GigaVUE Cloud Suite Deployment Guide - VMware

GigaVUE Cloud Suite

Product Version: 6.4

Document Version: 1.0

Last Updated: Friday, November 24, 2023

(See Change Notes for document updates.)

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

Contents

GigaVUE Cloud Suite Deployment Guide - VMware

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 Visibility Platform, 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 acquires, optimizes, and distributes selected traffic to your monitoring and security tools. GigaVUE Cloud Suites for VMware provides tight integration with orchestration tools to deliver intelligent network traffic visibility for workloads running in Virtual machine in VMware. GigaVUE-FM , part of the Cloud Suite, works with VMware vCenter and VMware NSX-T to automatically deploy GigaVUE V Series Node to support a growing private cloud infrastructure. GigaVUE-FM leverages dynamic service chaining and workload relocation monitoring to ensure visibility and policy integrity.

GigaVUE Cloud Suite for VMware provides the following benefits:

Flexible Traffic Acquisition: Acquires traffic through port mirroring in VMware ESXi or service insertion for VMware NSX-Tenvironments.

Automated Visibility Provisioning: Dynamically provisions and applies traffic policies as new tenants come on board or as groups scale.

Increased Tool Efficiency: Reduces load on tools by selectively filtering, de-duplicating, and load balancing traffic sent to security and performance monitoring tools.

Application Intelligence solution: You can use Application Intelligence to identify thousands of applications and utilize over 7,000 application metadata elements.

Components for GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware comprises multiple elements that enable traffic acquisition, aggregation, intelligence and distribution, along with centralized, single-pane-of-glass orchestration and management. The solution consists of these components:

Component	Description
GigaVUE® Fabric Manager (GigaVUE-FM)	GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud Suite for VMware. GigaVUE-FM generates an end-to-end topology view through a single-pane-of-glass GUI, which gives you insights into which cloud instances are or are not part of the deep observability pipeline. A single instance of GigaVUE-FM can manage hundreds of visibility nodes across on-premises and multi-cloud environments. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform.
GigaVUE® V Series Proxy	The GigaVUE V Series Proxy is a optional component. If GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network, a Proxy should be used. It can also be used if there is a large number of nodes connected to GigaVUE-FM or if you wish to keep IP addresses of the nodes private. It manages multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series Nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series Nodes. A single GigaVUE V Series Proxy can be launched to provide the GigaVUE-FM network communication to hundreds of GigaVUE V Series Nodes present in private networks behind the Proxy.

Component	Description
GigaVUE® V Series Node	A visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools.

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
	v8.0	v8.0	v8.0	v6.3.00, v6.4.00
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
	v4.0.0	v7.0U3	v7.0U3	v6.0.00, v6.1.00, v6.2.00, v6.3.00
	v4.1.0	v7.0U3 v8.0	v7.0U3 v8.0	v6.3.00, v6.4.00

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 provide information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics.

Licensing for Cloud Suite is volume-based. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your V Series Nodes to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility on the actual amount of data, each licensed application is using on each node, and tracks the overuse, if any.

Volume-based licenses are available as monthly subscription licenses with a service period of 1 month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

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

Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

The bundles are available as SKUs[1]. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

Bundle Replacement Policy

Refer to the following notes:

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

- You can always upgrade to a higher bundle but you cannot move to a lower version.
- You cannot have two different base bundles at the same time however, you can have multiple base bundles of the same type.
- Once upgraded to a higher bundle, the existing lower bundles will be automatically deactivated.

Add-on Packages

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

Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

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

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

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM tracks the license usage for each V series node as follows:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
- When a license goes into grace period, you will be notified with an audit log.
- When a license finally expires (and has not been renewed yet), you will be notified by an audit log. Monitoring sessions using the corresponding license will not be undeployed.

For releases prior to 6.4:

- The monitoring sessions using the corresponding license will be undeployed (but not deleted from the database).
- When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

Manage Volume-based Licenses

To manage active Volume-based License:

1. On the left navigation pane, click ⚙.
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

   This page lists the following information about the active Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license
Bundles	Bundle to which the license belongs to
Volume	Total daily allowance volume
Starts	License start date
Ends	License end date
Type	Type of license (Commercial, Trial, Lab and other license types).
Activation ID	Activation ID
Entitlement ID	Entitlement ID

Note: The License Type and Activation ID are displayed by default in the VBL Active page. To display the Entitlement ID field, click on the column setting configuration option to enable the Entitlement ID field.

The expired licenses are displayed in the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar. This page lists the following information about the inactive Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license.
Bundles	Bundle to which the license belongs to.
Ends	License end date
Grace Period	Number of days the license is in grace period

Field	Description
Deactivation Date	Date the license got deactivated.
Revocation Code	License revocation code.
Status	License status.

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

Use the following buttons to manage your VBL.

Button	Description
Activate Licenses	Use this button to activate a Volume-based License. Refer to Activate Volume-based Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page.
Export	Use this button to export the details in the VBL active page to a CSV or XLSX file.
Deactivate	Use this button to deactivate the licenses. You can only deactivate licenses that are in grace period or that have expired.

For more detailed information on dashboards and reports generation for Volume-based Licensing refer to the following table:

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

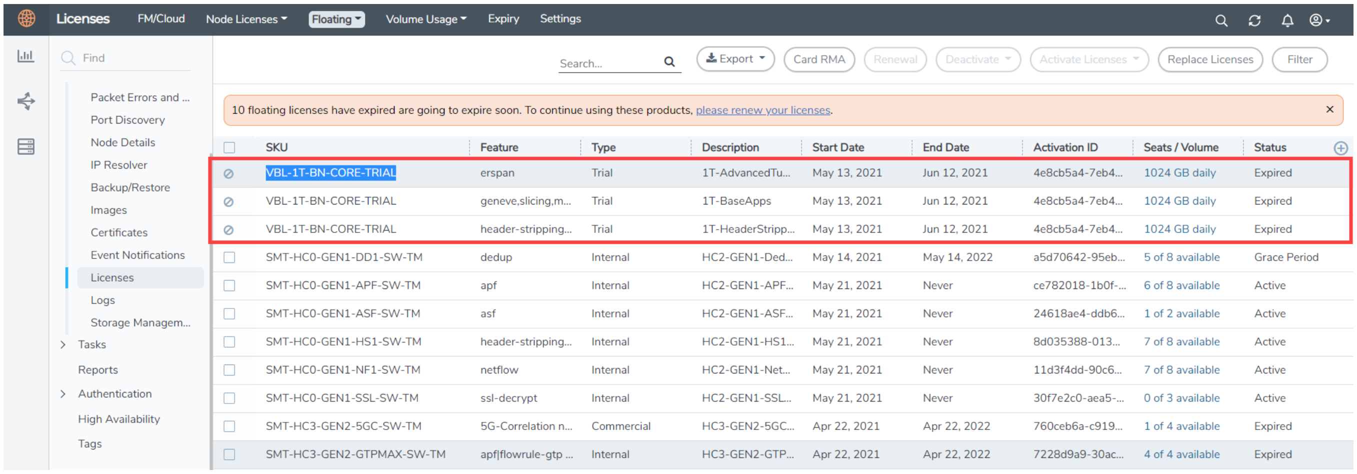
Activate Volume-based Licenses

To activate Volume-based licenses:

1. On the left navigation pane, click ⚙.
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears. Perform the following steps:
   a. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the What is a Fabric Inventory File? section for more details.
   b. Navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
   c. Return to GigaVUE-FM and add the additional licenses.

Default Trial Licenses

After you install GigaVUE-FM, a default free 1TB of CoreVUE trial volume-based license (VBL) is provided one-time for 30 days (from the date of installation).



10 floating licenses have expired are going to expire soon. To continue using these products, please renew your licenses.

