or family. For details, refer to [Application Filtering Intelligence](#).
- **Selected Virtual Machines:** Using this option, you can select an individual Network adapter of a virtual machine as a target. Both ingress and egress traffic of the network adapter chosen are redirected for monitoring. You can also view and filter the list of virtual machines available. When using this option, you cannot use Automatic Target Selection (ATS).

- **Virtual Machine List:** Save the list or filter.

- To save,

- Select **Virtual Machine List**.

The Virtual Machine List quick view opens.

- Select the virtual machines you wish to use as the target.
 - Select **Apply** in the Virtual Machine List quick view to save your changes.

- To filter,


- Select **Filter** and select one of the following criteria:

- Data Center
 - Cluster
 - Host Name
 - VM Name
 - VM Tag Category
 - VM Tag Name

- After selecting the details, select **Apply** in the filter dialog box to apply the filters.

The list of virtual machines appears based on the filter criteria.


- Select the virtual machines you wish to use as the target, and select **Apply** in the Virtual Machine List quick view to save your changes.
- VMware tools are not required to discover targets, as GigaVUE-FM can discover targets with ATS using the tags attached to the VMs.
- Targets are selected when you provide the VM's node name or the hostname as selection criteria. A host is selected when the hostname matches all the active targets.

- Pass and Drop rule selection with Automatic Target Selection (ATS) differs 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 and perform the following:
 - a. Create a new rule set:
 - i. Click **Actions > New Ruleset**.
 - ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
 - iii. Enter the Application Endpoint in the Application EndPoint ID field.
 - iv. Select a required condition from the drop-down list.
 - v. Select the rule to **Pass** or **Drop** through the map.
 - b. Create a new rule:
 - i. Click **Actions > New Rule**.
 - ii. Select a required condition from the drop-down list.
 - iii. Select  and select **Add Condition**.
 - iv. Select the rule to **Pass** or **Drop** through the map.
- 4. Select **Save**.

Through the map, packets is dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions.

You must select at least one rule condition to add ATS rules for an Inclusion/Exclusion map. For details, refer to [Example- Create a New Map using Inclusion and Exclusion Maps](#).

You can also perform the following actions on the Monitoring session canvas.

- To edit a map, select the  menu button of the required map on the canvas and select **Details**, or click **Delete** to delete the map.
- To apply the threshold template to maps, select the required map on the canvas and select **Details**. The quick view appears, select 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 rules 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** will be included.
6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
 - a. In the **GENERAL** tab, enter the name as Exclusionmap1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
 - b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then the instance **target-1-3** will be excluded.

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

Map Library

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

To add a map,

1. From the Monitoring Session screen, select **TRAFFIC PROCESSING**.
The GigaVUE-FMCanvas page appears.
2. From the page,, select the desired map and save it as a template.

3. Select **Details**.

The Application quick view appears.

4. Select **Add to Library** and perform one of the following:

- From the **Select Group** list, select an existing group.
- Select **New Group** to create a new one.

5. In the **Description** field, add details and select **Save**.

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

Reusing a map

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

Add Applications to Monitoring Session

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

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter
- SSL Decrypt
- GigaSMART NetFlow Generation
- 5G-Service Based Interface Application
- 5G-Cloud Application

For details on configuring these applications, refer to *GigaVUE V Series Applications Guide*.

Interface Mapping

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

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

To perform interface mapping:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Navigate to the **V SERIES NODES** tab and select **Interface Mapping**. The **Deploy Monitoring Session** dialog box appears.
3. Select the GigaVUE V Series Nodes to which you wish to map the interface.
4. From the drop-down menu of the GigaVUE V Series Node, select the interfaces for the following deployed in the Monitoring Session:
 - REPs (Raw Endpoints)
 - TEPs (Tunnel Endpoints)
5. Select **Deploy**.

NOTE: The updated mappings take effect when deployed.

Deploy Monitoring Session

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

To deploy the Monitoring Session,

1. **Add components to the canvas**
Drag and drop the following items to the canvas as required:
 - **Ingress tunnel** (as a source): From the **New** section.
 - **Maps:** From the **Map Library** section.
 - **Inclusion and Exclusion maps:** From the Map Library to their respective section at the bottom of the workspace.
 - GigaSMART **apps:** From the **Applications** section.
 - **Egress tunnels:** From the **Tunnels** section.

