GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite

Product Version: 6.11

Document Version: 1.0

(See Change Notes for document updates.)

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

Change Notes

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

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

Contents

GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite for VMware provides an intelligent filtering technology that allows virtual machine (VM) traffic flows of interest to be selected, forwarded, and delivered to the monitoring infrastructure centrally attached to the Gigamon Deep Observability Pipeline, thereby eliminating any traffic blind spots in the enterprise private clouds or service provider NFV deployments.

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

Topics:

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:

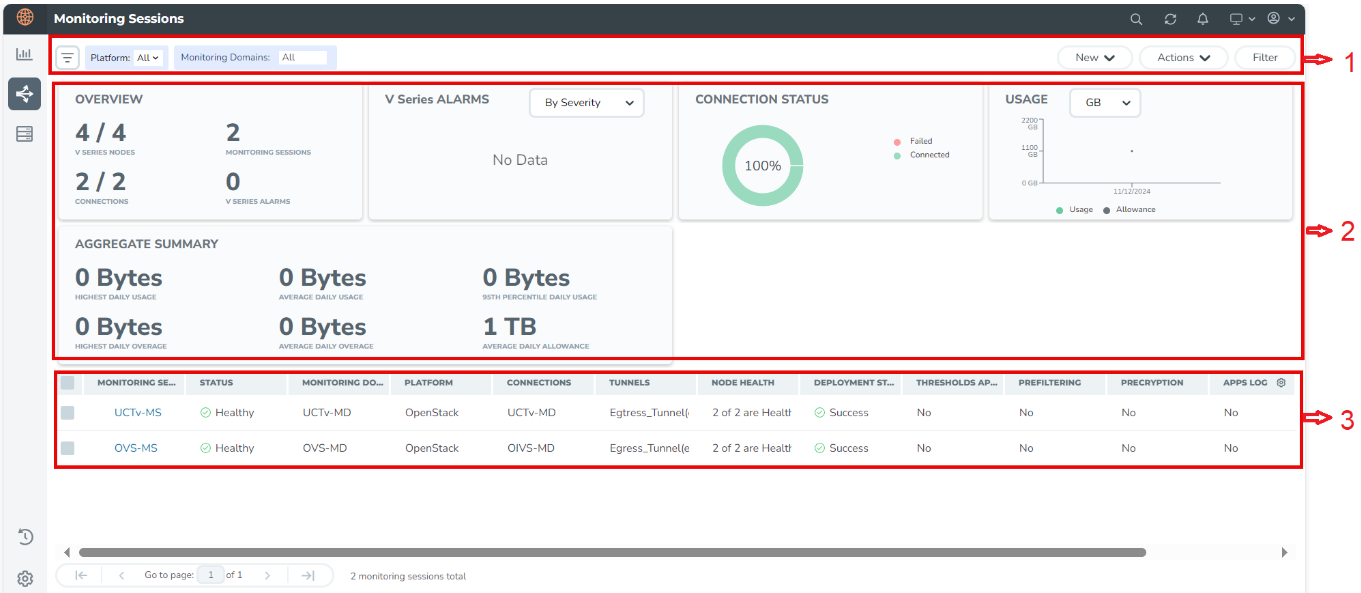
- Basic statistics
- V Series alarms
- Connection status
- Volume usage vs. allowance
- A summary table of active monitoring sessions

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:
    1. Go to Traffic > Virtual > Overview.
    2. On the top-left menu, select the name of your cloud from the Platform drop-down option.



Platform: All
Monitoring Domains: All

OVERVIEW

4 / 4 V SERIES NODES
2 MONITORING SESSIONS
2 / 2 CONNECTIONS
0 V SERIES ALARMS

V Series ALARMS By Severity

No Data

CONNECTION STATUS

USAGE GB

AGGREGATE SUMMARY

0 Bytes HIGHEST DAILY USAGE
0 Bytes AVERAGE DAILY USAGE
0 Bytes 95TH PERCENTILE DAILY USAGE
0 Bytes HIGHEST DAILY OVERAGE
0 Bytes AVERAGE DAILY OVERAGE
1 TB AVERAGE DAILY ALLOWANCE

MONITORING SE...	STATUS	MONITORING DO...	PLATFORM	CONNECTIONS	TUNNELS	NODE HEALTH	DEPLOYMENT ST...	THRESHOLDS AP...	PREFILTERING	PRECRYPTION	APPS LOG
UCTv-MS	✓ Healthy	UCTv-MD	OpenStack	UCTv-MD	Egtress_Tunnel(	2 of 2 are Healtl	✓ Success	No	No	No	No
OVS-MS	✓ Healthy	OVS-MD	OpenStack	OIVS-MD	Egress_Tunnel(e	2 of 2 are Healtl	✓ Success	No	No	No	No

Go to page: 1 of 1

2 monitoring sessions total

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
	• **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*Monitor Cloud* 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. 1. From the **Platform** drop-down list, select the required platform.
2. 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 Filter

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.

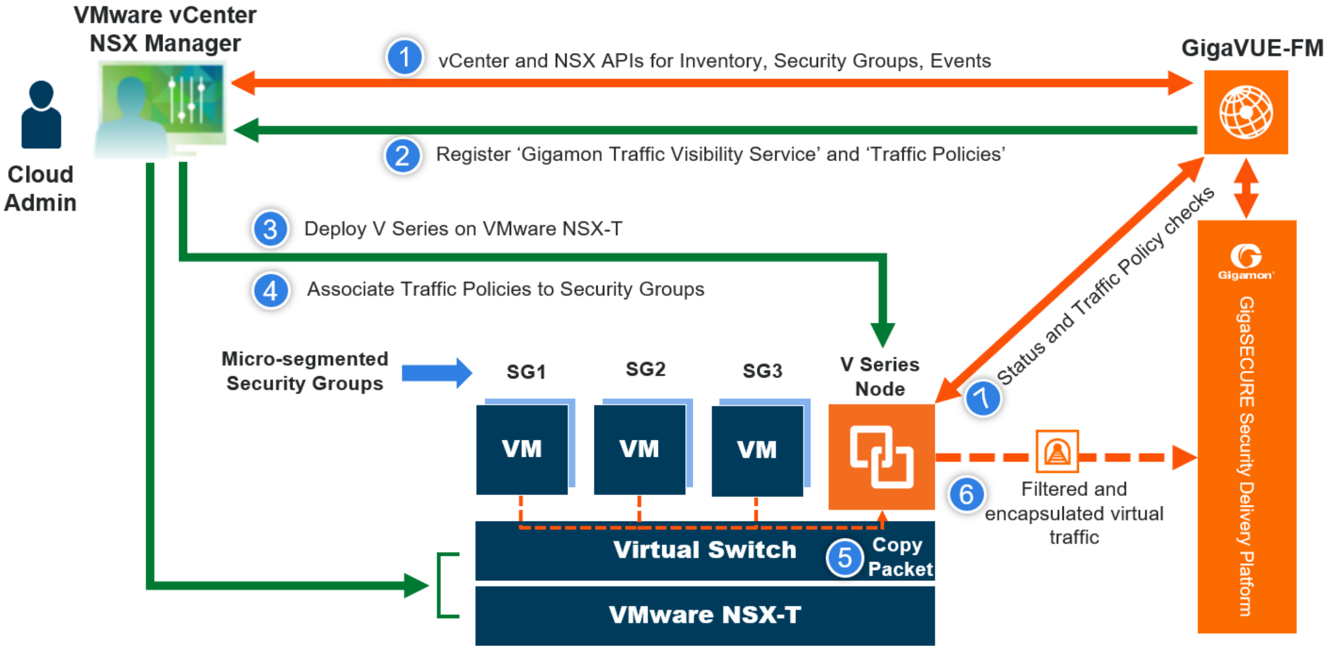
NOTE: Select the settings icon ⚙ and customize the options visible in the table.

Architecture for GigaVUE Cloud Suite for VMware NSX-T

This section provides an overview of the GigaVUE V Series Node deployment on the VMware NSX-T platform and describes the procedure for setting up the traffic monitoring sessions using the GigaVUE V Series Nodes. The GigaVUE V Series Nodes support traffic visibility on the NSX-T NVDS switch.

GigaVUE-FM creates, manages and deletes the GigaVUE V Series Nodes in the VMware NSX-T based on the configuration information provided by the user. GigaVUE-FM can communicate directly with the GigaVUE V Series Nodes.

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


VMware vCenter
NSX Manager
Cloud Admin
GigaVUE-FM
1 vCenter and NSX APIs for Inventory, Security Groups, Events
2 Register 'Gigamon Traffic Visibility Service' and 'Traffic Policies'
3 Deploy V Series on VMware NSX-T
4 Associate Traffic Policies to Security Groups
7 Status and Traffic Policy checks
Micro-segmented Security Groups
SG1
SG2
SG3
VM
VM
VM
V Series Node
Virtual Switch
5 Copy Packet
VMware NSX-T
6 Filtered and encapsulated virtual traffic
Gigamon
GigaSECURE Security Delivery Platform

Introduction to Supported Features in GigaVUE Cloud Suite for VMware NSX-T

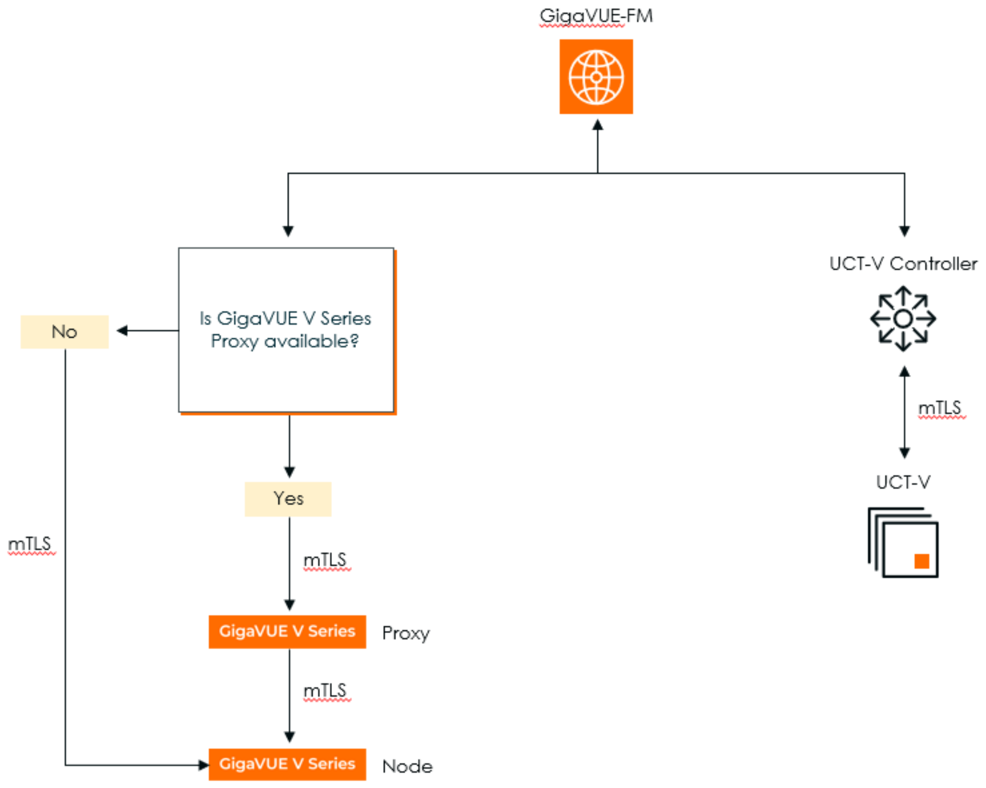
GigaVUE Cloud Suite for VMware (NSX-T) supports the following features:

- Increase or Decrease GigaVUE V Series Node
- Sharing the Same Host across Different Monitoring Domains
- Analytics for Virtual Resources
- Cloud Health Monitoring

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.

Increase or Decrease GigaVUE V Series Node

You can add more nodes or remove nodes from an existing monitoring domain using GigaVUE-FM or VMware NSX-T manager, based on method you have deployed the GigaVUE V Series Nodes.

Refer to the following topics for more detailed information:

- Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM
- Increase or Decrease GigaVUE V Series Nodes using VMware NSX-T Manager

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.

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects.

Refer to Analytics for Virtual Resources for more detailed information.

Cloud Health Monitoring

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

For more information on how to configure cloud health monitoring, refer to the topic Monitor Cloud Health.

Customer Orchestrated Source - Use Case

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

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

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

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 SKUs [1]. 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:

[1] Stock 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

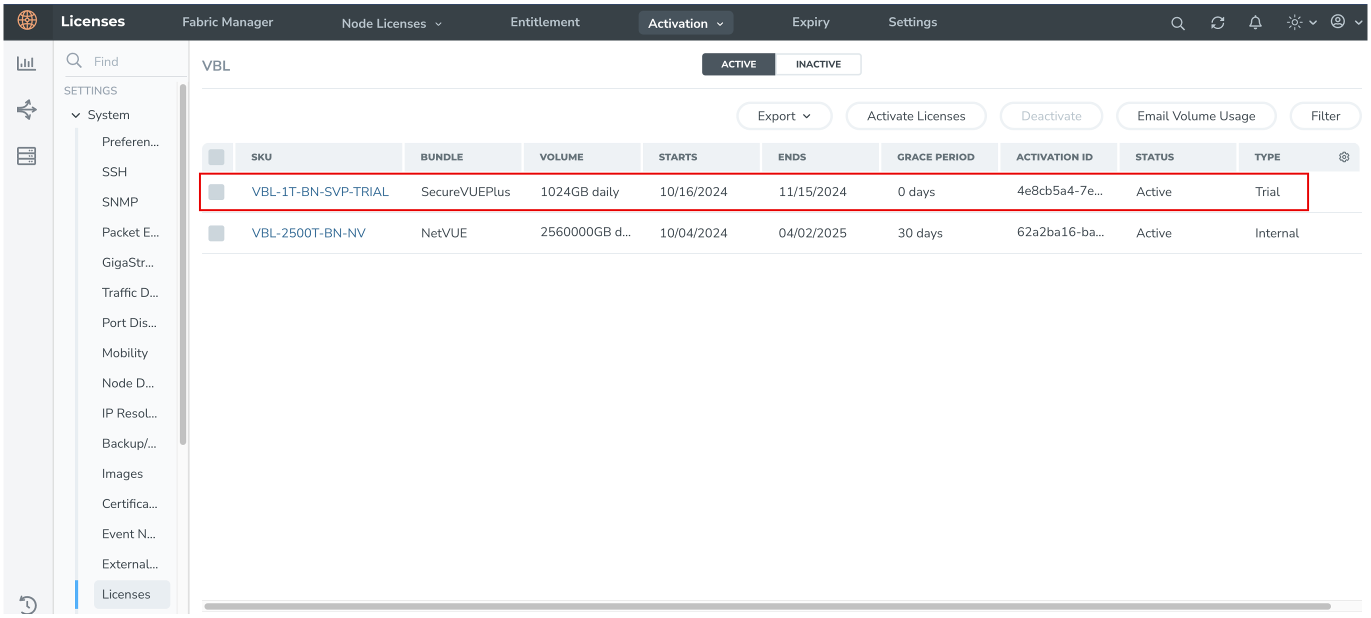
GigaVUE-FM applies the following methods to track the license usage for each GigaVUE V Series Node:

- 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, dentify 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, 6.10.00, v6.11.00

Points to Note (VMware NSX-T)

- The steps in the documentation assume that VMware NSX-T is installed and configured. Refer to VMware Documentation for configuration details.
- GigaVUE-FM supports service insertion only for overlay transport zone associated with the E-W traffic. Service insertion is not supported for VLAN transport zone associated with the N-S traffic or when the VMware NSX-T manager in federation mode. However, the traffic from the workload virtual machines in NSX-T federated environments can be acquired using UCT-V. Refer to Configure GigaVUE Fabric Components using Third party Orchestration on NSX-T Federation Environment in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration for more detailed information on how to deploy UCT-V, UCT-V Controller to acquire traffic from NSX-T federated environment.

Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T

The following are the prerequisites for integrating GigaVUE V Series Nodes with VMware NSX-T:

- ESXi hosts must be prepared as NSX-T Data Center transport nodes by using transport node profiles.
- ESXi hosts where workload VMs that needs to be monitored must be attached to the overlay transport zone.
- GigaVUE-FM supports service insertion only for overlay transport zone associated with the E-W traffic. Service insertion is not supported on VLAN transport zone associated with the N-S traffic or when the VMware NSX-T manager in federation mode.
- Before deploying GigaVUE V Series Nodes using GigaVUE-FM, Service segment must be created in the NSX-T manager on Overlay Transport Zone. Refer to Create a Service Segment in VMware NSX-T for step-by-step instructions on how to create service segment.
- Refer to Supported Hypervisors for VMware for supported VMware vCenter, VMware ESXi and VMware NSX-T versions.
- Only IPv4 traffic is supported.
- If a guest VM running on an ESXi host is connected to a VLAN segment. and that ESXi host is not configured to an Overlay Transport zone, then the traffic destined to a service VM is disrupted. Such a configuration can also cause traffic to be routed to a black hole.
- For more detailed VMware requirements on East-West traffic monitoring, refer to the below links and select the appropriate NSX-T version.
  - NSX-T Data Center Requirements for East-West Traffic - For versions 3.x.x
  - NSX Requirements for East-West Traffic - For versions 4.x.x
- Refer to Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T for ESXi host resource requirement to deploy GigaVUE V Series Nodes.
- GigaVUE V Series Node device OVA image file.

  > **NOTE:** An external HTTP(S) server for hosting the GigaVUE V Series image OVFs and VMDK file (extracted from the OVA file) when using **Use External Image** Option in Monitoring Domain. Refer to Create Monitoring Domain for VMware NSX-T for more detailed information on what is an external image and how to configure it.

  The GigaVUE V Series Node OVA image files can be downloaded from Gigamon Customer Portal.

Unsupported Configurations when using VMware NSX-T:

- Service Insertion is not supported on Global NSX-T managers in federation mode. Use Local NSX-T Managers for deploying our solution in this case.
- Service Insertion is not supported on Multi tenancy environments.
- Multiple monitoring domains cannot be configured with same NSX-T manager.

Refer to the following topics for the requirements:

- Network Firewall Requirements
- Recommended Form Factor (Instance Types)
- Required VMware Virtual Center Privilege
- Required Roles in VMware NSX-T
- Disable Certification Validation in VMware NSX-T
- Default Login Credentials

Network Firewall Requirements

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	NSX-T Manager	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and NSX-T.
	vCenter					
GigaVUE-FM	GigaVUE V Series Node	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)	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	Management connection to GigaVUE-FM
			22		ssh	
Administrator	GigaVUE V Series Nodes	Not Applicable	22		ssh	Troubleshooting GigaVUE V Series Nodes.
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive

						the traffic health updates with GigaVUE V Series Node
Remote Source	GigaVUE V Series Node	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 for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Node	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
			N/A	IP 47	GRE	
GigaVUE V Series Node	Tool/ GigaVUE HC Series instance	N/A	N/A	ICMP	echo Request	Allows V Series node to health check tunnel destination traffic (Optional)
					echo Response	
GigaVUE V Series Node	GigaVUE-FM	Any (1024-65535)	5671	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.
GigaVUE-FM	External Image Server URL	Any (1024-65535)	Custom port on web Server	TCP	http	Access to image server to image lookup and checks, and downloading the image
NSX-T Manager						

vCenter						
NSX-T Manager	GigaVUE-FM	Any (1024-65535)	443	TCP	http	When using GigaVUE-FM as the image server for uploading the GigaVUE V Series Image.
vCenter						

Recommended Form Factor (Instance Types)

The form factor (instance type) size of the GigaVUE V Series Node is configured on the OVF file and packaged as part of the OVA image file. The following table lists the available form factors and sizes based on memory and the number of vCPUs for a single V Series node. Instances sizes can be different for GigaVUE V Series Nodes in different ESXi hosts and the default size is Small.

Type	Memory	vCPU	Disk space
Small	4GB	2vCPU	8GB
Medium	8GB	4 vCPU	8GB
Large	16GB	8 vCPU	8GB

Required VMware Virtual Center Privilege

This section lists the minimum privileges required for the GigaVUE-FM user in vCenter.

Category	Required Privilege	Purpose
vApp	• vApp application configuration	V Series Node Deployment
Virtual machine	**Interaction** ▪ Power on ▪ Power Off	• V Series Node Deployment • Used to power on and power off GigaVUE V Series Node.

Required Roles in VMware NSX-T

This section lists the minimum roles required for the GigaVUE-FM user in VMware NSX-T.

Deploying GigaVUE V Series Node using GigaVUE-FM

When deploying GigaVUE V Series Node using GigaVUE-FM, the following is the minimum required role combination:

For **NSX-T version 3.2.x** and **NSX-T version 4.x.x**, select the following Role combination:

- NETX Partner Admin and Security Admin

For **NSX-T version 3.1.x**, select LDAP with any one of the following Role combinations:

- NETX Partner Admin and Security Operator
- NETX Partner Admin and Network Operator

Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM section for more detailed information on how to deploy GigaVUE V Series Nodes using GigaVUE-FM

Deploying GigaVUE V Series Nodes using VMware NSX-T

When deploying GigaVUE V Series Node using VMware NSX-T manager, the minimum required role is NETX Partner Admin.

Refer to Deploy GigaVUE V Series Nodes using VMware NSX-T Manager section for more detailed information on how to deploy GigaVUE V Series Nodes using VMware NSX-T Manager.

Disable Certification Validation in VMware NSX-T

When using uncertified GigaVUE V Series Node image, due to certificate validation requirement in VMware NSX-T, GigaVUE V Series Node deployment may fail. Before deploying the GigaVUE V Series Nodes, disable the certificate validation as follows.

1. Login to each NSX-T manager using CLI with root credentials.
2. Open **/config/vmware/auth/ovf_validation.properties** file
3. Set a value for **THIRD_PARTY_OVFS_VALIDATION_FLAG** as **2**. The definition of the legends are as follows:
   - 0: only VMware-signed OVFs are allowed for deployment
   - 1: only VMware-signed and well-known CA-signed OVFs are allowed for deployment
   - 2: no validation
4. Save and Exit the file.

Default Login Credentials

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

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!

Install and Upgrade GigaVUE-FM

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

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

- Installation: Refer to GigaVUE-FM Installation and Upgrade Guide available in the Gigamon Documentation Library.
- Upgrade: Refer toUpgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

Deployment Options for GigaVUE Cloud Suite for VMware (NSX-T)

This section provides detailed information on the multiple ways in which GigaVUE Cloud Suite for VMware can be configured to provide visibility for physical and virtual traffic. Based on the method in which you want to deploy the GigaVUE V Series Nodes, there are two ways in which you can configure GigaVUE Cloud Suite for VMware (NSX-T). Refer to the Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T section for prerequisites that are required to be configured. For more detailed information and the work flow refer the following topics:

- Deploy GigaVUE V Series Nodes using GigaVUE-FM
- Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

Deploy GigaVUE V Series Nodes using GigaVUE-FM

Step No	Task	Refer the following topics
1	Create users in GigaVUE-FM and VMware NSX-T for communication.	Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM
2	Upload the GigaVUE V Series Node Image (OVA FIle) into GigaVUE-FM (optional- use only when using GigaVUE-FM as the image server)	Upload GigaVUE V Series Node Image into GigaVUE-FM
3	Create a service segment in NSX-T	Create a Service Segment in VMware NSX-T
4	Create a Monitoring Domain	Create Monitoring Domain for VMware NSX-T
5	Deploy GigaVUE V Series Nodes using GigaVUE-FM	Configure GigaVUE V Series Nodes for VMware NSX-T Refer to *Deploy GigaVUE V Series Nodes using GigaVUE-FM* section
6	Create Monitoring session	Create a Monitoring Session (VMware NSX-T)
7	Create a Ingress and Egress Tunnels to tunnel traffic	Create Ingress and Egress Tunnel (VMware NSX-T)
8	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
9	Deploy Monitoring Session	Deploy Monitoring Session
10	View Monitoring Session Statistics	View Monitoring Session Statistics
11	Create NSX-T Group and Service chain	Create Service Chain and NSX-T Group

Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

Step No	Task	Refer the following topics
1	Create users in GigaVUE-FM and VMware NSX-T for communication.	Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM
2	Upload the GigaVUE V Series Node Image (OVA FIle) into GigaVUE-FM (optional- use only when using GigaVUE-FM as the image server)	Upload GigaVUE V Series Node Image into GigaVUE-FM
3	Create a service segment in NSX-T	Create a Service Segment in VMware NSX-T
4	Create a Monitoring Domain	Create Monitoring Domain for VMware NSX-T

Step No	Task	Refer the following topics
5	Deploy GigaVUE V Series Nodes using GigaVUE-FM	Configure GigaVUE V Series Nodes for VMware NSX-T Refer to *Deploy GigaVUE V Series Nodes using VMware NSX-T* Manager section
6	Create Monitoring session	Create a Monitoring Session (VMware NSX-T)
7	Create a Ingress and Egress Tunnels to tunnel traffic	Create Ingress and Egress Tunnel (VMware NSX-T)
8	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
9	Deploy Monitoring Session	Deploy Monitoring Session
10	View Monitoring Session Statistics	View Monitoring Session Statistics
11	Create NSX-T Group and Service chain	Create Service Chain and NSX-T Group

Deploy GigaVUE Cloud Suite for VMware (NSX-T)

To integrate V Series nodes with NSX-T, perform the following steps:

- Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM
- Create a Service Segment in VMware NSX-T
- Upload GigaVUE V Series Node Image into GigaVUE-FM
- Create Monitoring Domain for VMware NSX-T
- Configure GigaVUE V Series Nodes for VMware NSX-T
- Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM
- Increase or Decrease GigaVUE V Series Nodes using VMware NSX-T Manager

Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM

For VMware NSX-T and GigaVUE-FM to communicate, an user must be created in VMware NSX-T Manager, VMware vCenter, and GigaVUE-FM.

NOTE: GigaVUE-FM connects to NSX-T Manager that supports TLSv1.0, TLSv1.1, and TLSv1.2.

Refer to the following topics for step-by-step instructions on how to create users in vCenter, NSX-T Manager and GigaVUE-FM:

- Create User in VMware vCenter
- Create User in NSX-T manager
- Create user in GigaVUE-FM

Create User in VMware vCenter

For GigaVUE-FM to communicate with vCenter, you must first create a user with the minimum required privileges in VMware vCenter.

Refer to Required VMware Virtual Center Privilege for the minimum privileges required in Vmware vCenter.

Create User in NSX-T manager

For GigaVUE-FM to communicate with NSX-T, you must first create a user with the minimum required role in NSX-T manager.

To create a user in VMware NSX-T:

1. In NSX-T, navigate to **System > Settings > User Management** and click **User Role Assignment** tab.
2. On the **User Role Assignment** tab, click **ADD**. Select the Roles based on the GigaVUE V Series Node deployment type as mentioned in Required Roles in VMware NSX-T
3. Click **Save** and then a GigaVUE-FM user is created in NSX-T.

Create user in GigaVUE-FM

For VMware NSX-T Manager to be able to communicate with GigaVUE-FM, you need to create a user in GigaVUE-FM who has the admin role.

Refer to Add Users section in *GigaVUE Administration Guide* for detailed and step-by-step instructions on how to create users in GigaVUE-FM.

Tips: You can follow these tips to easily identify the user created for VMware NSX-T.

- In the **Name** field, enter the name of the call back user. For example, you can use NSX-T Manager Callback as the user name to help you associate this user with the NSX-T Manager.
- In the **Username** field, enter a username for the user. For example, you can use nsxv to help you remember that this user is associated with NSX-T.

The username and password created for vCenter, NSX-T Manager, and GigaVUE-FM in this section will be used when creating Monitoring Domain in GigaVUE-FM. Refer to Create Monitoring Domain for VMware NSX-T for step-by-step instructions on how to create monitoring domain.

Create a Service Segment in VMware NSX-T

Registering the NSX-T details on GigaVUE-FM is a prerequisite to create the service segment.

To create a service segment in VMware NSX-T:

1. On the NSX manager, go to **Security** and select **Network Introspection** from the left navigation pane. The **Network Introspection Settings** page opens. Select **Service Segment** from the top navigation bar. Then, the Service Segment page appears.
2. On the Service Segment page, click **ADD SERVICE SEGMENT** and a new row appears to create a service segment.
3. Enter the name and map it to the overlay transport zone created for the VMs.
4. Click **Save**.