	SKU	Feature	Type	Description	Start Date	End Date	Activation ID	Seats / Volume	Status
⊘	VBL-1T-BN-CORE-TRIAL	erspan	Trial	1T-AdvancedTu...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
⊘	VBL-1T-BN-CORE-TRIAL	geneve,slicing,m...	Trial	1T-BaseApps	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
⊘	VBL-1T-BN-CORE-TRIAL	header-stripping...	Trial	1T-HeaderStripp...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
□	SMT-HC0-GEN1-DD1-SW-TM	dedup	Internal	HC2-GEN1-Ded...	May 14, 2021	May 14, 2022	a5d70642-95eb...	5 of 8 available	Grace Period
□	SMT-HC0-GEN1-APF-SW-TM	apf	Internal	HC2-GEN1-APF...	May 21, 2021	Never	ce782018-1b0f-...	6 of 8 available	Active
□	SMT-HC0-GEN1-ASF-SW-TM	asf	Internal	HC2-GEN1-ASF...	May 21, 2021	Never	24618ae4-ddb6...	1 of 2 available	Active
□	SMT-HC0-GEN1-HS1-SW-TM	header-stripping...	Internal	HC2-GEN1-HS1...	May 21, 2021	Never	8d035388-013...	7 of 8 available	Active
□	SMT-HC0-GEN1-NF1-SW-TM	netflow	Internal	HC2-GEN1-Net...	May 21, 2021	Never	11d3f4dd-90c6...	7 of 8 available	Active
□	SMT-HC0-GEN1-SSL-SW-TM	ssl-decrypt	Internal	HC2-GEN1-SSL...	May 21, 2021	Never	30f7e2c0-aea5-...	0 of 3 available	Active
□	SMT-HC3-GEN2-5GC-SW-TM	5G-Correlation n...	Commercial	HC3-GEN2-5GC...	Apr 22, 2021	Apr 22, 2022	760ceb6a-c919...	1 of 4 available	Expired
□	SMT-HC3-GEN2-GTPMAX-SW-TM	apf|flowrule-gtp ...	Internal	HC3-GEN2-GTP...	Apr 22, 2021	Apr 22, 2022	7228d9a9-30ac...	4 of 4 available	Expired

This license includes the following applications:

- ERSPAN
- Geneve
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap

- Header-stripping
- Add header

> **NOTE:** There is no grace period for the trial license. If you do not have any other Volume-based licenses installed, then after 30 days, on expiry of the trial license, any deployed monitoring sessions will be undeployed from the existing GigaVUE V Series Nodes.

To deactivate the trial VBL refer to Delete Default Trial Licenses section for details.

Delete Default Trial Licenses

GigaVUE-FM allows you to deactivate the default trial licenses from this page. To deactivate the license:

1. On the left navigation pane, click ⚙ .
2. Go to **System > Licenses >Floating**. Click **Activated**.
3. Click **Deactivate** > **Default Trial VBL**.

The VBL trial licenses is deactivated and is no longer listed in the Activated page. However, you can view these deactivated licenses from the Deactivated page.

Install Custom Certificate

GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controllers have default self-signed certificates installed. The communication between GigaVUE-FM and the fabric components happens in a secure way using these default self-signed certificates, however you can also add custom certificates like SSL/TLS certificate to avoid the trust issues that occurs when the GigaVUE V Series Nodes, GigaVUE V Series Proxy, or UCT-V Controllers run through the security scanners.

You can upload the custom certificate in two ways:

- Upload Custom Certificates using GigaVUE-FM
- Upload Custom Certificate using Third Party Orchestration

Upload Custom Certificates using GigaVUE-FM

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

1. Go to **Inventory > Security > Custom SSL Certificate**. The **Custom Certificate Configuration** page appears.
2. On the Custom Certificate Configuration page, click **Add**. The **New Custom Certificate**

page appears.

3. Enter or select the appropriate information as shown in the following table.

Field	Action
Certificate Name	Enter the custom certificate name.
Certificate	Click on the Upload Button to upload the certificate.
Private Key	Click on the Upload Button to upload the private key associated with the certificate.

4. Click **Save**.

You must also add root or the leaf CA certificate in the Trust Store. For more detailed information on how to add root CA Certificate, refer to Trust Store topic in *GigaVUE Administration Guide*.

The certificates uploaded here can be linked to the respective GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in the Fabric Launch Configuration Page. Refer to *Configure GigaVUE Fabric Components in GigaVUE-FM* topic in the respective cloud guides for more detailed information.

Upload Custom Certificate using Third Party Orchestration

You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform at the time of deploying the fabric components. Refer to the following topics on more detailed information on how to upload custom certificates using third party orchestration in the respective platforms:

For integrated mode:

- Configure GigaVUE Fabric Components in AWS
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in OpenStack

For generic mode:

- Configure GigaVUE Fabric Components in AWS
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in GCP
- Configure GigaVUE Fabric Components in Nutanix
- Configure GigaVUE Fabric Components in OpenStack
- Configure GigaVUE V Series Nodes using VMware ESXi

Cloud Overview Page

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms, Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

Go to **Traffic > Virtual > Orchestrated Flows > Overview**. The Cloud Homepage appears.

Virtual Dashboard Widgets

This section describes the widgets that can be viewed on the overview page.

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Summary (Monitoring Session details)
- Traffic Rate
- Aggregate Summary

Overview

The overview dashboard displays the number of GigaVUE V Series Nodes active in GigaVUE-FM, number of Monitoring sessions and connections configured in all the platofrms, and the number of alarms triggered in V Series Nodes.

V Series Alarms

The V Series Alarms widget presents a pie chart that helps you to quickly to view the V Series alarms generated . Each type of alarm triggered is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of V Series alarms triggered.

Connection Status

The connection status presents a pie chart that helps you to quickly to view the connection status of connections configured in the monitoring domain. Each type of connection status is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of connected.

Usage

The Usage widget displays the amount of traffic that flows through the GigaVUE V Series Nodes. Each bar in the graph indicates the volume usage on a particular day. Hovering the mouse over a bar in the graph displays the volume allowance and volume usage on that particular day.

Summary

This widget allows you to view the list of all the available monitoring session along with the respective monitoring domain, platform, connection, their health status, V Series Node health status and the deployment status of the connection. You can click on the monitoring session name to view the **Edit Monitoring session** page of the respective monitoring session.

Traffic Rate

The traffic rate widget displays the rate of traffic flowing through the GigaVUE V Series Nodes. Each line in the graph indicates the rate of traffic flow for transmitting, receiving, and their ratio which is specified by the legend.

Aggregate Summary

The aggregate summary displays the highest daily volume usage, average daily volume usage, highest daily volume over usage, average daily volume over usage, 95th percentile daily volume usage and the average daily volume allowance.