2. **Connect components**

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

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

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

3. **(Optional) Review Sources** Select the SOURCES tab to view details about the subnets and monitored instances.

The monitored instances and the subnets are visible in orange.

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

4. **Deploy the Monitoring Session**

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

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

View the Deployment Report

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

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

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

View Monitoring Session Statistics

The OVERVIEW page of Monitoring Session allows you to analyze the incoming and outgoing traffic across multiple time intervals. For example, hourly, daily, weekly, and monthly.

You can view the high-level information of the selected Monitoring Session, such as:

- Connections
- Tunnel details
- Health status
- Deployment status
- Information related to Application Intelligence statistics.

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

View Statistics with Multiple Filters

You can apply different filters per the data analysis requirements to view the statistics.

GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- Full Screen View
- Time Interval Options
- View with Traffic Data
- Per-Node Statistics
- Element-Level Insights

Option 1: View Full Screen

You can view the Statistics on full screen.

To view in full screen,

1. From the right side of the window, select the Actions drop-down list.
2. Select Full Screen.

Statistics appear in full screen.

Option 2: View using Time Interval

Select the options from the drop-down list box to view the incoming and outgoing traffic hourly, daily, weekly, and monthly.

| Interval | Frequency of data points |
|----------|--------------------------|
| Hourly | Every five minutes |
| Daily | Every one hour |
| Weekly | Every six hours |
| Monthly | Everyday |

Note: The most recent data point shown is slightly earlier than the current time (for example, viewing hourly stats at 11:30 will show the latest point at 11:25).

For each interval, the data displayed reflects the period starting from that data point. For instance, a data point marked 11:30 in daily view represents traffic from 11:30 to 12:30.

Option 3: View with Traffic Data

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.

Option 4: View Per-Node

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,

1. On the bottom-left corner of the OVERVIEW page, go to the GigaVUE V Series Node drop-down list.
2. Select the name of the V Series Node for which you want to view the statistics.

Option 5: Element-level statistics

You can view the statistics of the elements involved in the Monitoring Session.

To view the statistics,

1. Go to the Select Chart Options page.
2. Select the elements associated with the session.
3. On the graph, directly select the following options to view the statistics individually:
 - Incoming(Mbps)
 - Outgoing (Mbps)
 - Ratio (Out/In) (Mbps)

Raw EndPoint (REP)

A Raw EndPoint (REP) is part of the monitoring session but can also receive bypassed traffic that is not filtered by the map, so it records more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive bypassed (non-IPv4) traffic, the recorded number of packets from the V Series node can be more than expected.

Visualize the Network Topology (VMware ESXi)

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.

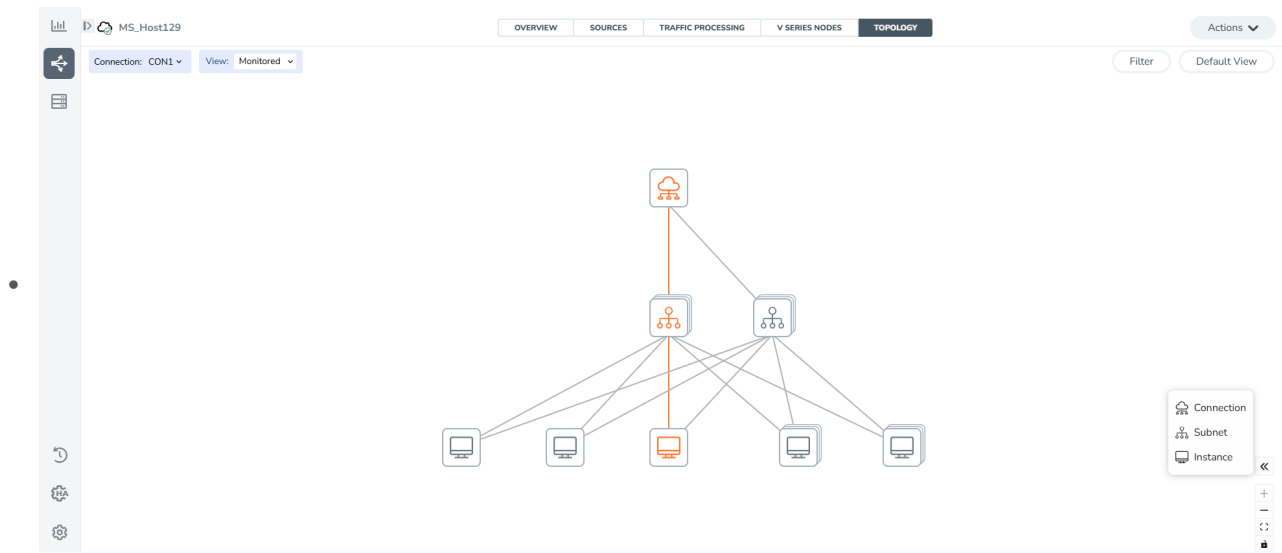
To view the topology in GigaVUE-FM:

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.
- Select the subnet or VM group icons to explore the subnets or instances within the group.

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.
- Apply Navigation controls, such as:
 - Use **+** or **-** icons to zoom in and zoom out of the topology view.
 - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, you must configure the Application Intelligence solution from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for a

virtual environment from the **Application Intelligence** page.

The following actions are available only when using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

It is highly recommended to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM seamlessly migrates all your virtual Application Intelligence sessions and their connections. If migration fails, all sessions return to their original states.



Points to Note:

- You must have write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. For details, refer to Create Roles section In GigaVUE Administration Guide
- The migration does not proceed:
 - If any of the existing Application Intelligence Session is in PENDING or SUSPENDED. Resolve the issue and start the migration process.
 - If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration. Resolve the issue and start the migration process.
 - If an existing Monitoring Session has the same name as the Application Intelligence Session. Change the existing Monitoring Session name to continue with the migration process.
- You cannot continue the session if any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set. In the Monitoring Session, the fifth Rule Set supports either Pass All or Advanced Rules as Drop. Delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for assistance.

Migrate your existing Application Intelligence Session to Monitoring Session Page

Follow these steps:

1. In the left navigation pane, select **Traffic > Solutions > Application Intelligence**. You cannot create a new Application Intelligence Session from this page. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
2. Review the message and select **Migrate**. The **Confirm Migration** dialog box appears with the list of Application Intelligence Session that you need to migrate.
3. Review the list and select **Migrate**. GigaVUE-FM verifies the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
4. Select **Go to Monitoring Session Page**.

You can view that all the virtual Application Intelligence Sessions in the Application Intelligence page are migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

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

1. Secure Tunnels in the Options page

If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow these steps:

- a. Enable Secure Tunnels in the **Options** page.

For more information, refer to [Configure Monitoring Session Options \(VMware ESXi\)](#)

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

The **Monitoring Sessions** page appears.

- c. Select the Monitoring Session for which you enabled Secure Tunnels.

- d. Select **Actions > Undeploy**.

The monitoring session is undeployed.

- e. Select the Monitoring Session for which you enabled Secure Tunnels.

- f. Select **Actions > Edit**.

The **Edit Monitoring Session** Canvas page appears.

- g. Add the Application Intelligence applications.

- h. Modify the Number of Flows as per the below table.

| Cloud Platform | Instance Size | Maximum Number of Flows |
|----------------|-----------------------------|-------------------------|
| VMware | Large (8 vCPU and 16GB RAM) | 200k |

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

- i. Select **Deploy**.

For details, 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 is possible while redeploying the monitoring session.

3. Configuration Changes Post-Migration

To make configuration changes post-migration, 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. GigaVUE-FM then uses this data to calculate traffic health.

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

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

This feature supports GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Third Party Orchestration

The following section provides step-by-step instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status. Refer to the following section for more detailed information:

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

Consideration to configure a threshold template

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session reapplies all the threshold policies associated with that Monitoring Session.
- Deleting the Monitoring Session clears all the threshold policies associated with that Monitoring Session.
- Threshold configuration is applied before deploying a Monitoring Session and remains even if the session is undeployed.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

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

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

| | | | |
|----------------------|--|--------------------------------|---------------------|
| | 3. Packets Dropped | | |
| Masking | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| Dedup | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| HeaderStripping | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| TunnelEncapsulation | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| LoadBalancing | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| SSLDecryption | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| Application Metadata | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| AMI Exporter | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| Geneve | 1. Tx Packets 2. Rx Packets 3. Packets Dropped | 1. Difference 2. Derivative | 1. Over 2. Under |
| 5G-SBI | 1. Tx Packets 2. Rx Packets | 1. Difference 2. Derivative | 1. Over 2. Under |

| | | | |
|--------|--|--------------------------------|---------------------|
| | 3. Packets Dropped | | |
| 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.
3. Enter the appropriate information for the threshold template as described in the following table:

| Field | Description |
|--------------------------------|---|
| Threshold Template Name | The name of the threshold template. |
| Thresholds | |
| 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. |