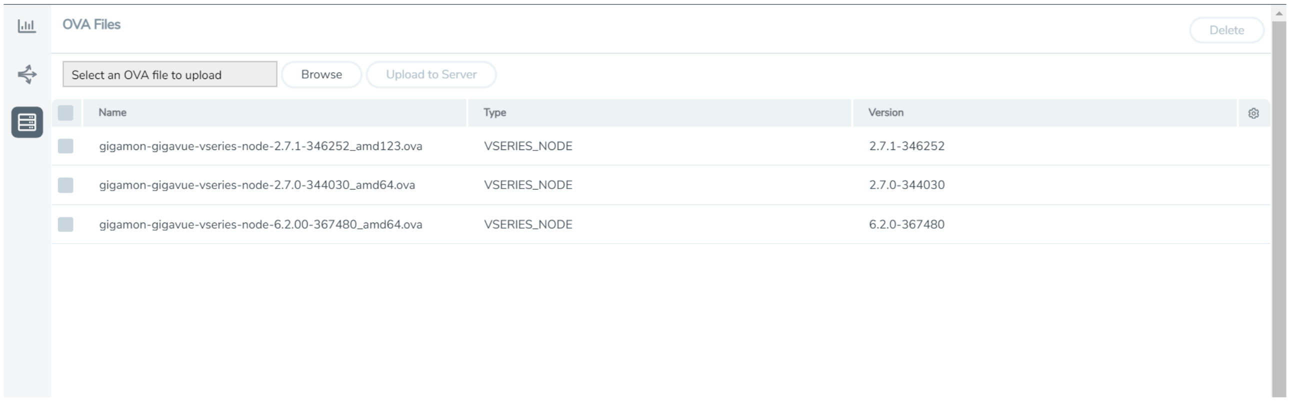
The segment created in this section will be used as service attachment when deploying GigaVUE V Series Nodes using GigaVUE-FM. Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information on how to deploy GigaVUE V Series Node using GigaVUE-FM.

Upload GigaVUE V Series Node Image into GigaVUE-FM

You can upload your V Series Node image into GigaVUE-FM. This step is optional, follow the steps given below only if you wish to use GigaVUE-FM as an internal image server.

To upload the V Series image into GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Settings > OVA Files**. The OVA Files page appears.



□	Name	Type	Version
□	gigamon-gigavue-vseries-node-2.7.1-346252_amd123.ova	VSERIES_NODE	2.7.1-346252
□	gigamon-gigavue-vseries-node-2.7.0-344030_amd64.ova	VSERIES_NODE	2.7.0-344030
□	gigamon-gigavue-vseries-node-6.2.00-367480_amd64.ova	VSERIES_NODE	6.2.0-367480

2. In the OVA Files page, click **Browse**to select the *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova*file.
3. Click **Upload** to Server to upload the selected OVA image file to GigaVUE-FM server.

> **NOTE:** The maximum number of OVA files that can be uploaded to GigaVUE-FM for VMware NSX-T is three.

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 NSX-T

This chapter describes how to create a Monitoring Domain for deploying GigaVUE V Series Nodes in the VMware NSX-T environment through GigaVUE-FM. You must establish a connection between GigaVUE-FM and the VMware NSX-T Manager. Creating a Monitoring Domain in GigaVUE-FM allows you to establish a connection between your VMware NSX-T environment and GigaVUE-FM.

Points to Note:

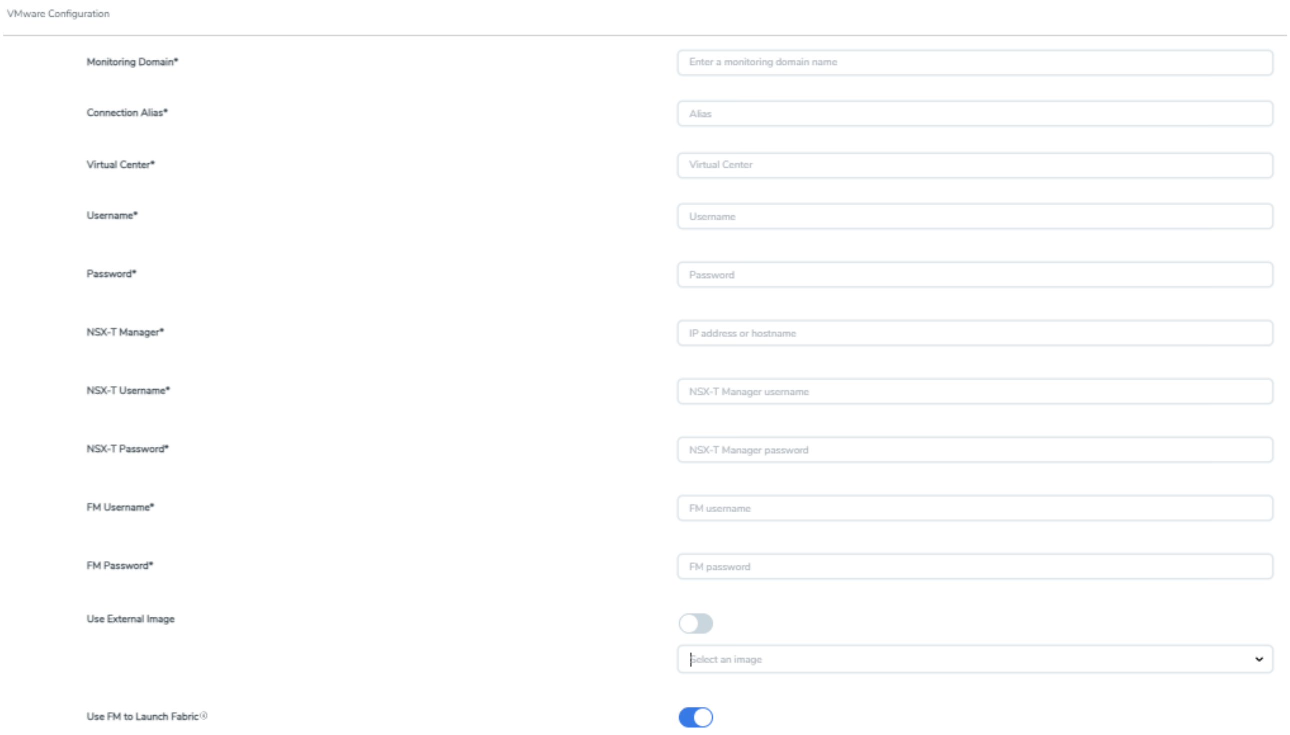
- You can create multiple Monitoring Domains using a single VMware NSX-T Manager. However, each Monitoring Domain must have unique VMware vCenters associated with it.
- When editing a Monitoring Domain that has GigaVUE V Series Nodes deployed, the **Use External Image** and **Use FM to Launch Fabric** toggle buttons are disabled. However, for a Monitoring Domain that does not have any GigaVUE V Series Nodes deployed, the **Use External Image** toggle button is enabled.
- Whenever you change the NSX-T user password in VMware NSX-T manager, you should update that in GigaVUE-FM by editing the Monitoring Domain. Otherwise, the NSX-T connection status will be in an authentication failure state.

Prerequisites:

- If you wish to use the **Use External Image** option, before creating a Monitoring Domain ensure all the contents of the OVA file are extracted into VMDK and OVF files and placed in the directory that represents the Image URL.
- If you wish to use GigaVUE-FM as your image server, save the OVA files in the dedicated directory before creating a Monitoring Domain. Refer to Upload GigaVUE V Series Node Image into GigaVUE-FMfor more detailed instructions on uploading the OVA files to GigaVUE-FM.

To create a Monitoring Domain in GigaVUE-FM for VMware NSX-T:

1. Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, click **New**. The **VMware Configuration** page appears.



VMware Configuration

Monitoring Domain*	Enter a monitoring domain name
Connection Alias*	Alias
Virtual Center*	Virtual Center
Username*	Username
Password*	Password
NSX-T Manager*	IP address or hostname
NSX-T Username*	NSX-T Manager username
NSX-T Password*	NSX-T Manager password
FM Username*	FM username
FM Password*	FM password
Use External Image	○ Select an image
Use FM to Launch Fabric	●

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	IP address or Hostname of the vCenter. **NOTE:** To ensure the validity of Nutanix Prism central certificates issued by a trusted Certificate Authority (CA), you must enable the Trust Store. Refer to the Trust Store section in GigaVUE Administration Guide for more detailed information.
Username	Username of the vCenter user.
Password	vCenter password that is used to connect to the vCenter.
NSX-T Manager	IP address or Hostname of your VMware NSX-T.
NSX-T Username	Username of your NSX-T account.
NSX-T Password	Password of your NSX-T account.
FM Username	Username of your GigaVUE-FM account.
FM Password	Password of your GigaVUE-FM account.
Use External Image	This toggle button allows you to choose between an external or internal image. If you wish to use the **Use External Image** option, you can use an external server (http or https server) to place all the OVF files and provide the URL of the web server. Otherwise, you can upload the OVA files to GigaVUE-FM and use it as an internal image server. a. **Yes**: Select this option to use an external image. To use an external image, enter the web server URL of the directory where VMDK and OVF files are available. The Web Server URL must be in the following format: *http (s)://<server-IP:port>/<path to where the OVF files are saved>* and the port can be any valid number. The default port number is 80. b. **No**: Select this option to use an internal image. To use an internal image, select the uploaded OVA files from the **Select an image** drop-down list.
Use FM to Launch Fabric	Enable this toggle button if you wish to deploy GigaVUE V Series Nodes using GigaVUE-FM. **NOTE:** If you disable this option, then you must deploy GigaVUE V Series Nodes using VMware NSX-T manager. Refer to Deploy GigaVUE V Series Nodes using VMware NSX-T Manager section for more detailed information.

4. Click **Save**.

Notes:

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

The newly created Monitoring Domain appears in the list view of the **Monitoring Domain** page. The **Status** column displays the overall connection status for both VMware vCenter and VMware NSX-T Manager. To view the individual connection statuses for each, hover over the connection status.

When creating multiple Monitoring Domains with the same NSX-T Manager, each Monitoring Domain is associated with a unique service name. You can view the service name of each Monitoring Domain on the **Monitoring Domain** page.

To edit a Monitoring Domain, select the Monitoring Domain and click **Actions**. From the drop-down list, select **Edit**, the **VMware configuration** page appears.

You can perform the following actions:

- **Edit** - You can select one fabric or multiple fabrics of the same Monitoring Domain to edit a fabric. You cannot choose different fabrics of multiple Monitoring Domains at the same time and edit their fabric components.
- **Deploy Fabric** - -You can select a Monitoring Domain to deploy a fabric, you cannot choose multiple Monitoring Domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific Monitoring Domain and GigaVUE-FM orchestration is enabled. You must create a fabric in the monitoring domain, if the option is disabled
- **Upgrade Fabric** - You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the GigaVUE V Series Nodes using this option.
- **Delete Monitoring Domain** - You can select a Monitoring Domain or multiple Monitoring Domains to delete them.
- **Edit SSL Configuration** - You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
- **Generate Sysdump** - You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting.For more information, refer to Debuggability and Troubleshooting.
- Manage Certificates - You can use this button to perform the following actions:
  - **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments.
  - **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.

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

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

What to do next:

- **Use FM to Launch Fabric** is enabled: You are navigated to the **VMware NSX-T Fabric Deployment** page. Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information on how to deploy GigaVUE V Series Node using GigaVUE-FM.
- **Use FM to Launch Fabric** is disabled: You must deploy GigaVUE V Series Nodes using VMware NSX-T Manager. Refer to Deploy GigaVUE V Series Nodes using VMware NSX-T Manager for more detailed information on how to deploy GigaVUE V Series Nodes using VMware NSX-T Manager.

Configure GigaVUE V Series Nodes for VMware NSX-T

This section provides step-by-step information on how to deploy GigaVUE V Series Nodes.

GigaVUE V Series Nodes can be deployed in GigaVUE-FM using two ways. You can either directly use VMware NSX-T manager to deploy your GigaVUE V Series Nodes or use GigaVUE-FM to deploy your GigaVUE V Series Nodes.

Points to Note:

- When VMware NSX-T is configured in a cluster on multiple hosts, ensure all the hosts are in a connected state. Even if one of the hosts is in a disconnected state then GigaVUE V Series Node host-based deployment will be unsuccessful.
- If a GigaVUE V Series Node is restarted, then the existing flows that is received by that GigaVUE V Series Node will not be forwarded to the other available GigaVUE V Series Nodes (if any). However, the new flows will be forwarded to any available GigaVUE V Series Node.

Refer to the following section for more detailed information:

- Deploy GigaVUE V Series Nodes using GigaVUE-FM
- Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

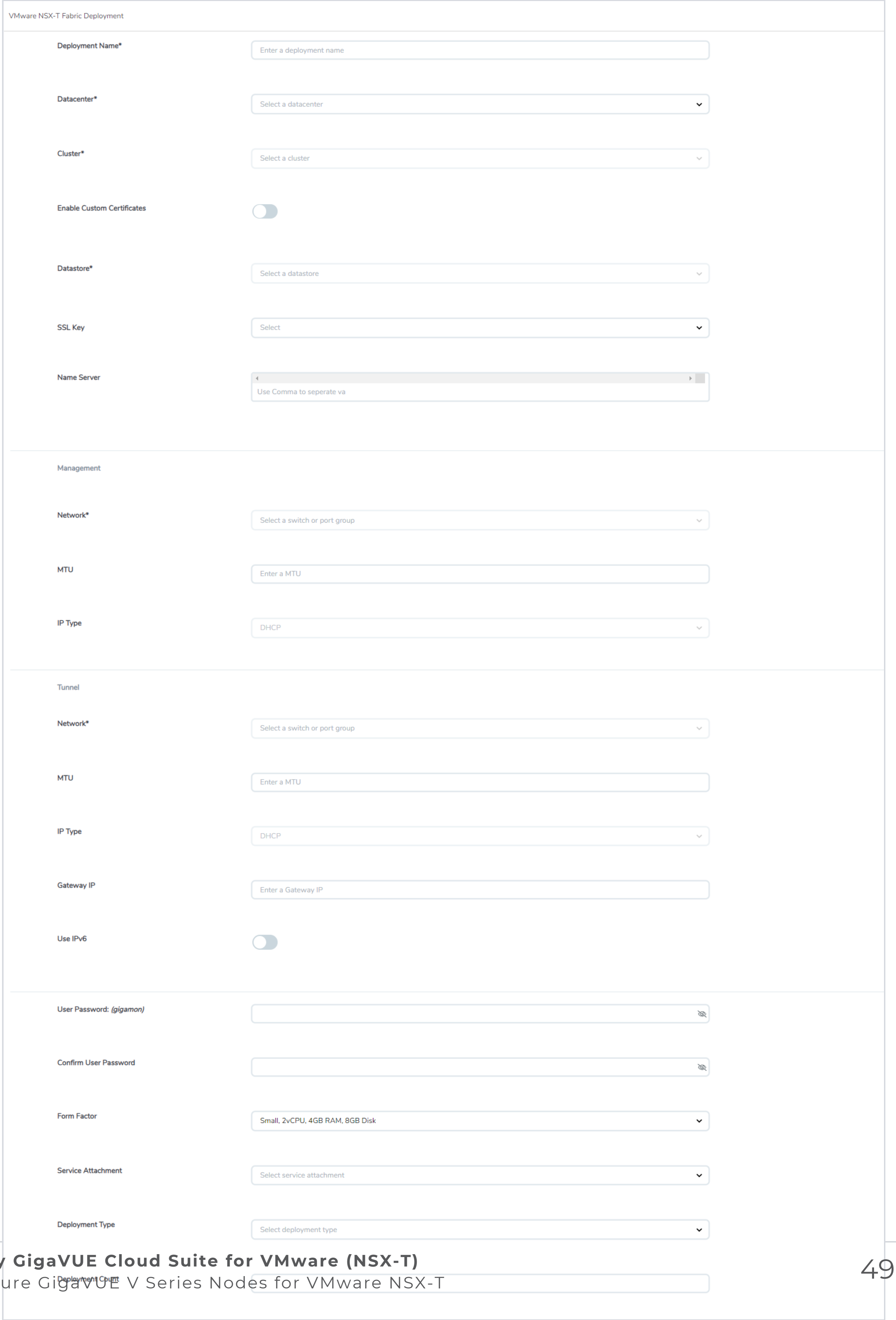
Deploy GigaVUE V Series Nodes using GigaVUE-FM

After creating a monitoring domain in GigaVUE-FM for VMware NSX-T, which establishes a connection between VMware NSX-T manager and GigaVUE-FM, GigaVUE-FM launches the **VMware NSX-T Fabric Deployment** page. Refer to Create Monitoring Domain for VMware NSX-T section for more detailed information on how to create a monitoring domain in GigaVUE-FM for VMware NSX-T.