Configure GigaVUE V Series Node on ESXi

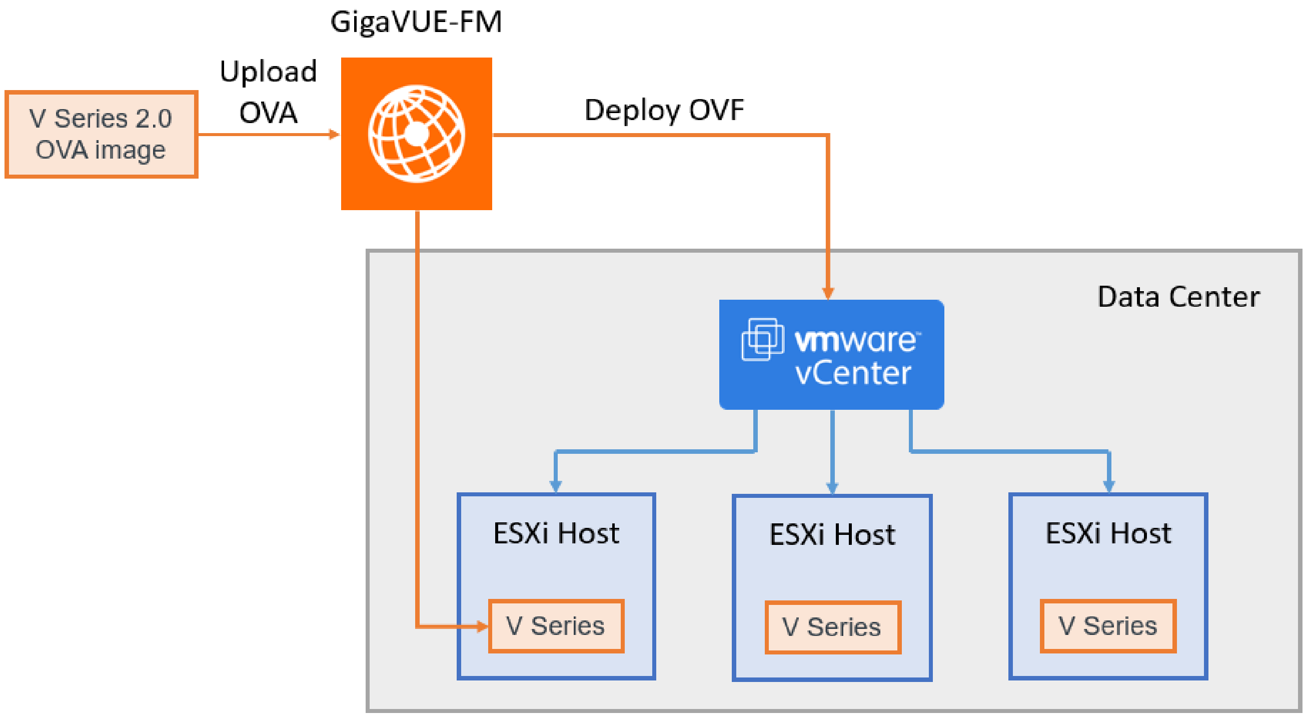
This document provides an overview of the GigaVUE V Series Node deployment on the VMware ESXi platforms and describes the procedure for setting up the traffic monitoring sessions using the GigaVUE V Series Nodes. TheGigaVUE V Series Nodes support traffic visibility on the following VMware networking elements:

- vSphere standard switch
- vSphere distributed switch

GigaVUE-FM creates, updates, and deletes the GigaVUE V Series Nodes in the ESXi hosts based on the configuration information provided by the user. The VMs and GigaVUE V Series Nodes are located in the same ESXi host and the traffic mirrored from VMs is sent to GigaVUE V Series Nodes. You can deploy only one GigaVUE V Series Node on a single ESXi host. GigaVUE-FM can communicate directly with the GigaVUE V Series Nodes.

- Ensure the source Virtual Machine and the tool is connected to different standard switches. When the source Virtual Machine and the tool are connected in the same standard switch, the traffic is looped.
- If NextGen Firewall (NGFW) with Deep Packet Inspection (DPI) is enabled to inspect your east-west traffic, there might be an increase in latency due to mirrored traffic. To avoid increased latency, create an exception rule for the tunneled traffic (mirrored traffic from the GigaVUE V Series Nodes to the tool) or configuring a private VDS that can bypass the NGFW rules for this traffic.

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



The chapter includes the following major sections:

- VMware ESXi System Requirements
- Prerequisites for Integrating V Series Nodes with ESXi
- Integrate GigaVUE V Series nodes with VMware ESXi
- Configure Application Intelligence Solutions on GigaVUE V Series Nodes for VMware ESXi

NOTE: These steps assume that VMware ESXi is installed and configured. Refer to VMware Documentation for configuration details.

Refer to the following Gigamon Validated Designs for more detailed information:

- Deploying GigaVUE Cloud Suite on VMware vCenter in a multi-tier DC Environment
- Deploying GigaVUE Cloud Suite for VMware vCenter 8 (6.3)

VMware ESXi System Requirements

To support internationalized characters in the VMware vCenter environment ensure that the vCenter character encoding is set to UTF-8.

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	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files
	vCenter					
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to communicate the traffic health updates with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
Remote Source	GigaVUE V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Nodes	Tool/ 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 Nodes	Tool/ HC Series instance	N/A	N/A	ICMP	Echo Request Echo Response	Allows GigaVUE V Series Node to health check tunnel destination traffic (Optional)
GigaVUE V Series Nodes	GigaVUE-FM	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM

Required VMware Virtual Center Privileges

This section lists the minimum privileges required for the GigaVUE-FM user in Virtual Center. You assign privileges to Virtual Center users by selecting **Administration** from the left navigation pane. Then select **Roles** under the **Access Control**. Roles should be applied at the vSphere Virtual Center level and not the Data Center or Host levels.

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

Category	Required Privilege	Purpose
Datastore	Allocate space	V Series Node Deployment
Distributed Switch	VSPAN Operation	VDS Tapping
Folder	Create Folder	V Series Node Deployment
Host	**Configuration** • Network Configuration	VSS Tapping
	Inventory • Modify Cluster	Pin V Series Node to the host in cluster configurations. This prevents automatic migration.
Network	• Assign network • Configure	● V Series Node Deployment/VSS Tapping ● V Series Node Deployment
Resource	Assign virtual machine to	V Series Node Deployment

Category	Required Privilege	Purpose
	resource pool	
vApp	● Import ● vApp instance configuration ● vApp application configuration	V Series Node Deployment
Virtual machine	**Configuration** • Add new disk • Add or remove device • Modify device settings • Rename	V Series Node Deployment V Series Node Deployment/VSS Tapping
	Interaction • Connect devices • Power on • Power Off • Reset	V Series Node Deployment
	Inventory ▪ Create from existing ▪ Remove	V Series Node Deployment
	Provisioning ▪ Clone virtual machine	V Series Node Deployment

Prerequisites for Integrating V Series Nodes with ESXi

The following are the prerequisites for integrating V Series nodes with ESXi:

- Refer to Supported Hypervisors for VMware for supported VMware vCenter, VMware ESXi and VMware NSX-T versions.
- ESXi hosts must have the minimum vCPU and memory resources for hosting the GigaVUE V Series Nodes. Refer to Recommended Form Factor (Instance Types) for more information.
- GigaVUE V Series Node device OVA image file.
- All the target VMs must have VMware guest tools or Open VM tools if you use IP based filtering.
- Refer to VMware ESXi System Requirements for ESXi host resource requirement to deploy GigaVUE V Series Nodes.

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

Recommended Form Factor (Instance Types)

The form factor (instance) 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 (instance types) and sizes based on memory and the number of vCPUs for a single GigaVUE 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	vNIC
Small	4GB	2vCPU	8GB	1 Management interface, 1 Tunnel interface, and 8 vTAP interfaces
Medium	8GB	4 vCPU		
Large	16GB	8 vCPU		

NOTE: For any queries on which form factor to use, reach out to your account manager or contact Gigamon Technical Support.

Default Login Credentials

You can login to the GigaVUE V Series Node 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: Enter the password provided during the fabric launch configuration. Refer Configure GigaVUE V Series Nodes for VMware ESXi for more detailed information on fabric launch configuration.

Integrate GigaVUE V Series nodes with VMware ESXi

To integrate V Series nodes with ESXi, perform the following steps:

- Upload GigaVUE V Series Node Image into GigaVUE-FM
- Create Monitoring Domain for VMware ESXi

- Configure GigaVUE V Series Nodes for VMware ESXi
- Rediscover
- Configure Monitoring Session
- Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi
- Configure VMware Settings

The below table provides step-by-step instructions on configuring GigaVUE Cloud Suite for VMware for providing visibility to physical and virtual traffic. Refer to the VMware ESXi System Requirements and Prerequisites for Integrating V Series Nodes with ESXi sections for prerequisites that are required to be configured.