4. 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:

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

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

Apply Threshold Template to Applications

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

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

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

Clear Thresholds

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

Clear Thresholds for Applications

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

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

Clear Thresholds across the Monitoring Session

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

1. In GigaVUE-FM, on the left navigation pane, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Select the Monitoring Session and navigate to **TRAFFIC PROCESSING > Options > Thresholds**,
3. Select **Clear Thresholds**.
4. On the **Clear Threshold** pop-up appears, select **Ok**.

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

View Health Status

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

View Health Status of an Application

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

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

This displays the application's configuration and traffic health and the thresholds applied to it.

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

View Health Status for Individual GigaVUE V Series Nodes

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

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

Configure VMware Settings

This section describes how to configure the maximum number of connections, refresh intervals for instance and non-instance Inventory, and maximum batch size for monitoring session updates.

To configure the VMware Settings,

1. Go to **Inventory > VIRTUAL > VMware vCenter (V Series)**
2. Select **Settings > Advanced Settings** to edit the VMware vCenter settings.

Advanced Settings

Edit

| | |
|---|-------|
| Maximum number of vCenter connections allowed | 20 |
| Refresh interval for VM target selection inventory (secs) | 300 |
| Refresh interval for fabric deployment inventory (secs) | 86400 |
| Traffic distribution tunnel range start | 8000 |
| Traffic distribution tunnel range end | 8512 |

Refer to the following table for details:

| Settings | Description |
|--|---|
| Maximum number of vCenter connections allowed | Specifies the maximum number of vCenter connections you can establish in GigaVUE-FM |
| Refresh interval for VM target selection inventory (secs) | Specifies the frequency for updating the state of target VMs in VMware vCenter |
| Refresh interval for fabric deployment inventory (secs) | Specifies the frequency for updating the state of GigaVUE-FM fabrics deployed in VMware vCenter |
| Traffic distribution tunnel range start | Specifies the start range value of the tunnel ID. |
| Traffic distribution tunnel range end | Specifies the closing range value of the tunnel ID. |

Configure 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: 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**.

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](#) 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. 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) | <p>Statistical details of the virtual inventory based on the platform and the health status.</p> <p>You can view the following metric details at the top of the dashboard:</p> <ul style="list-style-type: none"> Number of Monitoring Sessions Number of V Series Nodes Number of Connections Number of GCB Nodes <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> Platform Health Status | <i>V Series Node Status by Platform</i> | Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms. |
| | | <i>Monitoring Session Status by Platform</i> | Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms |
| | | <i>Connection Status by Platform</i> | Number of healthy and unhealthy connections for each of the supported cloud platforms |
| | | <i>GCB Node Status by Platform</i> | Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms |
| V Series Node Statistics | <p>Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> Platform Connection V Series Node | <i>V Series Node Maximum CPU Usage Trend</i> | <p>Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.</p> <div> <p>NOTE: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.</p> </div> |
| | | <i>V Series Node with Most CPU Usage For Past 5 minutes</i> | <p>Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.</p> <div> <p>NOTE: You cannot use the time based filter</p> </div> |

| Dashboard | Displays | Visualizations | Displays |
|--------------|---|---|---|
| | | | options to filter and visualize the data. |
| | | <i>V Series Node Rx Trend</i> | Receiving trend of the V Series node in 5 minutes interval, for the past one hour. |
| | | <i>V Series Network Interfaces with Most Rx for Past 5 mins</i> | Total packets received by each of the V Series network interface for the past 5 minutes. NOTE: You cannot use the time based filter options to filter and visualize the data. |
| | | <i>V Series Node Tunnel Rx Packets/Errors</i> | Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation. |
| | | <i>V Series Node Tunnel Tx Packets/Errors</i> | TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors |
| Dedup | <p>Displays visualizations related to Dedup application.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> Platform Connection V Series Node | <i>Dedup Packets Detected/Dedup Packets Overload</i> | Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload. |
| | | <i>Dedup Packets Detected/Dedup Packets Overload Percentage</i> | Percentage of the de-duplicated packets received against the de-duplication application overload. |
| | | <i>Total Traffic In/Out Dedup</i> | Total incoming traffic against total outgoing |