Deploy GigaVUE V Series Node from GigaVUE-FM

1. After creating a monitoring domain, you are navigated to the **VMware Fabric Launch Configuration** page.

2. You can also 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 NSX-T (V Series)**. Click **Actions > Deploy Fabric**. The **VMware Fabric Launch Configuration** page appears.



VMware NSX-T Fabric Deployment

Deployment Name*	Enter a deployment name
Datacenter*	Select a datacenter
Cluster*	Select a cluster
Enable Custom Certificates	○
Datastore*	Select a datastore
SSL Key	Select
Name Server	Use Comma to seperate va

Management

Network*	Select a switch or port group
MTU	Enter a MTU
IP Type	DHCP

Tunnel

Network*	Select a switch or port group
MTU	Enter a MTU
IP Type	DHCP
Gateway IP	Enter a Gateway IP
Use IPv6	○

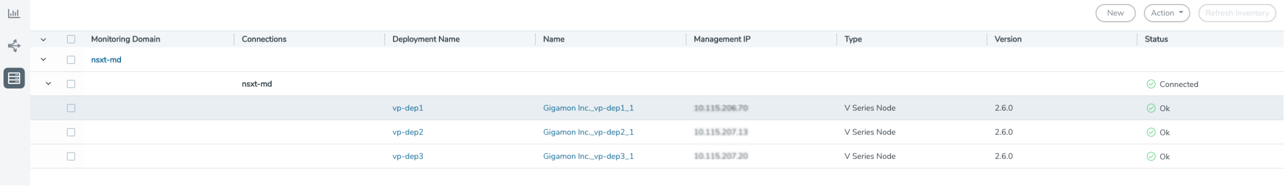
User Password: *(gigamon)*	
Confirm User Password	
Form Factor	Small, 2vCPU, 4GB RAM, 8GB Disk
Service Attachment	Select service attachment
Deployment Type	Select deployment type
Deployment Count	

3. Select or enter the following details in the VMware Fabric Launch Configuration page:

Field	Description
Deployment Name	Name of the deployment (NSX-T service deployment)
Datacenter	vCenter Data Center with the NSX-T hosts to be provisioned with V Series nodes
Cluster	Cluster where you want to deploy GigaVUE V Series Nodes
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and a handshake error occurs. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state.
Custom SSL Certificate **NOTE:** This field appears only when **Enable Custom Certificates** is enabled.	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes. For more detailed information.
Datastore	Network datastore shared among all NSX-T hosts in a cluster.
SSL Key	Reserved for future use.
Name Server	The 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 the valid IPv4 address, separated by comma.
Management	
Network	Management network for GigaVUE V Series Nodes
IP Type	Select the management network IP type as Static or DHCP
IP Pool **NOTE:** This field appears only when the Management **IP type** is Static.	Select the IP Pool
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.
Tunnel	
Network	Tunnel Network for the 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
IP Pool	Select the IP Pool

Field	Description
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.
Use IPv6	Enable to use IPv6.
User Password: (gigamon)	SSH Password for the built-in user, '**gigamon**' on the V Series node
Confirm Password	Confirm the SSH Password of the GigaVUE V Series Node
Form Factor	Instance size of the GigaVUE V Series Node. (eg: Small, Medium or Large)
Service Attachment	Service segment created in VMware NSX-T Manager. Refer to Create a Service Segment in VMware NSX-T for more detailed instructions on how to create service segment in VMware NSX-T.
Deployment Type	Type of GigaVUE V Series Node deployment. It can be either Clustered or Host-Based deployment type. **NOTE:** Select the deployment type as Clustered if you wish to increase or decrease the number of nodes in a cluster using GigaVUE-FM. Refer Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information.
Deployment Count (for Clustered deployment type)	Number of GigaVUE V Series Nodes (Service Instances) to deploy

4. Click **Deploy**. After the GigaVUE V Series Node is deployed in vCenter, it appears on the Monitoring Domain page under the deployment name of the selected Monitoring Domain. You can select a specific service deployment by clicking on the deployment name on the Monitoring Domain page.



Monitoring Domain	Connections	Deployment Name	Name	Management IP	Type	Version	Status
nsxt-md							
	nsxt-md						Connected
		vp-dep1	Gigamon Inc._vp-dep1_1	[redacted]	V Series Node	2.6.0	Ok
		vp-dep2	Gigamon Inc._vp-dep2_1	[redacted]	V Series Node	2.6.0	Ok
		vp-dep3	Gigamon Inc._vp-dep3_1	[redacted]	V Series Node	2.6.0	Ok

To view the fabric launch configuration specification of a fabric component, click on a GigaVUE V Series Node, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

Points to Note:

- The deployed GigaVUE V Series Node name is created automatically by VMware NSX-T. Do not change the name of the GigaVUE V Series Node in the vCenter.
- When rebooting a GigaVUE V Series Node, the existing traffic flows redirected to the GigaVUE V Series Node will stop being redirected to the GigaVUE V Series Nodes. However, new flows initiated after the reboot will be redirected to the GigaVUE V Series Nodes.
- When using cluster-based deployment, after deploying the GigaVUE V Series Node, migrating it to a different host and datastore does not update the datastore details in GigaVUE-FM. Therefore, Storage vMotion of the GigaVUE V Series Node must be avoided. Instead, the GigaVUE V Series Node should be deleted and redeployed.

Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

You can deploy your GigaVUE V Series Nodes using VMware NSX-T Manager. The GigaVUE V Series Nodes register themselves with GigaVUE-FM using the information provided by the user in the NSX-T Manager. Once the nodes are registered with GigaVUE-FM, you can configure Monitoring Session and related services in GigaVUE-FM.

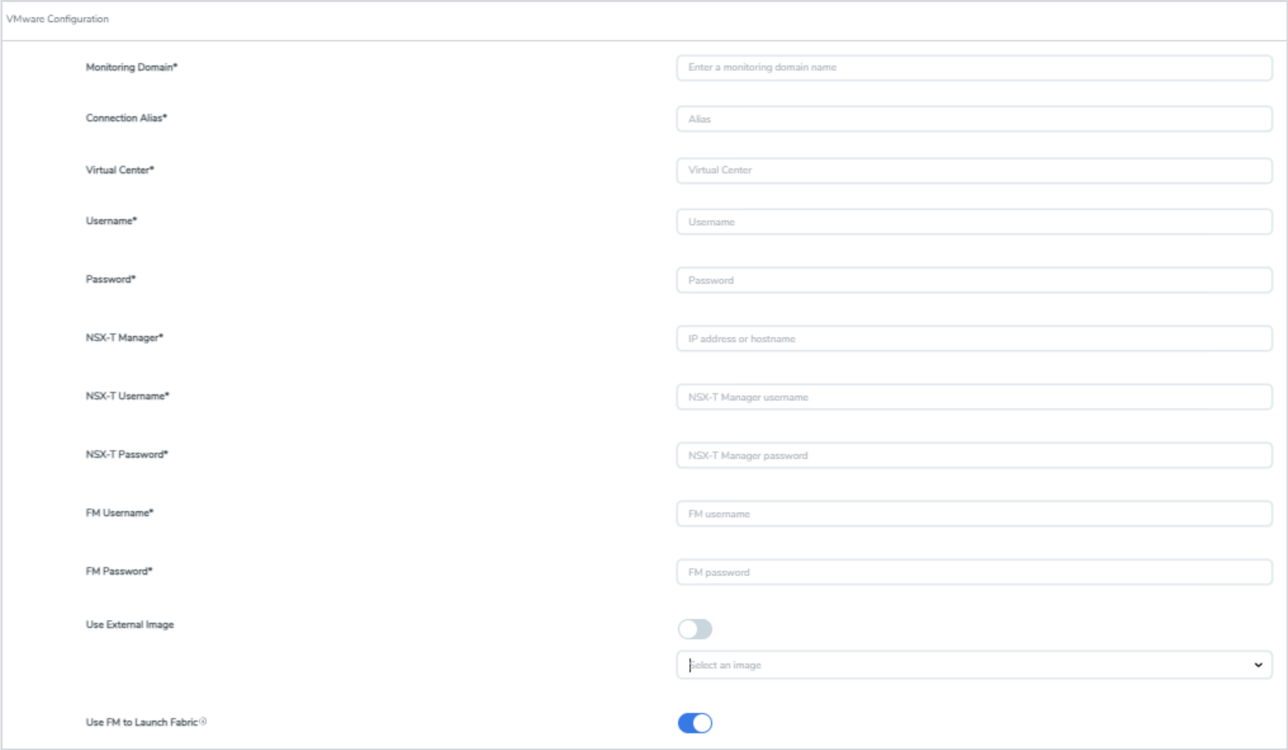
Refer to the following sections for details:

- Getting Started
- Deploying GigaVUE V Series Nodes in VMware NSX-T Manager
- Delete GigaVUE V Series Nodes and Monitoring Domain

Getting Started

To register your GigaVUE V Series Nodes using VMware NSX-T Manager, follow the steps given below:

1. Create a Monitoring Domain in GigaVUE-FM. Refer to Create Monitoring Domain for VMware NSX-T for detailed instructions.
2. In the **VMware Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you wish to deploy GigaVUE V Series Nodes using VMware NSX-T Manager.



VMware Configuration

Monitoring Domain*	Enter a monitoring domain name
Connection Alias*	Alias
Virtual Center*	Virtual Center
Username*	Username
Password*	Password
NSX-T Manager*	IP address or hostname
NSX-T Username*	NSX-T Manager username
NSX-T Password*	NSX-T Manager password
FM Username*	FM username
FM Password*	FM password
Use External Image	○ Select an image
Use FM to Launch Fabric	●

> **NOTE:** When creating the Monitoring Domain for deploying GigaVUE V Series Nodes, you can use the VMware NSX-T username and password that has at least "NETX Partner Admin" role assigned to it.

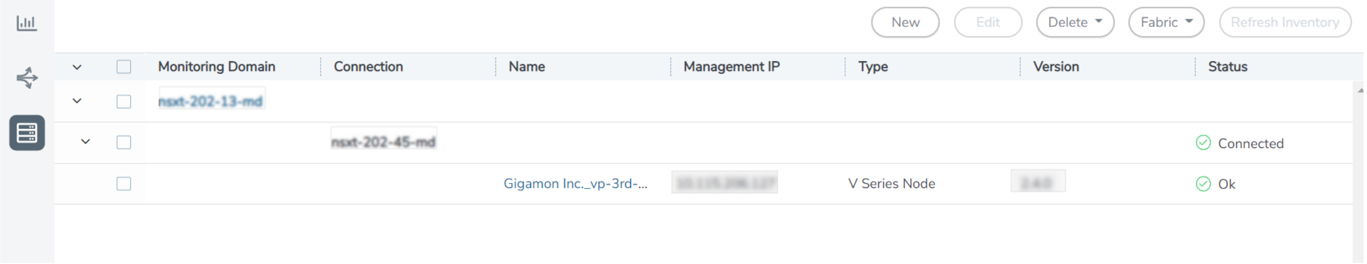
After creating your monitoring domain, you can use VMware NSX-T manager to deploy your GigaVUE V Series Nodes. When creating multiple Monitoring Domain with the same NSX-T Manager, a unique service name is associated with it. You can view the service name of each Monitoring Domain in the **Monitoring Domain** page.

Deploying GigaVUE V Series Nodes in VMware NSX-T Manager

1. In the Service Deployment page of the VMware NSX-T manager, select **Deployment**. Then, select the service name of the Monitoring Domain from the **Partner Service** drop-down in which you wish to deploy the GigaVUE V Series Nodes. For detailed information, refer to Deploy a Partner Service topic in VMware Documentation.
2. After selecting the **Deployment template** and **Deployment Specification**, click **Configure Attributes**. The **Configure Attributes** page appears.

3. In the **Configure Attributes** page, enter the Service VM Host Name and Admin user password details. If you wish to use custom certificate for GigaVUE V Series Node, then enter the **SSL Private Key** and the **SSL Certificate**. For more details on Custom Certificate refer to Secure Communication topic for more detailed information on Custom Certificates.
4. Once the GigaVUE V Series Node is successfully deployed, the deployed node is registered with GigaVUE-FM after the run time status of the node is displayed as **UP** in VMware NSX-T manager.