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

Upload GigaVUE V Series Node Image into GigaVUE-FM

This step is optional, you can also upload the GigaVUE V Series Node Image into GigaVUE-FM, when deploying the GigaVUE V Series Node. Refer to Configure GigaVUE V Series Nodes for VMware ESXi .

To upload the V Series image into GigaVUE-FM:

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

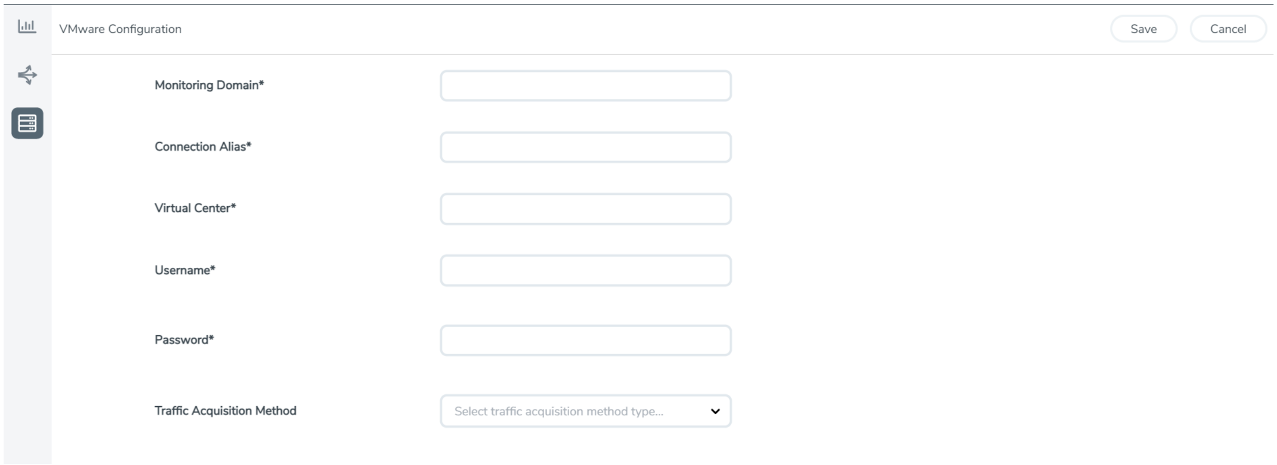
> **NOTE:** The maximum number of OVA files that can be uploaded to GigaVUE-FM is three.

Create Monitoring Domain for VMware ESXi

This chapter describes how to create a monitoring domain for deploying V Series node in VMware ESXi hosts. You must establish a connection between GigaVUE-FM and your vCenter environment before you can perform the configuration steps for GigaVUE V Series Node.

To configure VMware vCenter in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware vCenter (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*	
Connection Alias*	
Virtual Center*	
Username*	
Password*	
Traffic Acquisition Method	Select traffic acquisition method type...

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 FQDN of the vCenter
Username	Username of the vCenter user with minimum privileges as described in **Required VMware Virtual Center Privileges** section.
Password	vCenter password used to connect to the vCenter
Traffic Acquisition Method	Select a Tapping method. **Platform Tapping**: Platform tapping can be done in two ways. • VSS: Platform Tapping can be used when a workload Virtual Machine is connected to a Virtual Standard Switch network. Promiscuous network will be created on VSS switch by GigaVUE-FM for tapping the traffic. • VDS: Platform Tapping can be used when a workload Virtual Machine is connected to a Virtual Distributed Switch portgroup. Port Mirroring will be created on the VDS switch by GigaVUE-FM for tapping the traffic **Customer Orchestrated Source**: If you use select Customer Orchestrated Source as the tapping method, you can select the tunnel or raw endpoint as a source where the traffic is directly tunneled to GigaVUE V Series nodes. **NOTE:** When using AMX application select the traffic acquisition Method as Customer Orchestrated Source.

4. Click **Save**.

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

Buttons	Description
Edit	Use to edit a monitoring domain.
Deploy Fabric	Use to deploy GigaVUE V Series Nodes.
Upgrade Fabric	Use to upgrade GigaVUE V Series Nodes. Refer to Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi for more detailed information on how to upgrade.
Delete Monitoring Domain	Use to delete a monitoring domain.
Delete Fabric Nodes	Use to delete a GigaVUE V Series Node.
Disconnect	Use to stop the communication between GigaVUE-FM and the VMware vCenter.
Rediscover	The changes made in vCenter for the GigaVUE V Series Node will be reflected in GigaVUE-FM. Refer to Rediscover topic for more detailed information.
Power On	You can select an individual GigaVUE V Series Node and power it on. The status of the GigaVUE V Series Node is changed to **Ok**.
Power Off	You can select an individual GigaVUE V Series Node and power it off. If the GigaVUE V Series Node is turned off from GigaVUE-FM, then it will not be considered as part of Cloud Health Monitoring and GigaVUE-FM will not try to turn it on. The status of the GigaVUE V Series Node is changed to **Down**.
Reboot	You can select an individual GigaVUE V Series Node and reboot it.

Configure GigaVUE V Series Nodes for VMware ESXi

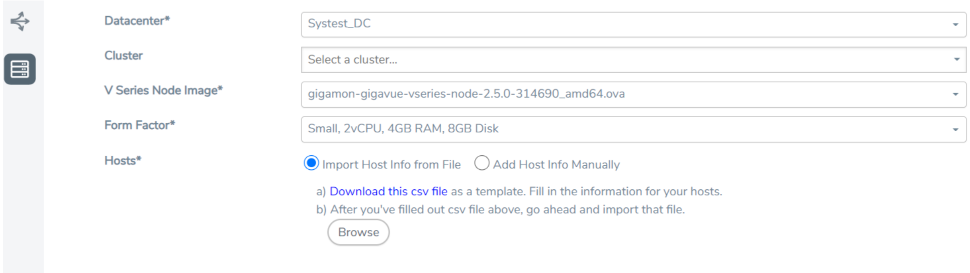
This section provides step-by-step information on how to deploy GigaVUE V Series Nodes.

After establishing a connection between GigaVUE-FM and VMware ESXi, GigaVUE-FM launches the configuration for the GigaVUE V Series Node.

To deploy GigaVUE V Series Nodes using GigaVUE-FM, follow the steps given below:

1. After VMware Configuration in GigaVUE-FM, you are navigated to the **VMware Fabric Launch Configuration** page.

2. You can also open **VMware Fabric Launch Configuration** page from the monitoring domain. To launch the **VMware Fabric Launch Configuration** from the Monitoring Domain, click **Actions** and then select **Deploy Fabric** from the drop-down. The **VMware Fabric Launch Configuration** page appears.



Datacenter*	Systest_DC
Cluster	Select a cluster...
V Series Node Image*	gigamon-gigavue-vseries-node-2.5.0-314690_amd64.ova
Form Factor*	Small, 2vCPU, 4GB RAM, 8GB Disk
Hosts*	● Import Host Info from File ○ Add Host Info Manually

a) Download this csv file as a template. Fill in the information for your hosts.
b) After you've filled out csv file above, go ahead and import that file.