| Dashboard | Displays | Visualizations | Displays |
|-------------------------|---|-----------------------|---|
| | | | traffic |
| Tunnel (Virtual) | <p>Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V Series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • V Series node: Management IP of the V Series node. Choose the required V Series node from the drop-down. • Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. <p>The following statistics are displayed for the tunnel:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets | <i>Tunnel Bytes</i> | <p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero. |
| | | <i>Tunnel Packets</i> | <p>Displays packet-level statistics for input and output tunnels that are part of a monitoring session.</p> |
| App (Virtual) | <p>Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node.</p> | <i>App Bytes</i> | <p>Displays received traffic vs transmitted traffic, in Bytes.</p> |

| Dashboard | Displays | Visualizations | Displays |
|----------------------------|--|-----------------------|---|
| | <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets | | |
| | | <i>App Packets</i> | Displays received traffic vs transmitted traffic, as the number of packets. |
| End Point (Virtual) | <p>Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V Series nodes.</p> <p>The following statistics that are shown for Endpoint (Virtual):</p> <ul style="list-style-type: none"> • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets <p>The endpoint drop-down shows <V Series Node Management IP address : Network Interface> for each endpoint.</p> | <i>Endpoint Bytes</i> | Displays received traffic vs transmitted traffic, in Bytes. |

| Dashboard | Displays | Visualizations | Displays |
|-----------|---|------------------|---|
| | <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> • Monitoring session • V Series node • Endpoint: Management IP of the V Series node followed by the Network Interface (NIC) | | |
| | | Endpoint Packets | Displays received traffic vs transmitted traffic, as the number of packets. |

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

Debuggability and Troubleshooting

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

Sysdumps

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

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

Sysdumps—Rules and Notes

Consider the following points before you generate sysdumps:

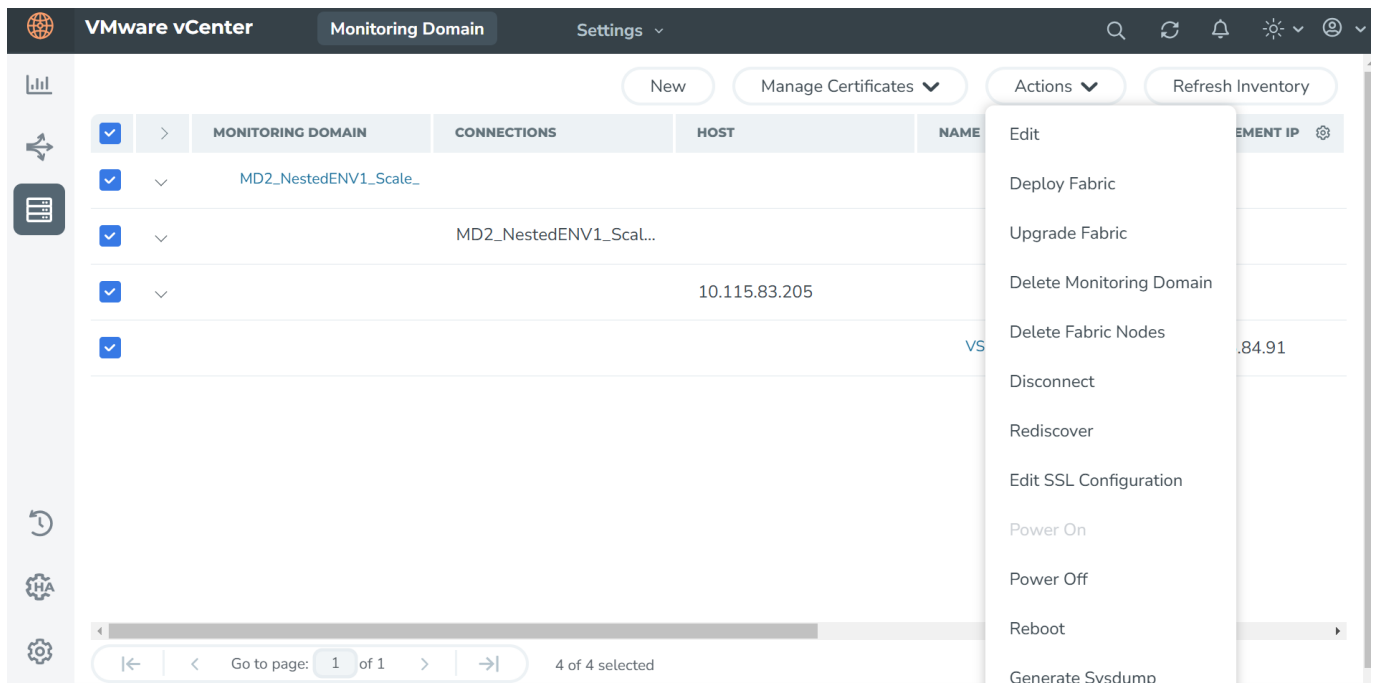
- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when generation of another sysdump file is in progress.

- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- You can download only one sysdump file per GigaVUE V Series Node at a time.
- You can delete sysdump files in bulk for a GigaVUE V Series Node.
- To ensure efficient usage, the system limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

Generate a Sysdump File

To generate a sysdumps file:

1. 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**.



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

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. For more details, refer to the Secure Communication between GigaVUE Fabric Components section.

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 Network Firewall Requirements . |

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

| GigaVUE Cloud Suite 6.11 Hardware and Software Guides | |
|--|---|
| GigaVUE-TA200 Hardware Installation Guide | |
| GigaVUE-TA200E Hardware Installation Guide | |
| GigaVUE-TA400 Hardware Installation Guide | |
| GigaVUE-TA400E Hardware Installation Guide | |
| GigaVUE-OS Installation Guide for DELL S4112F-ON | |
| G-TAP A Series 2 Installation Guide | |
| GigaVUE M Series Hardware Installation Guide | |
| GigaVUE-FM Hardware Appliances Guide | |
| Software Installation and Upgrade Guides | |
| GigaVUE-FM Installation, Migration, and Upgrade Guide | |
| GigaVUE-OS Upgrade Guide | |
| GigaVUE V Series Migration Guide | |
| Fabric Management and Administration Guides | |
| GigaVUE Administration Guide | covers both GigaVUE-OS and GigaVUE-FM |
| GigaVUE Fabric Management Guide | how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features |
| GigaVUE Application Intelligence Solutions Guide | |
| Cloud Guides | |
| how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms | |
| GigaVUE V Series Applications Guide | |
| GigaVUE Cloud Suite Deployment Guide - AWS | |
| GigaVUE Cloud Suite Deployment Guide - Azure | |
| GigaVUE Cloud Suite Deployment Guide - OpenStack | |
| GigaVUE Cloud Suite Deployment Guide - Nutanix | |
| GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) | |
| GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T) | |
| GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration | |

| GigaVUE Cloud Suite 6.11 Hardware and Software Guides | |
|--|---|
| Universal Cloud TAP - Container Deployment Guide | |
| Gigamon Containerized Broker Deployment Guide | |
| GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions | |
| GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions | |
| Reference Guides | |
| GigaVUE-OS CLI Reference Guide | library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices |
| GigaVUE-OS Security Hardening Guide | |
| GigaVUE Firewall and Security Guide | |
| GigaVUE Licensing Guide | |
| GigaVUE-OS Cabling Quick Reference Guide | guidelines for the different types of cables used to connect Gigamon devices |
| GigaVUE-OS Compatibility and Interoperability Matrix | compatibility information and interoperability requirements for Gigamon devices |
| GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide | samples uses of the GigaVUE-FM Application Program Interfaces (APIs) |
| Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices | Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices. |
| Release Notes | |
| GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes | new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release |
| NOTE: Release Notes are not included in the online documentation. | |
| NOTE: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon . Refer to How to Download Software and Release Notes from My Gigamon . | |
| In-Product Help | |
| GigaVUE-FM Online Help | how to install, deploy, and operate GigaVUE-FM. |

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

documentationfeedback@gigamon.com

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

| Documentation Feedback Form | | |
|-----------------------------|--------------|--|
| About You | Your Name | |
| | Your Role | |
| | Your Company | |
| | | |

| | | |
|----------------------------|--|--|
| For Online Topics | Online doc link | (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 VÜECommunity is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)