The GigaVUE V Series Node deployed in your VMware NSX-T manager appears on the Monitoring Domain page of GigaVUE-FM. In GigaVUE-FM the **Status** of the node is displayed as **Launching** and once the node is successfully registered the **Status** is changed to **Ok.**



	Monitoring Domain	Connection	Name	Management IP	Type	Version	Status
□	nsxt-202-13-md						
□		nsxt-202-45-md					Connected
□			Gigamon Inc._vp-3rd-...	[redacted]	V Series Node	[redacted]	Ok

- IPv6 address is not supported for gateway of the tunnel interface when nodes are deployed through the VMware NSX-T manager.
- When you deploy nodes using VMware NSX-T manager, ensure all your GigaVUE V Series Nodes are of the same version. GigaVUE-FM does not support GigaVUE V Series Nodes with different version in the Monitoring Domain.
- The deployed GigaVUE V Series Node name is created automatically by VMware NSX-T. Do not change the name of the GigaVUE V Series Node in the vCenter.

Delete GigaVUE V Series Nodes and Monitoring Domain

NOTE: When you deploy your V Series Nodes using VMware NSX-T manager, you cannot directly delete your GigaVUE V Series Node in GigaVUE-FM. In this case, the Delete button in GigaVUE-FM is disabled, so the Service Deployment in NSX-T Manager must be deleted first.

To delete a GigaVUE V Series Node deployed using VMware NSX-T Manager, follow the steps given below:

1. Delete the **Policy** and **Service Chain** in the VMware NSX-T manager.
2. Then, delete the Monitoring Session in GigaVUE-FM.
3. Delete the node in VMware NSX-T manager. Then, the node will be unregistered from the Monitoring Domain in GigaVUE-FM.
4. Finally, delete the Monitoring Domain in GigaVUE-FM.

Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM

You can add more nodes or remove nodes from an existing Monitoring Domain using GigaVUE-FM. These steps are applicable only when you deploy GigaVUE V Series Nodes using GigaVUE-FM.

> **NOTE:** Increasing or Decreasing the number of nodes in a cluster is only applicable when using Clustered based deployment.

Refer to the following topics for more detailed information on how to add or remove GigaVUE V Series Node deployed using GigaVUE-FM for an existing monitoring domain :

- Add GigaVUE V Series Nodes to Existing Monitoring Domain
- Decrease GigaVUE V Series Nodes from Existing Monitoring Domain

Add GigaVUE V Series Nodes to Existing Monitoring Domain

To increase the number of GigaVUE V Series Node in an existing Monitoring Domain follow the steps given below:

1. On the Monitoring domain page, select the monitoring domain to which you wish to add more GigaVUE V Series Nodes.
2. Click on the **Actions** button and select **Deploy Fabric**.
3. The **VMware Fabric Deployment** page opens. Enter the details as mentioned in Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM

   > - The Deployment type must be Clustered to have multiple deployment on the same cluster.
   > - A cluster can have only one Host Based Deployment, however there can be multiple clustered deployment on the same cluster.

4. Enter the number of GigaVUE V Series Nodes you wish to add in the **Deployment Count** column.
5. Click Deploy.

   The newly added GigaVUE V Series Nodes will be displayed under the existing monitoring domain with the new Deployment Name.

Decrease GigaVUE V Series Nodes from Existing Monitoring Domain

To decrease the number of nodes in an existing Monitoring Domain follow the steps given below:

1. On the Monitoring domain page, select the **Deployment** from which you wish to remove the GigaVUE V Series Nodes or select the entire Monitoring Domain to remove all the deployments from the Monitoring Domain.

   > **NOTE:** You can select the Deployment either by using the check-box on the left side or by clicking on the deployment name.

2. Click on the **Actions** button and select **Delete Deployment**.
3. All the GigaVUE V Series Nodes under that deployment will be deleted.

   The number of GigaVUE V Series Nodes in the Monitoring Domain will be decreased by the number of nodes in the deployment that were deleted.

Example use-case for Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM

This feature can be used in a scenario where you are migrating from GigaVUE-VM visibility solution to GigaVUE V Series visibility solution, you can simply add the GigaVUE V Series Node to the existing Monitoring Domain instead of undeploying and redeploying the Monitoring Domain every time you wish to add more GigaVUE V Series Nodes to the Monitoring Domain.

Increase or Decrease GigaVUE V Series Nodes using VMware NSX-T Manager

You can now add more nodes or remove nodes from an existing monitoring domain using VMware NSX-T Manager. These steps are applicable only when you deploy GigaVUE V Series Nodes using VMware NSX-T Manager.

Refer to the following topics for more detailed information on how to add or remove GigaVUE V Series Node deployed using NSX-T manager for an existing monitoring domain :

- Add V Series Nodes to Existing Monitoring Domain
- Decrease V Series Nodes from Existing Monitoring Domain

Add V Series Nodes to Existing Monitoring Domain

To increase the number of V Series Node in an existing monitoring domain using VMware NSX-T Manager follow the steps given below:

1. On the Service Deployment page of the VMware NSX-T manager, select **Deployment**. This page lists the service deployments that are already deployed.
2. Then, click **Deploy Service** button. For more details on how to deploy a service refer Deploy a Partner Service.
3. Enter the same details as given for the service mapped to the existing monitoring domain in GigaVUE-FM to which you wish to add more nodes.

4. In the **Clustered Deployment Count**, enter the number of nodes you wish to add to the existing monitoring domain.
5. Click **Save**.

Once the Service deployment is successful and the nodes are deployed, you can view the nodes on the monitoring domain page of GigaVUE-FM.

Example - Consider a scenario where the monitoring domain in GigaVUE-FM has two V Series Nodes. To increase the number of nodes in this monitoring domain, go to VMware NSX-T Manager and create a new service using the steps mentioned above. Then, the number of V Series Nodes in the monitoring domain in GigaVUE-FM goes up by the number you have mentioned in **Clustered Deployment Count** column in the VMware NSX-T.

Decrease V Series Nodes from Existing Monitoring Domain

To decrease the number of nodes in an existing monitoring domain using VMware NSX-T follow the steps given below:

1. On the **Service Deployment** page of the VMware NSX-T manager, select **Deployment**.
2. The service deployment page lists the service deployments that are already deployed. .
3. Select the service deployment that you want to delete. The GigaVUE V Series Nodes that are part of that service deployment will be deleted from the host. These GigaVUE V Series Nodes will also be removed from the monitoring domain in the GigaVUE-FM. This way the number of service VMs (V Series nodes) can be decreased in a monitoring domain

Example - Consider a scenario where the monitoring domain in GigaVUE-FM has five V Series Nodes. To reduce the number of nodes in this monitoring domain, go to VMware NSX-T Manager and delete a service deployment using the steps mentioned above. Then, the number of V Series Nodes in the monitoring domain in GigaVUE-FM goes down by the number you have mentioned in **Clustered Deployment Count** column of the service you have deleted.

Upgrade GigaVUE V Series Node for VMware NSX-T

GigaVUE V Series Nodes can be deployed in two ways. You can either directly use VMware NSX-T manager to deploy your GigaVUE V Series Nodes or use GigaVUE-FM to deploy your GigaVUE V Series Nodes. Based on the method you deploy GigaVUE V Series Nodes, you can upgrade them in two ways. Refer to the following topic for more detailed information.

Version Compatibility

GigaVUE-FM version 6.11 supports the latest version (6.11) of GigaVUE V Series Node as well as (n-2) versions. For better compatibility, it is always recommended to use the latest version of GigaVUE V Series Node with GigaVUE-FM.

Refer to the following sections:

- Prerequisite
- Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM
- Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager

Prerequisite

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

Obtaining Software Images

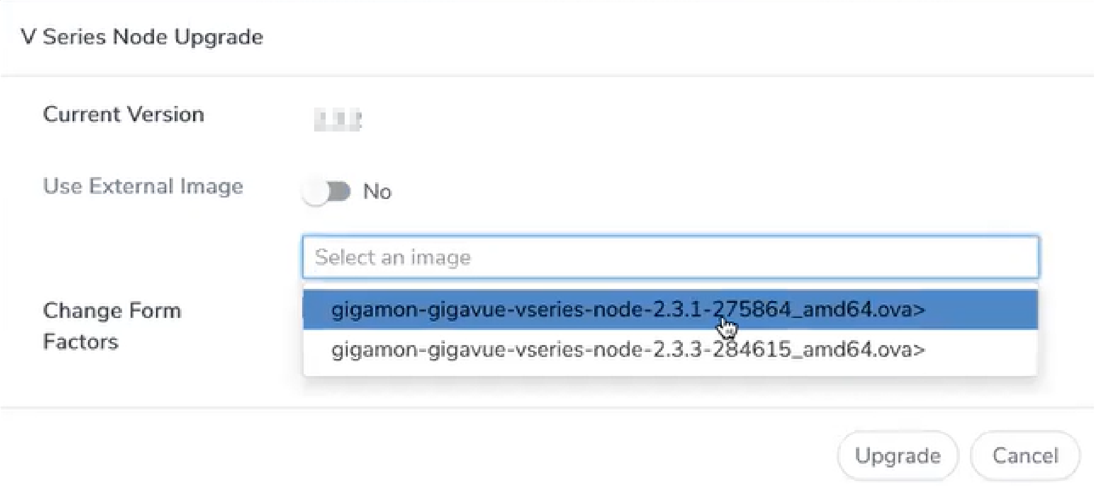
To obtain software images:

1. Login to the **Gigamon Community** portal.
2. Search for V Series OVA images.
3. Download the file to the local servers and place it in Internal server / External server.

Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM

Before upgrading the nodes ensure that all the current V Series nodes are of same version. To upgrade GigaVUE V Series Node in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select a deployed monitoring domain and click **Actions**. From the drop-down list, select **Upgrade Fabric**, the **V Series Node Upgrade** dialog box appears.


V Series Node Upgrade
Current Version
Select an image
Change Form Factors
gigamon-gigavue-vseries-node-2.3.1-275864_amd64.ova>
gigamon-gigavue-vseries-node-2.3.3-284615_amd64.ova>
Upgrade
Cancel

Use External Image No

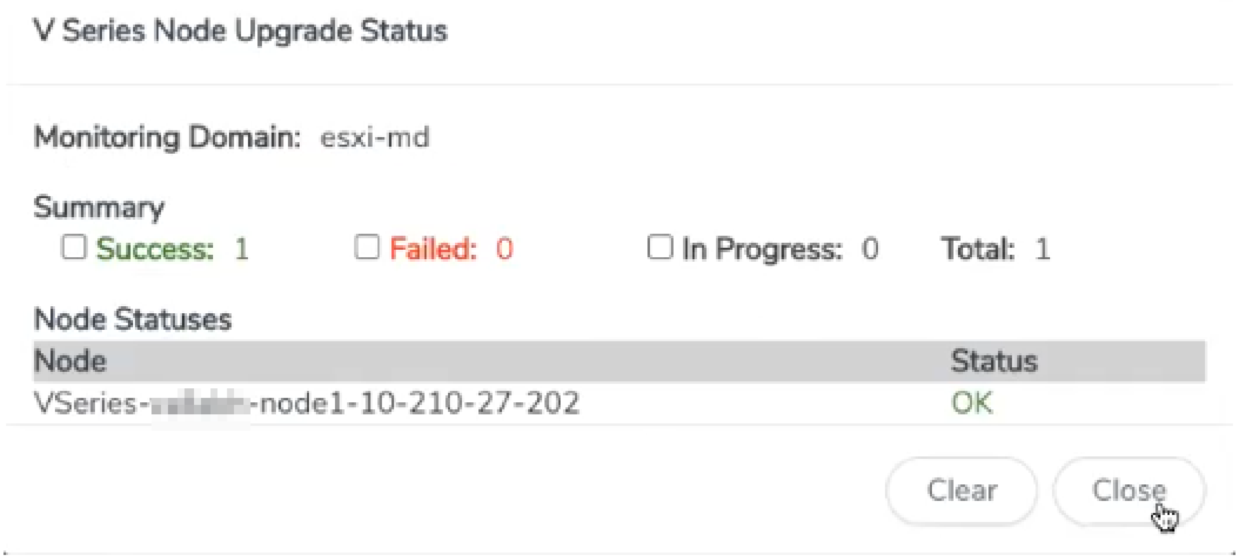
3. Use the **Use External Image** toggle button to choose between internal and external image.
   - **Yes** to use an external image. Enter the Image URL of the latest V Series Node OVA image. Ensure all the contents of the OVA file are extracted into VMDK and OVF files and placed in the directory that represents the Image URL.
   - **No** to use an internal image. To use an internal image, select the uploaded OVA files from the **Select an image** drop-down menu.
4. Click the **Change Form Factors** check box to modify the form factor (instance) size.

   > **NOTE:** Both the new and the current V Series nodes appears on the same monitoring domain until the new nodes replaces the current and the status changes to **Ok**.

5. Click **Upgrade**.

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

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



V Series Node Upgrade Status

Monitoring Domain: esxi-md

Summary

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

Node Statuses

Node	Status
VSeries-[redacted]-node1-10-210-27-202	OK

Click **Clear** to delete the logs of successfully upgraded nodes.

NOTE: Monitoring Domain upgrade can be only done when there is a single service deployment in the monitoring domain.

Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager

To upgrade V Series Nodes deployed using VMware NSX-T, follow the steps given below:

1. Delete the existing V Series Node in VMware NSX-T Manager.
2. Click **Actions > Edit** in the Monitoring Domain page. The **VMware Configuration** page appears.
3. Enter the new **Image URL** or select a new image if **Use External Image** toggle button is disabled.
4. Then, deploy the new V Series Nodes in the VMware NSX-T manager

Notes:

- When you deploy your V Series Nodes using VMware NSX-T manager, you cannot directly upgrade V Series Node in GigaVUE-FM. In this case, the upgrade button in GigaVUE-FM is disabled.

- If a V Series Node upgrade on the VMware NSX-T platform fails initially but later succeeds, GigaVUE-FM does not receive the updated status and continues to show the upgrade as failed. Since VMware NSX-T does not trigger an event to automatically retry the upgrade, the failed V Series deployment must be manually deleted from GigaVUE-FM and redeployed to reflect the correct status.

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 that 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 and based on the selection criteria, the detected target VMs are added into your monitoring session. Similarly, when a traffic monitoring target VM is removed, it updates the monitoring sessions to show the removed instance. Before deploying a monitoring session, you need to deploy a V Series node in each host where you want to monitor the traffic.

NOTE:
- Link transformation and multiple links between two entities are not supported in V Series nodes of ESXi.
- 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 NSX-T)
- Interface Mapping
- Create Ingress and Egress Tunnel (VMware NSX-T)
- Create a New Map (VMware NSX-T)
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics

Create a Monitoring Session (VMware NSX-T)

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.