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

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td><b>Datacenter</b></td><td colspan="2">vCenter Data Center with the ESXi hosts to be provisioned with V Series nodes</td></tr>
<tr><td><b>Cluster</b></td><td colspan="2">Cluster where you want to deploy V Series nodes</td></tr>
<tr><td rowspan="10"><b>Hosts</b></td><td colspan="2">Select the ESXi hosts for V Series deployment.
Select <b>Import Host Info from file</b> or <b>Add Host Info Manually</b>.
<b>Import Host Info from file:</b>
To import host details from a .csv file:
a. Download the .csv template file.
b. Enter the required values in the Excel sheet and save the file.
c. Click Browse and select the .csv file saved in the previous step.
<b>Add Host Info Manually:</b>
Select the ESXi hosts for V Series deployment.
The Common Configuration drop-down wizard appears. Expand the <b>Common Configuration</b> drop-down wizard and update the following details to apply the configuration to all the selected hosts.
You can also expand the individual hosts and modify the configurations that were applied in the <b>Common Configuration</b>.</td></tr>
<tr><td colspan="2"><b>Common Configuration</b></td></tr>
<tr><td>Datastore</td><td>Network datastore shared among all ESXi hosts.</td></tr>
<tr><td>V Series Node Name Prefix</td><td>Enter the prefix for the V Series Node name.</td></tr>
<tr><td>V Series Node Name Suffix</td><td>Enter the suffix for the V Series Node name.</td></tr>
<tr><td colspan="2"><b>Management</b></td></tr>
<tr><td>Network</td><td>Management network for V Series nodes.</td></tr>
<tr><td>IP Type</td><td>Select the management network IP type as Static or DHCP.</td></tr>
<tr><td>Gateway IP
<b>NOTE:</b> This field appears only when the Management <b>IP type</b> is Static.</td><td>Gateway IP address of the Management Network.</td></tr>
<tr><td>Netmask Length
<b>NOTE:</b> This field appears only when the Management <b>IP</b></td><td>Management network's subnet mask value in CIDR format. Eg. 21 for /21.</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td><b>type</b> is Static.</td><td></td></tr>
<tr><td colspan="2"><b>Tunnel</b></td></tr>
<tr><td>Network</td><td>Tunnel Network for the V Series nodes.</td></tr>
<tr><td>IP Type</td><td>Select the tunnel network IP address type as Static or DHCP.</td></tr>
<tr><td>Gateway IP (optional)</td><td>Gateway IP address of the Tunnel Network.</td></tr>
<tr><td>Netmask Length
<b>NOTE:</b> This field appears only when the Tunnel <b>IP type</b> is Static.</td><td>Tunnel network's subnet mask value in CIDR format. Eg. 21 for /21.</td></tr>
<tr><td>Use IPv6
<b>NOTE:</b> This field appears only when the Tunnel <b>IP type</b> is DHCP.</td><td>Enable to use IPv6.</td></tr>
</table>
</td></tr>
<tr><td><b>V Series Node Image</b></td><td>Select the OVA file uploaded in the Upload GigaVUE V Series Node Image into GigaVUE-FM, from the drop-down menu.
You can also add OVA files when launching the fabric. To add OVA files:
a. Click on the <b>Add</b> button.
b. The <b>Upload Image</b> dialog box opens. In the <b>Upload Image</b> dialog box, click <b>Browse</b> to select the <i>gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova</i> file.
c. Click <b>Upload to Server</b> to upload the selected OVA image file to GigaVUE-FM server.</td></tr>
<tr><td><b>Form Factor</b></td><td>Instance size of the V Series node. Refer Prerequisites for Integrating V Series Nodes with ESXi for more information.</td></tr>
<tr><td>Enable Custom Certificates</td><td>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.
<b>NOTE:</b> If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state.</td></tr>
<tr><td>Custom SSL Certificate</td><td>Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.</td></tr>
</table>

4. Click **Deploy**. After the V series node is deployed in vCenter, it appears on the Monitoring Domain page under Fabric tab of the selected Monitoring Domain.

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

Rediscover

When modifying the configurations of the GigaVUE V Series Node deployed in VMware vCenter, it may lead to configuration mismatch between the GigaVUE V Series Node and the virtual machine configuration present in GigaVUE-FM. You can use the Rediscover button in GigaVUE-FM to overcome this. The following GigaVUE V Series Node configuration can be rediscovered from GigaVUE FM:

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

NOTE: GigaVUE-FM performs an auto-rediscovery every 24 hours. Every 24 hours GigaVUE-FM checks for the above-mentioned things and updates the GigaVUE V Series Node configuration.

You can select an individual or multiple GigaVUE V Series Node in the Monitoring Domain page and click **Actions > Rediscover**.

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

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 traffics.

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

Refer to the following topics for details:

- Create a Monitoring Session
- Interface Mapping
- Create Raw Endpoint
- Create a New Map
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics
- Visualize the Network Topology
- Configure VMware Settings

Create a Monitoring Session

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

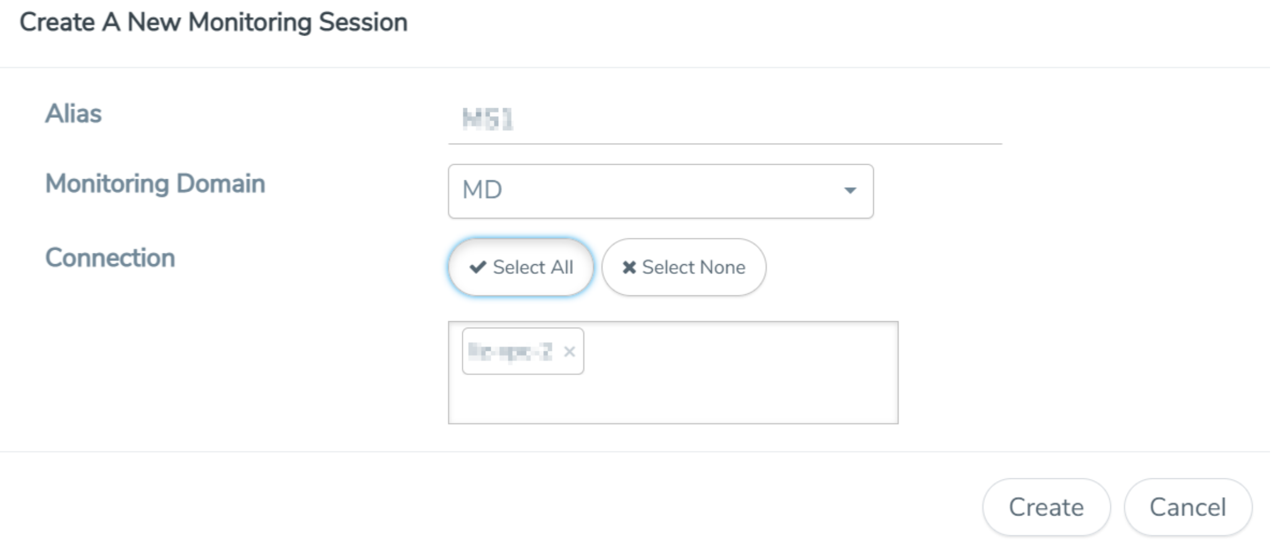
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

NOTE: You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows > VMware**. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.



Create A New Monitoring Session

Alias: MS1

Monitoring Domain: MD

Connection: ✓ Select All ✖ Select None

[illegible] ×

Create Cancel

3. Enter the appropriate information for the monitoring session as described in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain that you want to select.
Connection	The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.

4. Click **Create**. The Monitoring Session details page appears displaying the specified session information and target VMs.

> **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.

The Monitoring Session page also has the following buttons:

Button	Description
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
Delete	Deletes the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Deploy	Deploys the selected monitoring session.
Undeploy	Undeploys the selected monitoring session.
Apply Threshold	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates and how to apply threshold templates.

Edit Monitoring Session

In the edit monitoring session canvas page, you can add and configure applications, tunnel endpoints, raw endpoints, and maps.