> **Points to Note:**
>
> - In a Monitoring Session, if a selected VM is connected to VSS and VDS, then the GigaVUE-FM can create tapping for both VSS and VDS network.
> - When you undeploy or edit a Monitoring Session and redeploy it, the existing traffic flows redirected to the GigaVUE V Series Node will stop being redirected to the GigaVUE V Series Nodes. However, new flows initiated after the redeployment will be redirected to the GigaVUE V Series Nodes.

Monitoring Session Page

You can view the following tabs on the Monitoring Session page:

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

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

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 NSX-T)

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

> **NOTE:** GigaVUE-FMlets 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.

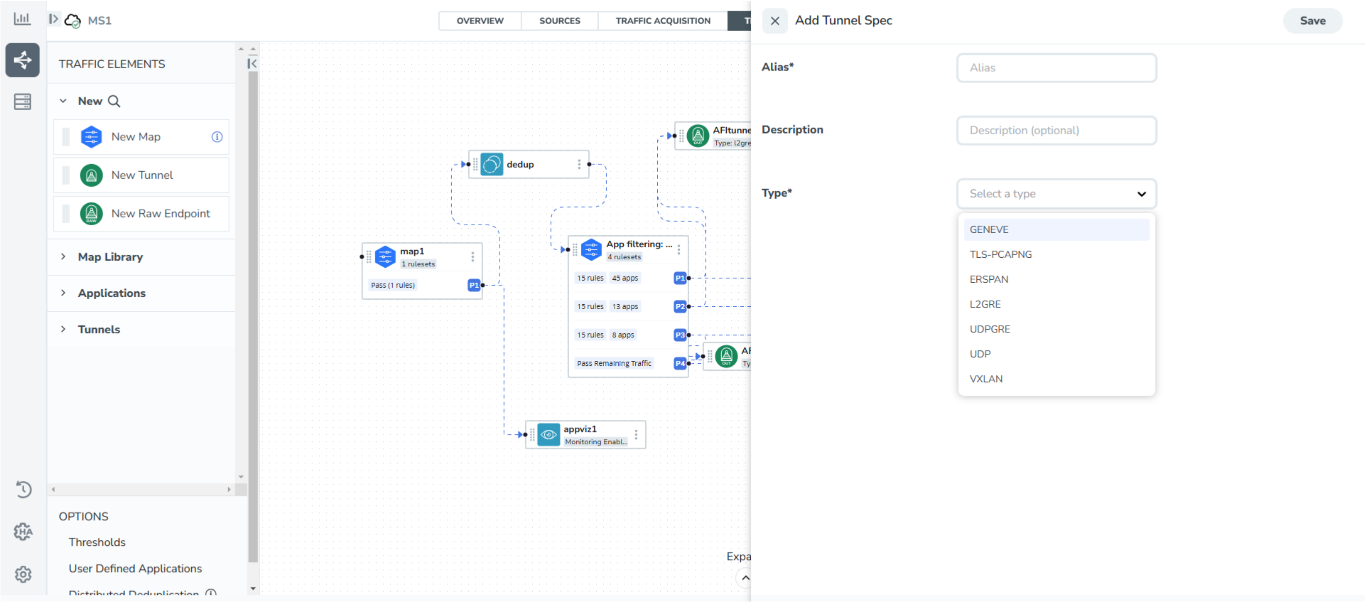
3. 2. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.

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

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

   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 **NOTE:** This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable or down tools. Each egress tunnel configured on the GigaVUE V 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. **NOTE:** This option is not supported for TLS-PCAPNG tunnels.
Type	The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.
VXLAN	
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **NOTE:** In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to configure secure tunnels on your physical device conveniently. For	

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-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session.
	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 UPDGRE/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.

Tunnel End Points created will be listed in the **Tunnel Specifications** page. You can create, edit, and delete tunnel end point from this page. Refer to Create Tunnel Specifications for more detailed information on how to create tunnel end points.

Create Raw Endpoint (VMware NSX-T)

This section provides step-by-step instructions on configuring a RAW Endpoint (REP) in the Monitoring Session.

Refer to the below sections for more detailed information:

- Rules and Notes
- Create Raw Endpoint (VMware NSX-T)
- Configure Raw Endpoint in Monitoring Session
- Configuration Support for Non IP-Addressable (l2 supported) Tools

Rules and Notes

- When using VMware NSX-T, Monitoring session supports only egress RAW Endpoint.
- REP is not supported on NSX Segments, you can use Virtual Standard Switch (VSS) port group to configure REPs.
- GigaVUE-FM expects the IP address to be configured on the GigaVUE V Series Node interface which will be used for creating RAW Endpoint (REP).

Points to Note:

Refer to the following table for more detailed information on the number of interfaces, their roles for the GigaVUE V Series Nodes deployed in the Monitoring Domain.

Display Name	Interface Name	Role	Comments
Network Adapter 1	ens160	Management	-
Network Adapter 2	ens192	Tunnel	Supports Tunnel and Egress RAW endpoint.
Network Adapter 3	ens224	Data	Reserved and used by NSX-T for Service Insertion (Traffic Acquisition)

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 add Raw Endpoint to the Monitoring Session:

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

Configuration Support for Non IP-Addressable (l2 supported) Tools

Follow the steps given below to deliver RAW traffic to tools or sensors that do not have IP address support:

1. Create a Virtual Standard Switch (VSS) with the details given below. No uplink is required (and hence no physical NIC is required).
2. Create two port groups on the vSwitch created in the previous step:
   a. Create a port group (For example, EgressPortgroup for GigaVUE V Series Node to egress RAW packets)
   b. Create a port group (IngressPortgroup) with promiscuous mode enabled for mirroring the packets.

   > **NOTE:** Refer to Port Group Configuration for Virtual Machines section in the VMware Documentation for more detailed information on how to create a VSS and how to configure the port groups.

3. Connect the tool or sensor interface to IngressPortgroup.

   > **NOTE:**
   > - The sensor or tool should be deployed on the same host where the GigaVUE V Series Node is deployed.
   > - The GigaVUE V Series Node should be deployed using Host Based Deployment. Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information on how to deploy GigaVUE V Series Node using Host Based deployment type.

4. Deploy GigaVUE V Series Node on the ESXi host where the tool or sensor is deployed.
5. Select EgressPortgroup for the GigaVUE V Series Node Tunnel Interface (Network Adapter 2 or ens192) while deploying the GigaVUE V Series Node.
6. Deploy Monitoring Session with RAW Endpoint for egress and then select ens192 as the interface during interface mapping step as in the Configure Raw Endpoint in Monitoring Session.

> **NOTE:** Promiscuous mode Port Group will mirror the entire switch traffic

Create a New Map (VMware NSX-T)

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

Keep in mind the following when creating a map:

Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.

Priority	Priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
Pass	The traffic from the virtual machine will be passed to the destination.
Drop	The traffic from the virtual machine is dropped when passing through the map.
Traffic Filter Maps	A set of maps that are used to match traffic and perform various actions on the matched traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination - Not applicable to Nutanix. • VM Tag Source - Not applicable to Nutanix. • VM Category Source - Applicable only to Nutanix. • VM Category Destination - Applicable only to Nutanix. • Host Name -Applicable only to Nutanix and VMware. The traffic direction is as follows: • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **Notes:** • 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.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

Rules and Notes:

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

- If 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 will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide* for detailed information.

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, click on **General** tab and enter the required information as described below.
   a. Enter the **Name** and **Description** of the new map.
   b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence. Enabling this option allows you to filter traffic based on Application name or family. Refer to Application Filtering Intelligence.

   > **NOTE:** Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
   > - Traffic Map—Only Pass rules for ATS
   > - Inclusion Map—Only Pass rules for ATS
   > - Exclusion Map—Only Drop rules for ATS

3. Click on **Rule Sets** tab.
   a. **To 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. **To create a new rule:**
      i. Click **Actions > New Rule**.
      ii. Select a required condition from the drop-down list. Click ... and select **Add Condition** to add more conditions.
      iii. Select the rule to **Pass** or **Drop** through the map.
4. Click **Save**.

Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to Example- Create a New Map using Inclusion and Exclusion Maps for more detailed information on how to configure Inclusion and Exclusion maps using ATS.

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

- To edit a map, click the ⋮ menu button of the required map on the canvas and click **Details**, or click **Delete** to delete the map.
- To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Thresholds tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Click 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. Click on the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
   a. In the **GENERAL** tab, enter the name as Inclusionmap1 and enter the description. In the **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 more detailed information on how to configure these application, 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 Monitoring Session **OVERVIEW** page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

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

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

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

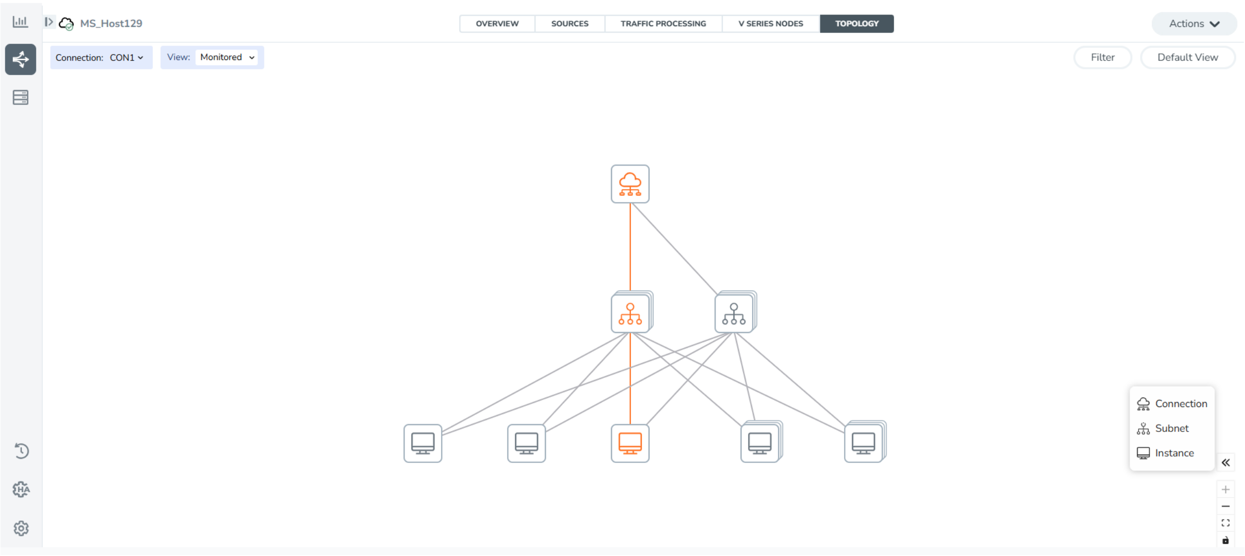
> Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of packets from the V Series node can be more than expected.

Visualize the Network Topology (VMware NSX-T)

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
   - 

     Connection: CON1

     View: Monitored
6.

7. (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.
8. 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.

Create Service Chain and NSX-T Group

A VMware NSX-T group and service chain must be created to redirect network traffic to the GigaVUE Cloud Suite. A VMware NSX-T group defines which VMs are to be monitored. The service chain associates the GigaVUE Cloud Suite and maps the profile to the group.

Create Service Chain

The steps presented in this section create a service chain with the source virtual machines defined as the virtual machines in the applied groups. Additional configurations of the service chain are available. For additional details on creating security policies, refer to the "Service Composer" chapter of the *NSX Administration Guide* in the VMware documentation.

To create the service chain in VMware NSX-T:

1. Select **Security > Settings >Network Introspection** and then click **SERVICE CHAINS** tab.
2. On the SERVICE CHAINS tab, click **ADD CHAIN**.

3. On the New Service Chain, do the following:
   a. In the **Name** and **Description** fields, enter a name and description for the service chain, respectively.
   b. For **Service Segments**, select a service segment.
   c. Click **Forward Path** and a **Set Forward Path** dialog box appears.
      - Select a Service Profile for Forward Path.
   d. For the **Reverse Path**, select or deselect the **Inverse Forward Path** to define the direction of the traffic.
   e. For **Failure Policy**, specify whether to allow or block the service chain.
4. Click **Save**. A Service Chain is created.

Create Group

A group should be created that contains the VMs to forward NSX-T network traffic to the GigaVUE Cloud Suite.

To create the group, do the following in the NSX-T:

1. In the VMware NSX manager, select **Inventory > Groups**. The Groups page appears.
2. On the Groups page, click **ADD GROUP**.
3. On the New Group, enter or select the values as follows.
   a. Enter a name for the new group.
   b. Click **Set Members** and the **Select Members** dialog box appears.
4. Click **Save** and then a group is created and appears on the **Groups** page.
   - Add or select Membership Criteria, Members, IP/MAC Addresses, and AD Groups.
   a. Enter the description for the group.

Create and Publish a Policy

A Policy is a set of rules defined to filter the traffic. A Policy is to be created and published for passing the traffic from NSX-T to the configured tunnel endpoint.

To create and publish a policy in NSX-T:

1. In the VMware NSX manager, select **Security > Service Chain Management > Network Introspection (E-W)**.
2. Click **ADD POLICY**.

3. On the New Policy, enter or select the values as follows:
   a. Enter a name for the policy.
   b. Select the **Sources** of the traffic.
   c. Select the **Destinations** of the traffic.
   d. Select the **Services** for the traffic.
   e. For the **Applied To** field, select the appropriate groups.

   > **Points to Note:**
   >
   > - When using the same NSX-T manager to create multiple Monitoring Domains, if you prefer to associate a single vCenter with each Monitoring Domain, ensure that you select only the members of the vCenter related to that specific Monitoring Domain.
   > - All the workload VMs from the vCenters that are selected in the **Applied To** group will send traffic to the GigaVUE V Series Node. Ensure to select only the workload VMs from the vCenters that are associated with the Monitoring Domain, else the GigaVUE V Series Node will receive traffic from the vCenters that are not associated with the Monitoring Domain.

   f. On the **Action** field, specify whether to redirect the traffic or not.
4. Click **Publish**. On publishing the rule or policy you can view the traffic flow from the GigaVUE V Series Nodes to the tunnel endpoint.