Refer to the following topics for detailed information:

- Create Ingress and Egress Tunnels
- Add Applications to Monitoring Session
- Create Raw Endpoint
- Create a New Map

The **Edit Monitoring Session** page has the following buttons:

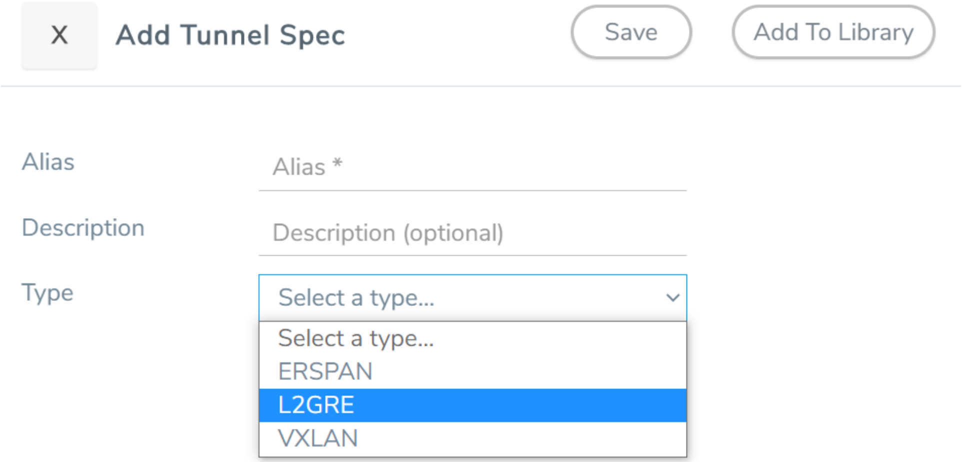
Button	Description
Show Targets	Use to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
Interface mapping	Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping topic for more details.
Deploy	Deploys the selected monitoring session. Refer to Deploy Monitoring Session topic for more details.

Create Ingress and Egress Tunnel

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.

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.


X
Add Tunnel Spec
Save
Add To Library
Alias
Alias *
Description
Description (optional)
Type
Select a type...
Select a type...
ERSPAN
L2GRE
VXLAN

3. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description	
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.	
Description	The description of the tunnel endpoint.	
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, or UDPGRE to create a tunnel.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled

Field	Description	
		with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the	

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

Field	Description	
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

Field	Description	
Out	**IP Version**	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

4. Click **Save**.

To delete a tunnel, select the required tunnel and click **Delete**.

To apply threshold template to Tunnel End Points, select the required tunnel end point on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold template, refer to *Monitor Cloud Health* topic.

After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

Tunnel End Points created here can also be viewed in the Tunnel Specifications page. Refer to Create Tunnel Specifications for more detailed information.

Interface Mapping

You can change the interface of individual GigaVUE V Series Nodes deployed in a monitoring session. After deploying the monitoring session, if you wish to change the interfaces mapped to an individual GigaVUE V Series Node, you can use the **Interface Mapping** button to map the interface to the respective GigaVUE V Series Nodes. To perform interface mapping:

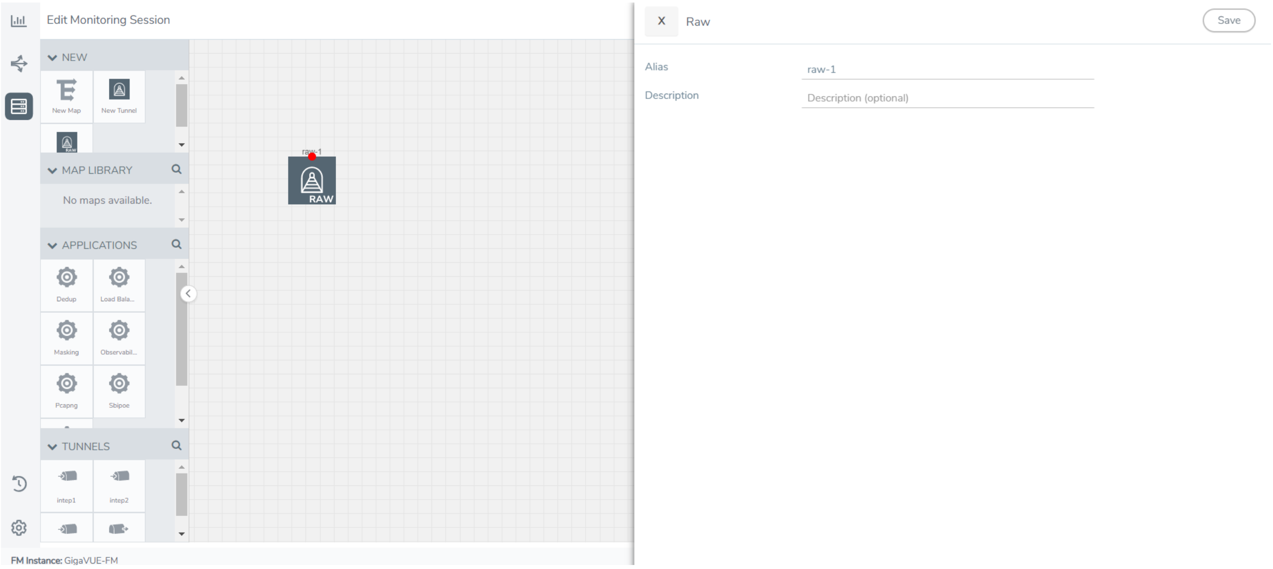
1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.
3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

Create Raw Endpoint

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

To add Raw Endpoint to the monitoring session:

1. Drag and drop **New RAW** from **NEW** to the graphical workspace.
2. Click the **New RAW** icon and select **Details**. The **RAW** quick view page appears.
3. Enter the alias and description. In the **Alias** field, enter a name for the Raw End Point and click **Save**.



Alias: raw-1

Description: Description (optional)

4. To deploy the monitoring session after adding the Raw Endpoint click the **Deploy** button on the edit monitoring session page.
5. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the V Series Nodes for which you wish to deploy the monitoring session.
6. After selecting the V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual V Series Nodes. Then, click **Deploy**.

Create a New Map

You must have the flow map license to deploy a map in monitoring session.

For new users, the free trial bundle will expire after 30 days and the GigaVUE-FM prompts you to buy a new license. For licensing information refer to *GigaVUE Licensing Guide*.

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

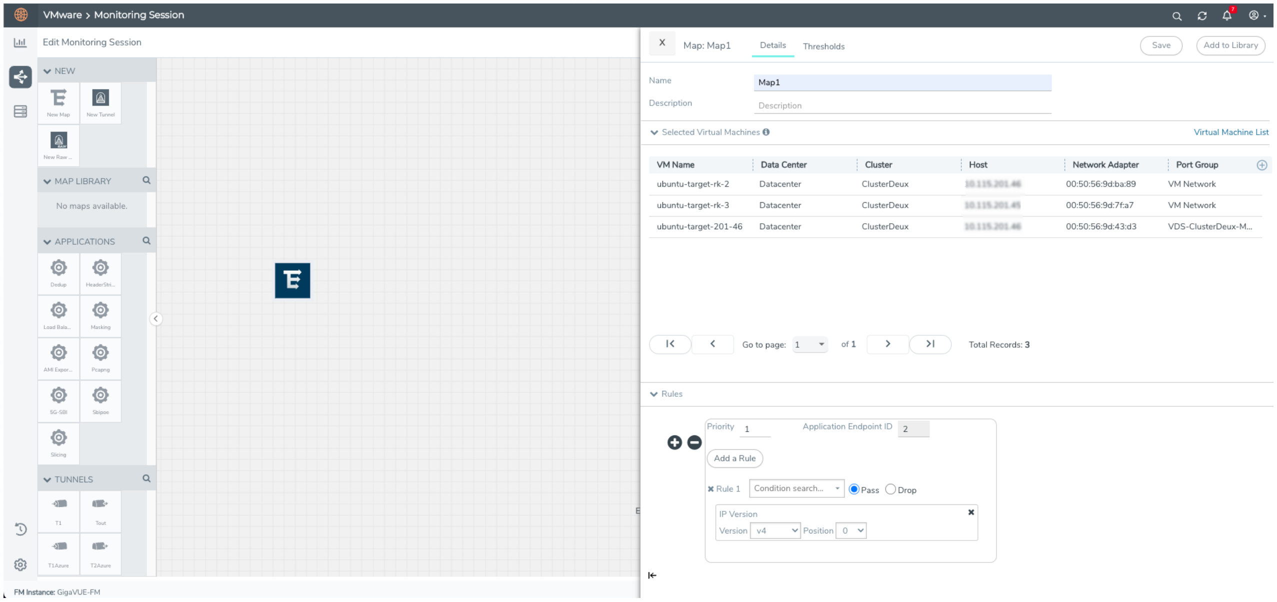
Keep in mind the following when creating a map:

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

Priority	A 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 ● VM Tag Source ● Host Name The traffic direction is as follow: ● For any rule type as Source - the traffic direction is egress. ● For Destination rule type - the traffic direction is ingress. ● For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **NOTE:** If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

To create a new map:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.



Name: Map1

Description: Description

VM Name	Data Center	Cluster	Host	Network Adapter	Port Group
ubuntu-target-rk-2	Datacenter	ClusterDeux	[redacted]	00:50:56:9d:ba:89	VM Network
ubuntu-target-rk-3	Datacenter	ClusterDeux	[redacted]	00:50:56:9d:7f:a7	VM Network
ubuntu-target-201-46	Datacenter	ClusterDeux	[redacted]	00:50:56:9d:43:d3	VDS-ClusterDeux-M...

Go to page: 1 of 1 Total Records: 3

Priority: 1 Application Endpoint ID: 2

Rule 1 Condition search... ● Pass ○ Drop

IP Version

Version: v4 Position: 0

3. On the New Map quick view, enter or select the required information as described in the following table.

Field	Description
Name	Name of the new map
Description	Description of the map
Selected Virtual Machines Using this option, you can select an individual Network adapter of a virtual machine as a target. You can also view and filter the list of virtual machines available. When using this option, you cannot use Automatic Target Selection (ATS).	
Virtual Machine List	Click on the **Virtual Machine List** button. The Virtual Machine List quick view opens. Select the virtual machines you wish to use as the target and click on the **Apply** button in the Virtual Machine List quick view to save your changes. You can also use the filter button to filter the virtual machines. To filter the list of virtual machines: Click on the **Filter** button to filter the virtual machines based on any of the following criteria: • Data Center • Cluster • Host Name • VM Name • VM Tag Category • VM Tag Name After selecting the details, click on the **Apply** button in the filter dialog box to apply the filters. The list of virtual machines appears based on the filter criteria. Select the virtual machines you wish to use as the target and click on the **Apply** button in the Virtual Machine List quick view to save your changes.

- VMware tools are not required to discover targets, since GigaVUE-FM can discover targets with ATS using the tags attached to the VMs.
- Targets can be selected by providing the VM's node name or the hostname as selection criteria. A host is selected when the hostname matches all the active targets.
- Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
    - Traffic Map—Only Pass rules for ATS
    - Inclusion Map—Only Pass rules for ATS
    - Exclusion Map—Only Drop rules for ATS

4. Click on **Rule Sets** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to Example- Create a New Map using Inclusion and Exclusion Maps for more detailed information on how to configure Inclusion and Exclusion maps using ATS.
    a. **To create a new rule set:**
        i. Click **Actions > New Rule Set**.
        ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
        iii. Enter the Application Endpoint in the Application EndPoint ID field.
        iv. Select a required condition from the drop-down list.
        v. Select the rule to **Pass** or **Drop** through the map.
    b. **To create a new rule:**
        i. Click **Actions > New Rule**.
        ii. Select a required condition from the drop-down list. Click ... and select **Add Condition** to add more conditions.
        iii. Select the rule to **Pass** or **Drop** through the map.
5. Click **Save**.

> **NOTE:** If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Map Statistics" section in *GigaVUE Fabric Management Guide*for detailed information.

To edit a map, select the map and click **Details**, or click **Delete** to delete the map.

To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.

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

- Click a map and select **Details** to edit the map
- Click a map and select **Delete** to delete the map.
- Click the **Show Targets** button to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
- Click ⤢ to expand the **Targets** dialog box. To view details about a GigaVUE V Series

Node, click the arrow next to the VM.

- In the Instances window, click ▼ to filter the list of instances.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a monitoring session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

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

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

Add Applications to Monitoring Session

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

- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- Header Stripping

- 5G-Service Based Interface Application
- Application Metadata Exporter
- SSL Decrypt

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

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

- Application Metadata Intelligence
- Application Filtering Intelligence

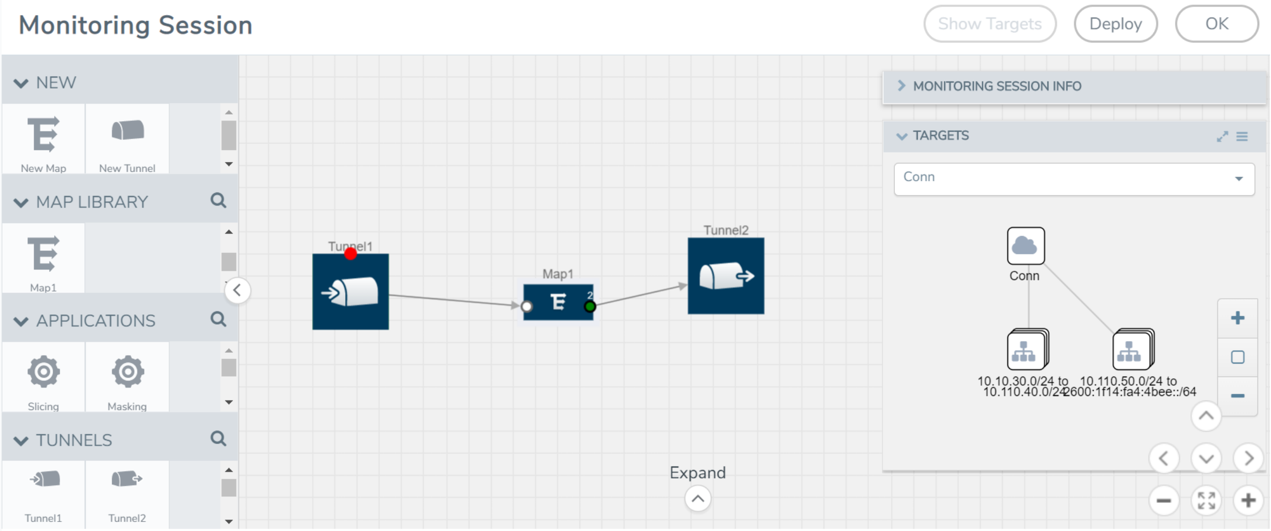
For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
   - Maps from the **MAP LIBRARY** section
   - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART apps from the **APPLICATIONS** section
   - Egress tunnels from the **TUNNELS** section
2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

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



3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
4. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.