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 things:

1. If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow the steps given below.
    a. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
    b. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the **TRAFFIC ACQUISITION** tab.
    c. Enable Secure tunnels. Refer to the *Configure Monitoring Session Options* topic in the respective GigaVUE Cloud Suite Deployment Guide for information about how to enable secure tunnel for a Monitoring Session.
    d. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The Monitoring Session is undeployed.
    e. Select the Monitoring Session for which you enabled Secure Tunnels and edit the Monitoring Session.
    f. Add the Application Intelligence applications.
    g. 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

    h. Click **Deploy**. Refer to Application Intelligence section in the GigaVUE V Series Applications Guide for more detailed information on how to deploy the Application Intelligence applications.

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

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

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 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
HeaderStripping	1. Tx Packets	1. Difference	1. Over

	2. Rx Packets 3. Packets Dropped	2. Derivative	2. Under
TunnelEncapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
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 > Resouces > 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:

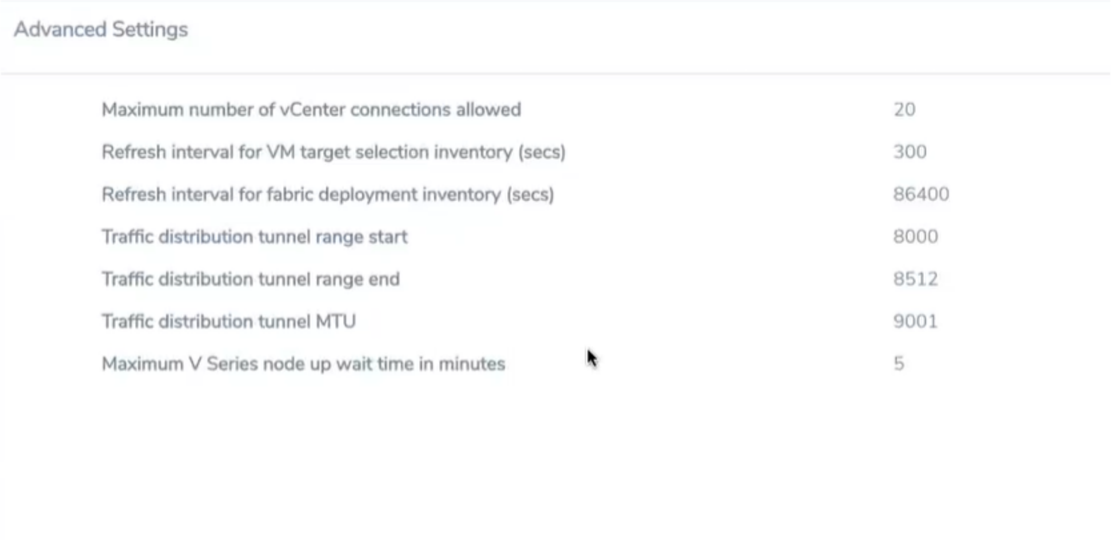
1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. In the **Overview** tab, view the health status of the required GigaVUE V Series Node from the chart options.

Configure VMware Settings

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

To configure the VMware Settings:

Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Settings > Advanced Settings** to edit the VMware V Series NSX-T settings.



Advanced Settings

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
Traffic distribution tunnel MTU	9001
Maximum V Series node up wait time in minutes	5

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

Settings	Description
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.
Traffic distribution tunnel MTU	Specifies the Tunnel MTU value.
Maximum V Series Node up wait time	Specifies the maximum amount of time taken for the GigaVUE Series Node state to go to OK.

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 Analytics [1],. you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards.

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

Rules and Notes:

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

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

Virtual Inventory Statistics and Cloud Applications Dashboard

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

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:

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: • Platform • Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms

Dashboard	Displays	*Visualizations*	Displays
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour. **NOTE:** The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Rx Trend	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the V Series network interface for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.

Dashboard	Displays	*Visualizations*	Displays
		V Series Node Tunnel Rx Packets/Errors	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the de-duplicated packets received against the de-duplication application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated:	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.

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

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

Remove Gigamon Service from NSX-T and GigaVUE-FM

To clean up the Gigamon Deep Observability Pipeline from VMware NSX-T and GigaVUE-FM, perform the following steps:

- Step 1: Remove the Rule and Policy
- Step 2: Remove the Service Chain
- Step 3: Delete the Monitoring Session
- Step 4: Delete the Monitoring Domain

Step 1: Remove the Rule and Policy

To delete the network monitoring services:

1. Select **Security > Service Chain Management > E-W Network Introspection**. The E-W Network Introspection page appears.
2. On the E-W Network Introspection page, expand the policy that was created for Gigamon tapping.
3. To delete the rule associated with the policy, click the ⋮ icon on the Rule Column and then select **Delete**
4. To delete the policy, Click the ⋮ icon on the policy and then select **Delete**.

Step 2: Remove the Service Chain

To delete the network monitoring services:

1. In NSX-T Manager, select **Security > Settings > Network Introspection**.
2. Select the **SERVICE CHAINS** tab.
3. On the service chain where service profile created for Gigamon is attached to it, click ⋮ and then select **Delete** to delete the selected Service Chain.

Step 3: Delete the Monitoring Session

To delete the Monitoring session from GigaVUE-FM:

1. From the left navigation pane, select **Traffic** > **VIRTUAL > Orchestrated Flows** > **VMware**. The Monitoring Sessions pertaining to all VMware deployment appears.
2. Select the NSX-T related Monitoring Session and click **Actions > Undeploy**. The Monitoring Session is Undeployed.
3. Select the Monitoring Session again and click **Actions > Delete**.
4. The service profile and the profile that corresponds to the Monitoring Session is deleted on NSX-T manager console.

Step 4: Delete the Monitoring Domain

To delete the Monitoring Domain and the GigaVUE V Series Node deployed in GigaVUE-FM:

1. From the left navigation pane, select **Inventory** > **VIRTUAL** > **VMware NSX-T** > **Monitoring Domain**. The Monitoring Domain page appears along with the deployed GigaVUE V Series Nodes.
2. Select the appropriate **Monitoring Domain**, click **Actions > Delete Monitoring Domain**.
3. The **Service Deployment** that corresponds to the Monitoring Domain is deleted from the NSX-T Manager.

GigaVUE V Series Deployment Clean up

On installation failure or incomplete service removal, you must clean up GigaVUE V Series Nodes before reattempting the installation. To clean up the V Series deployments from NSX-T and GigaVUE-FM, perform the following steps:

- Delete Rule and Policy in NSX-T Manager
- Remove Service Deployments
- Remove Service Reference
- Remove Service Manager
- Remove Vendor Template and Service Definition

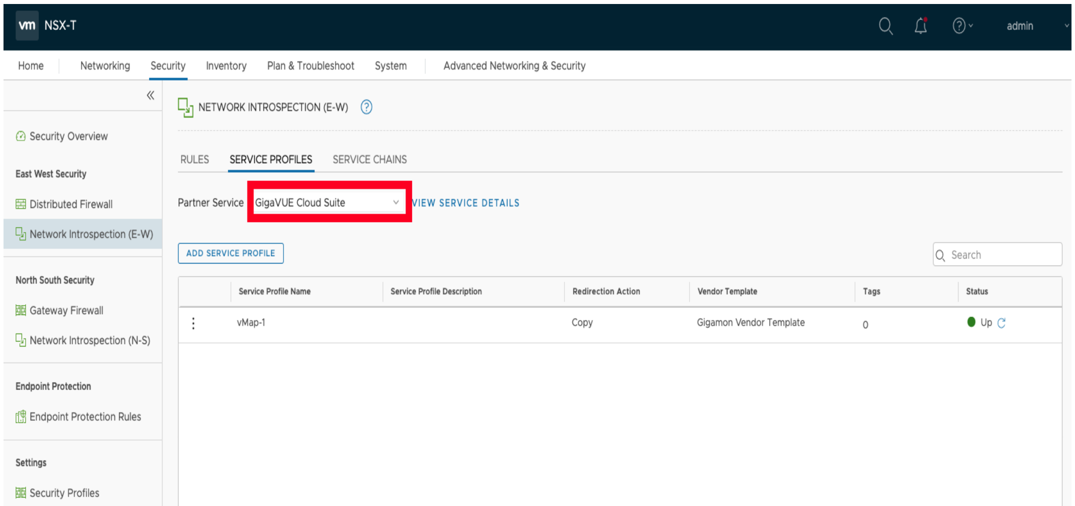
Delete Rule and Policy in NSX-T Manager

Delete Service Chain

Delete Monitoring Session - Service Profile is deleted.

To remove Service Profiles:

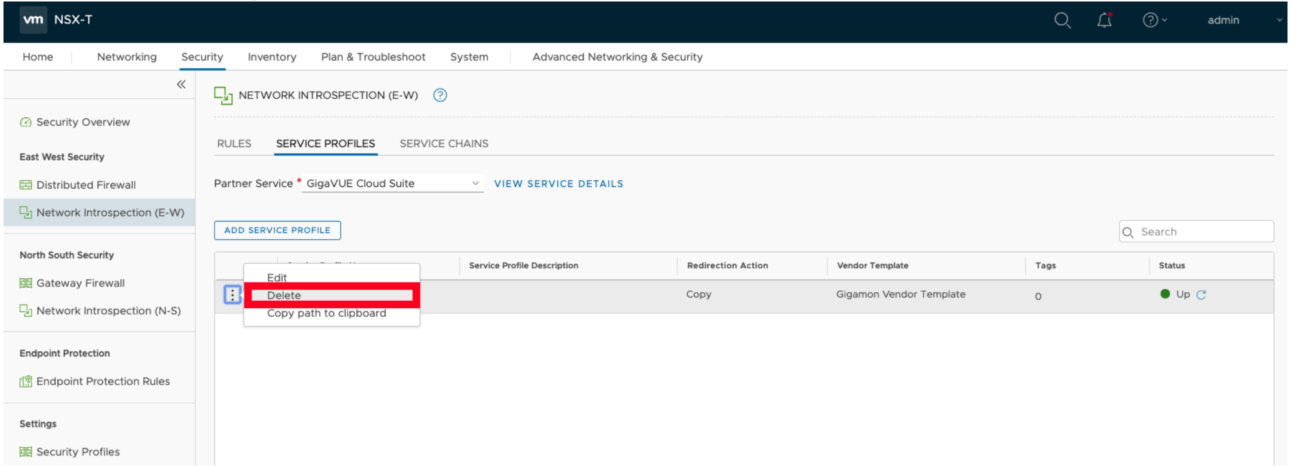
1. From NSX-T Manager, navigate to **Security > Network Introspection (E-W)**.
2. In the **SERVICE PROFILES** tab, select the service name of the Monitoring Domain from the **Partner Service** drop-down.



Partner Service GigaVUE Cloud Suite

	Service Profile Name	Service Profile Description	Redirection Action	Vendor Template	Tags	Status
⋮	vMap-1		Copy	Gigamon Vendor Template	0	● Up

3. Delete all existing Service Profiles.



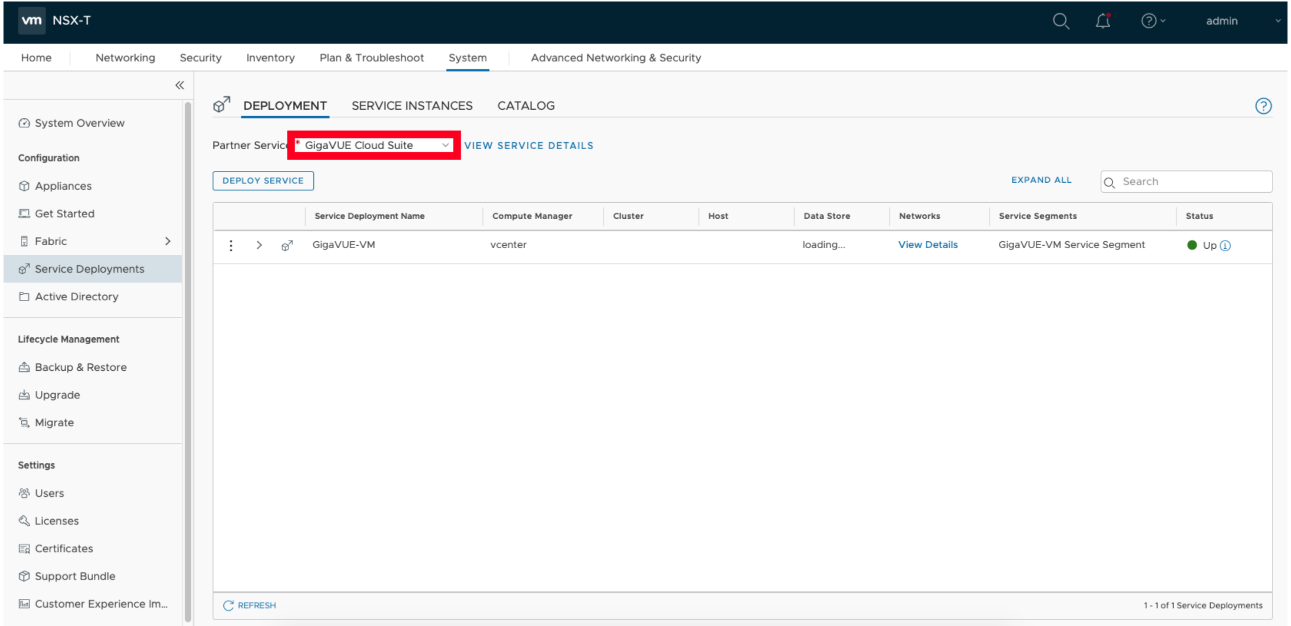
Partner Service * GigaVUE Cloud Suite

	Service Profile Description	Redirection Action	Vendor Template	Tags	Status
⋮		Copy	Gigamon Vendor Template	0	● Up

Remove Service Deployments

To remove Service Deployments:

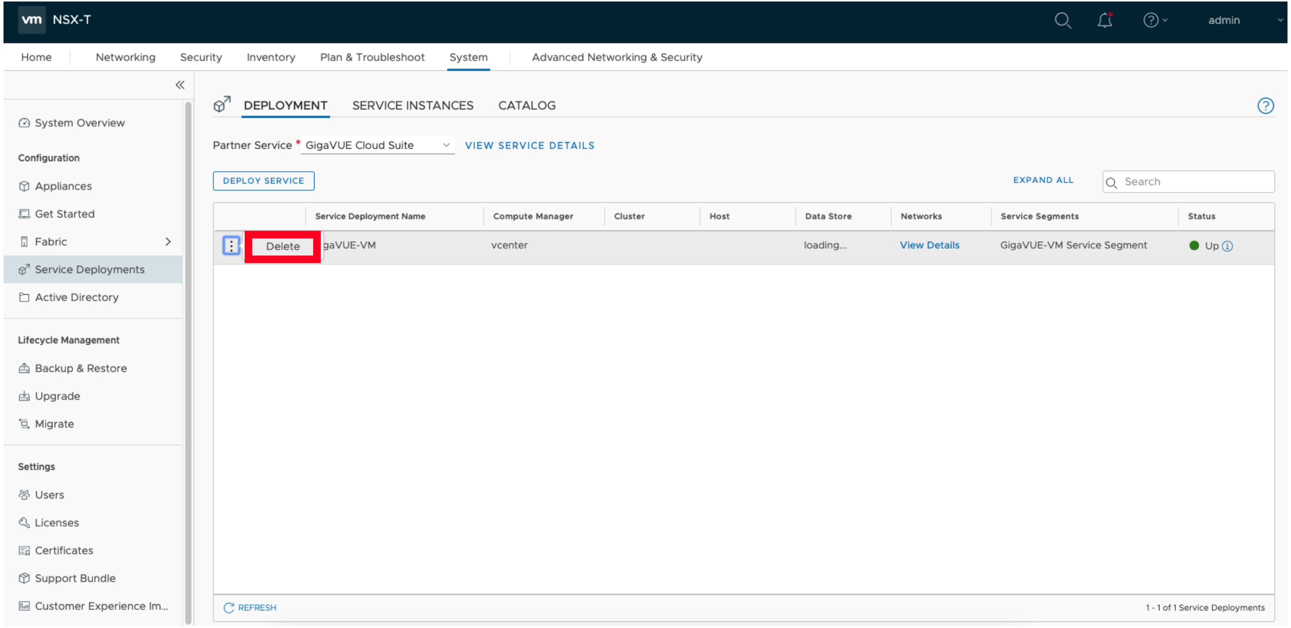
1. From NSX-T Manager, navigate to **System > Service Deployments**.
2. In the **DEPLOYMENT** tab, Select the select the service name of the Monitoring Domain from the **Partner Service** drop-down.



Partner Service * GigaVUE Cloud Suite

Service Deployment Name	Compute Manager	Cluster	Host	Data Store	Networks	Service Segments	Status
GigaVUE-VM	vcenter			loading...	View Details	GigaVUE-VM Service Segment	Up

3. Delete all the existing Service Deployments.

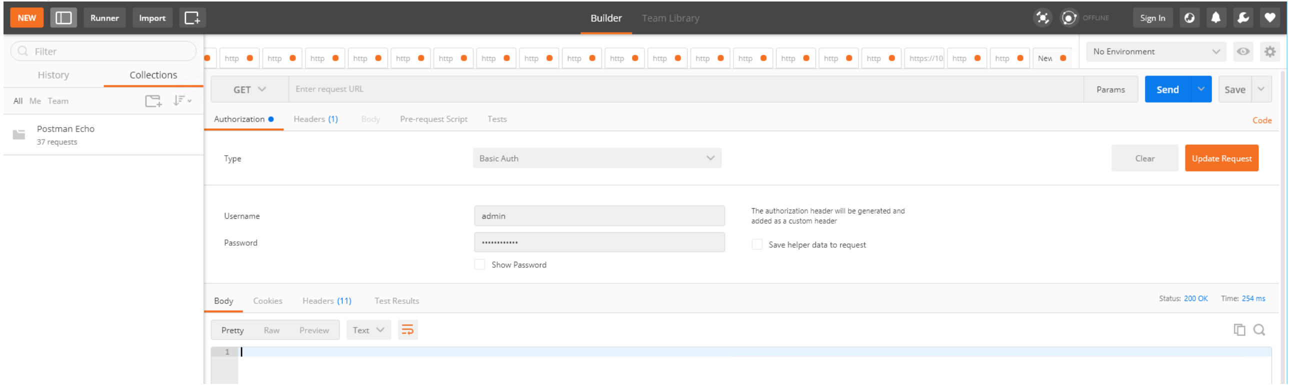


Partner Service * GigaVUE Cloud Suite

Service Deployment Name	Compute Manager	Cluster	Host	Data Store	Networks	Service Segments	Status
gaVUE-VM	vcenter			loading...	View Details	GigaVUE-VM Service Segment	Up

To remove the Service Deployments through NSX-T API:

1. Login to Postman.



Type: Basic Auth

Username: admin

Password: ••••••••••••

The authorization header will be generated and added as a custom header

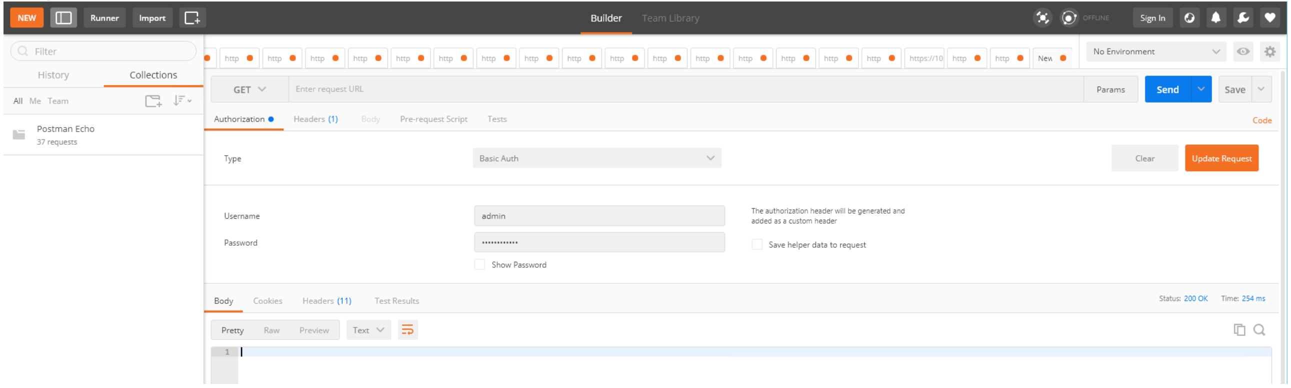
Status: 200 OK Time: 254 ms

2. Get the Service ID. **GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/
3. Get the ID of the Service Deployments.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/
4. Delete all Service Deployments.**DELETE** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/<Service_Deployment_ID>

Remove Service Reference

To remove Service References through NSX-T API:

1. Login to Postman.



Type: Basic Auth

Username: admin

Password: ••••••••••••

The authorization header will be generated and added as a custom header

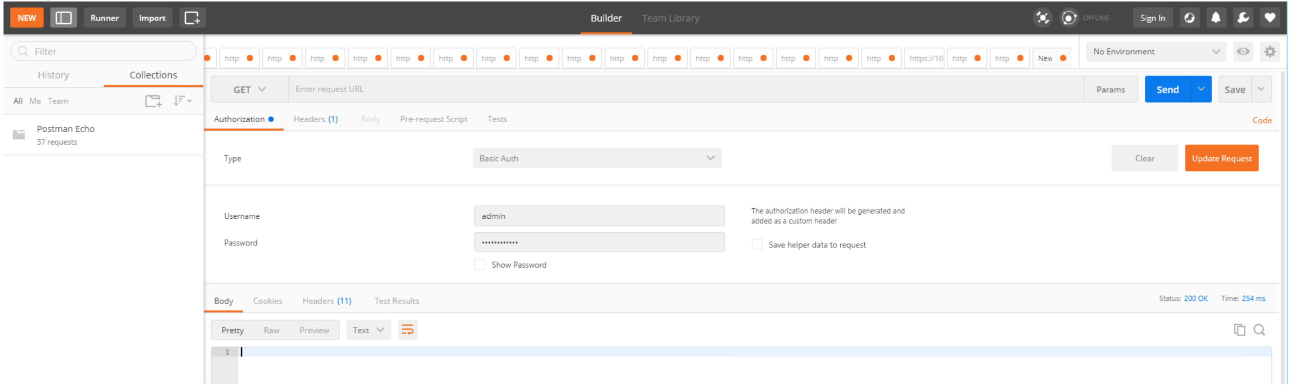
Status: 200 OK Time: 254 ms

2. Get the Service Reference ID.**GET** https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/
3. Delete the Service Reference.**DELETE** https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/<Service_Reference_ID>

Remove Service Manager

To remove Service Manager through NSX-T API:

1. Login to Postman.



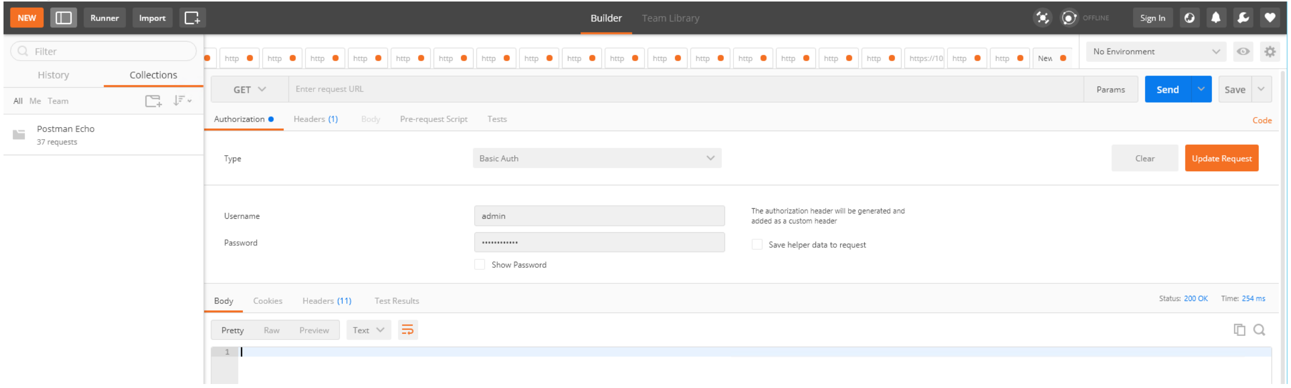
Type: Basic Auth
Username: admin
Password: ••••••••••••
Status: 200 OK Time: 254 ms

2. Get the Service Manager ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/service-managers/
3. Delete the Service Manager.**DELETE** https://<NSX_Manager_IP>/api/v1/serviceinsertion/serivce-managers/<Service_Manager_ID>

Remove Vendor Template and Service Definition

To remove Vendor Template and Service Definition through NSX-T API:

1. Login to Postman.



Type: Basic Auth
Username: admin
Password: ••••••••••••
Status: 200 OK Time: 254 ms

2. Get the Service ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/
3. Get the Vendor Templates' ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/vendor-templates/
4. Delete the Vendor Templates.**DELETE** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/vendor-templates/<Vendor_Template_ID>
5. Delete the Service.**DELETE** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>

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:

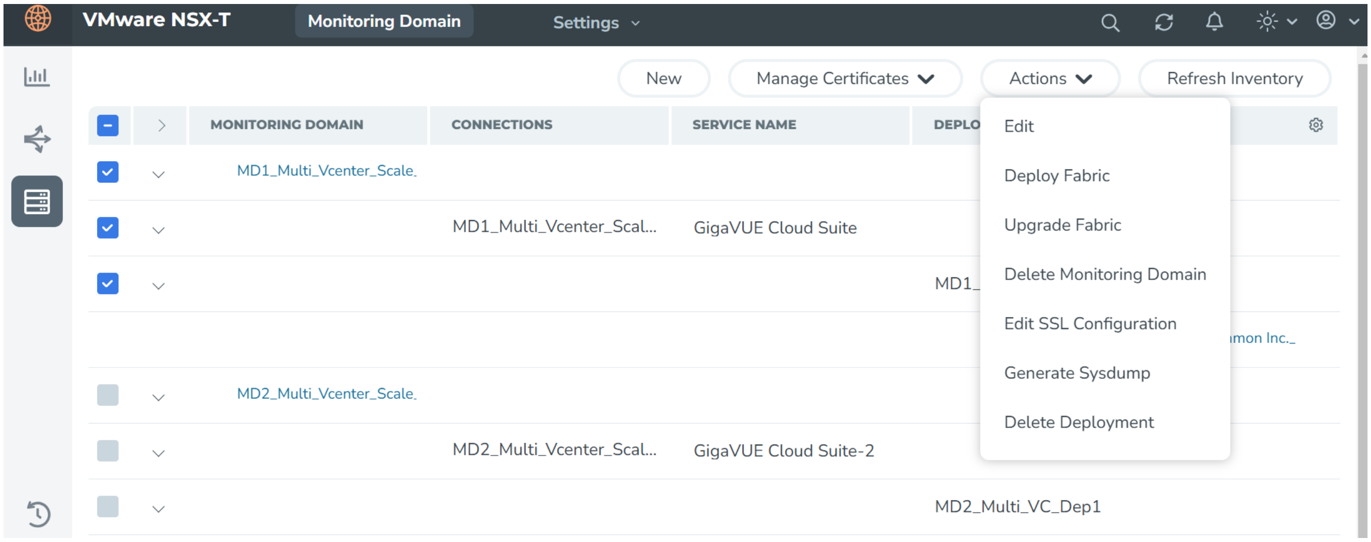
- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when generation of another sysdump file is in progress.
- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites 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. Perform one of the following:
   - Go to **Inventory > VIRTUAL > VMware NSX-T > Monitoring Domain.**
   - Go to **Inventory > VIRTUAL > VMware ESXi > Monitoring Domain.**
   - Go to **Inventory > VIRTUAL > Third Party Orchestration > Monitoring Domain.**
   - Go to **Inventory > VIRTUAL > Nutanix > Monitoring Domain.**

   The **Monitoring Domain** page appears.
2. 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**.
3. View the latest status, click **Refresh**.



MONITORING DOMAIN	CONNECTIONS	SERVICE NAME	DEPLO
MD1_Multi_Vcenter_Scale_			
	MD1_Multi_Vcenter_Scal...	GigaVUE Cloud Suite	
			MD1_
			ımon Inc._
MD2_Multi_Vcenter_Scale_			
	MD2_Multi_Vcenter_Scal...	GigaVUE Cloud Suite-2	
			MD2_Multi_VC_Dep1

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. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. **Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?**

   No. The upgrade process remains unchanged across all supported upgrade paths. You can upgrade your nodes without any additional steps. The upgrade results in the automatic deployment of the appropriate certificates based on the node versions

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self-Signed Certificate

2. **What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?**

   Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions:

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. **What are the new ports that must be added to the security groups?**

   The following table lists the port numbers that must be opened for the respective fabric components:

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80, 8892
GigaVUE V Series Proxy	8300, 80, 8892
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to 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 VÜE Community

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.11 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)