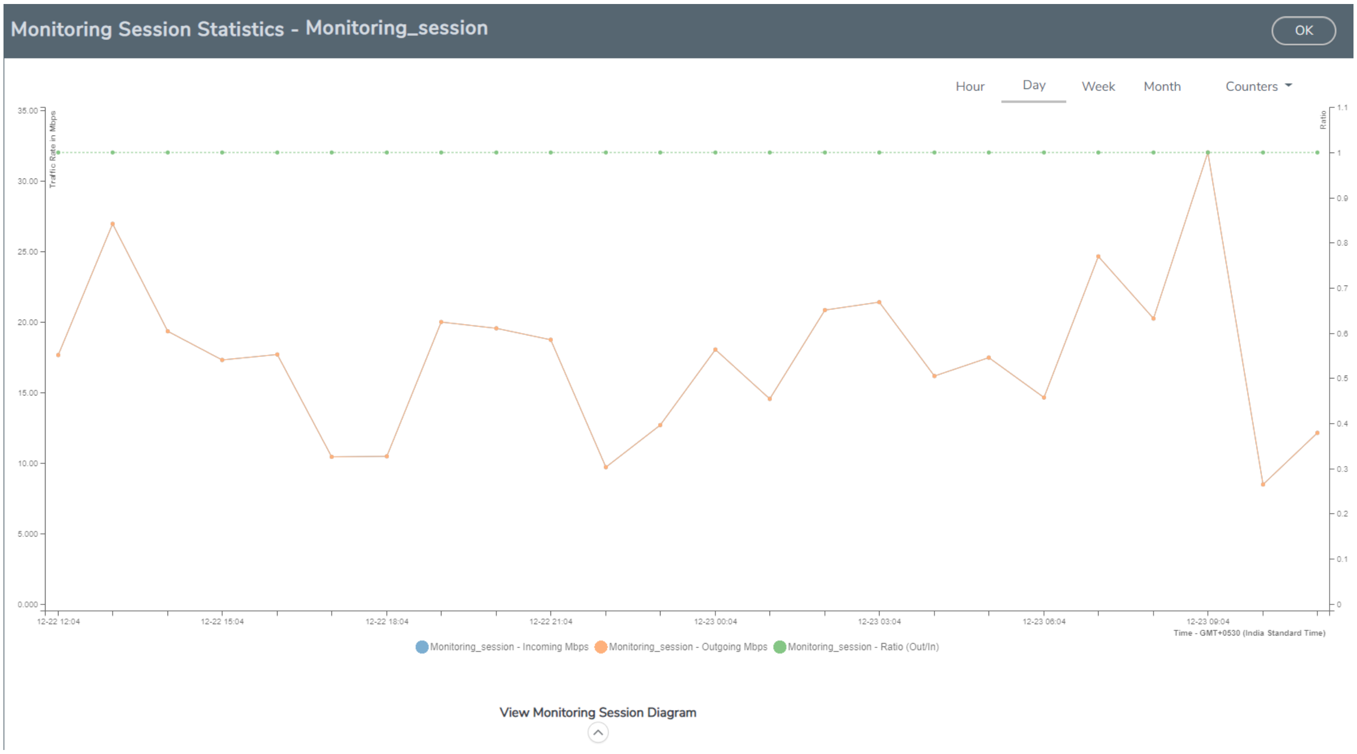
   The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

View Monitoring Session Statistics

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. The traffic can be viewed based on kilobits/second, megabits/second or gigabits/second.

On the Monitoring Sessions page, click **View** in the Statistics column to view the Monitoring Session Statistics page. The **Monitoring Session Statistics** page appears where you can analyze incoming and outgoing traffic.

> **NOTE:** If there are multiple monitoring sessions with different target selection, then the incoming maps will not show true statistics and it shows the aggregate traffic from all the targets.


Monitoring Session Statistics - Monitoring_session
OK
Hour
Day
Week
Month
Counters
Traffic Rate in Mbps
35.00
30.00
25.00
20.00
15.00
10.00
5.000
0.000
Ratio
1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
12-22 12:04
12-22 15:04
12-22 18:04
12-22 21:04
12-23 00:04
12-23 03:04
12-23 06:04
12-23 09:04
Time - GMT+0530 (India Standard Time)
● Monitoring_session - Incoming Mbps
● Monitoring_session - Outgoing Mbps
● Monitoring_session - Ratio (Out/In)
View Monitoring Session Diagram

You can also perform the following actions on the Monitoring Session Statistics page:

- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.
- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.
- Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

> 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.

View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page. Refer to Monitor Cloud Health for more detailed information on how to configure cloud health and view health status.

The following columns in the monitoring session page are used to convey the health status:

Health

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy then the health status is moved to unhealthy.

V Series Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

You can view the health status of the individual V Series Nodes by clicking on the V Series Node Health column.

NOTE: V Series Node health only displays the health status therefore even if the V Series Node is down it will not be reflected in the monitoring session page.

Target Source Health

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

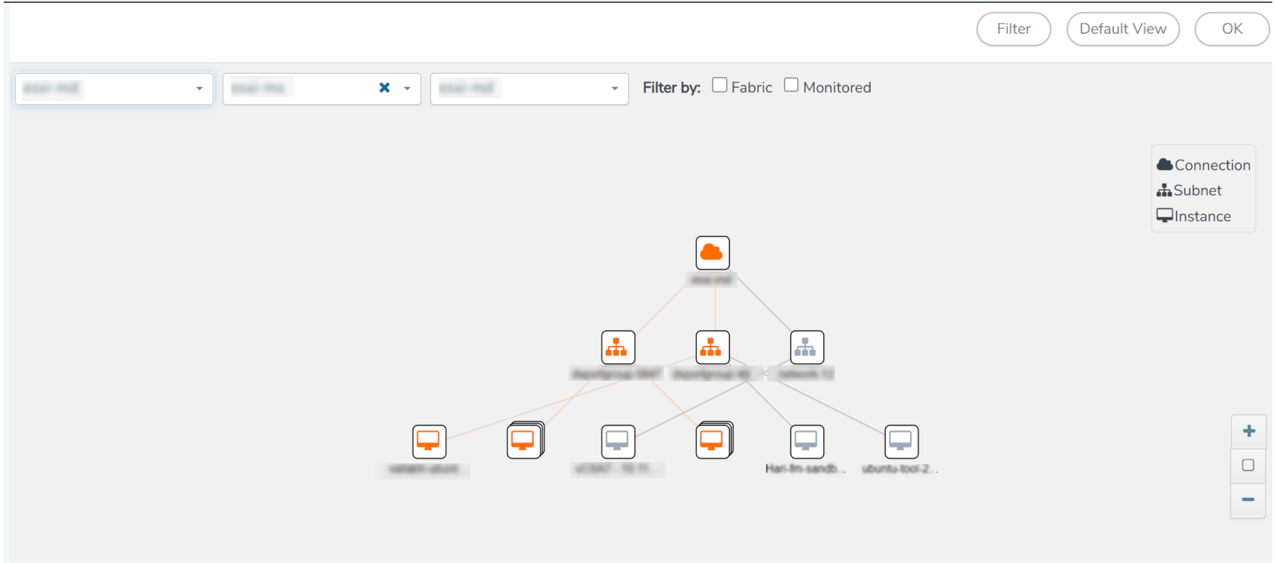
You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

Visualize the Network Topology

You can have multiple connections in GigaVUE-FM. Each connection can have multiple monitoring sessions configured within them. You can select the connection and the monitoring session to view the selected subnets and instances in the topology view.

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.
4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



5. (Optional) Hover over or click the subnet or VM Group icons to view the subnets or instances present within the group.

In the topology page, you can also do the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the right-bottom corner to move the topology page up, down, left, or right. Click the **Fit-to-Width** icon to fit the topology diagram according to the width of the page.
- Use **+** or **-** icons to zoom in and zoom out the topology view.

Upgrade GigaVUE V Series Node in GigaVUE-FM for ESXi

Keep in mind the following when upgrading the GigaVUE V Series Nodes:

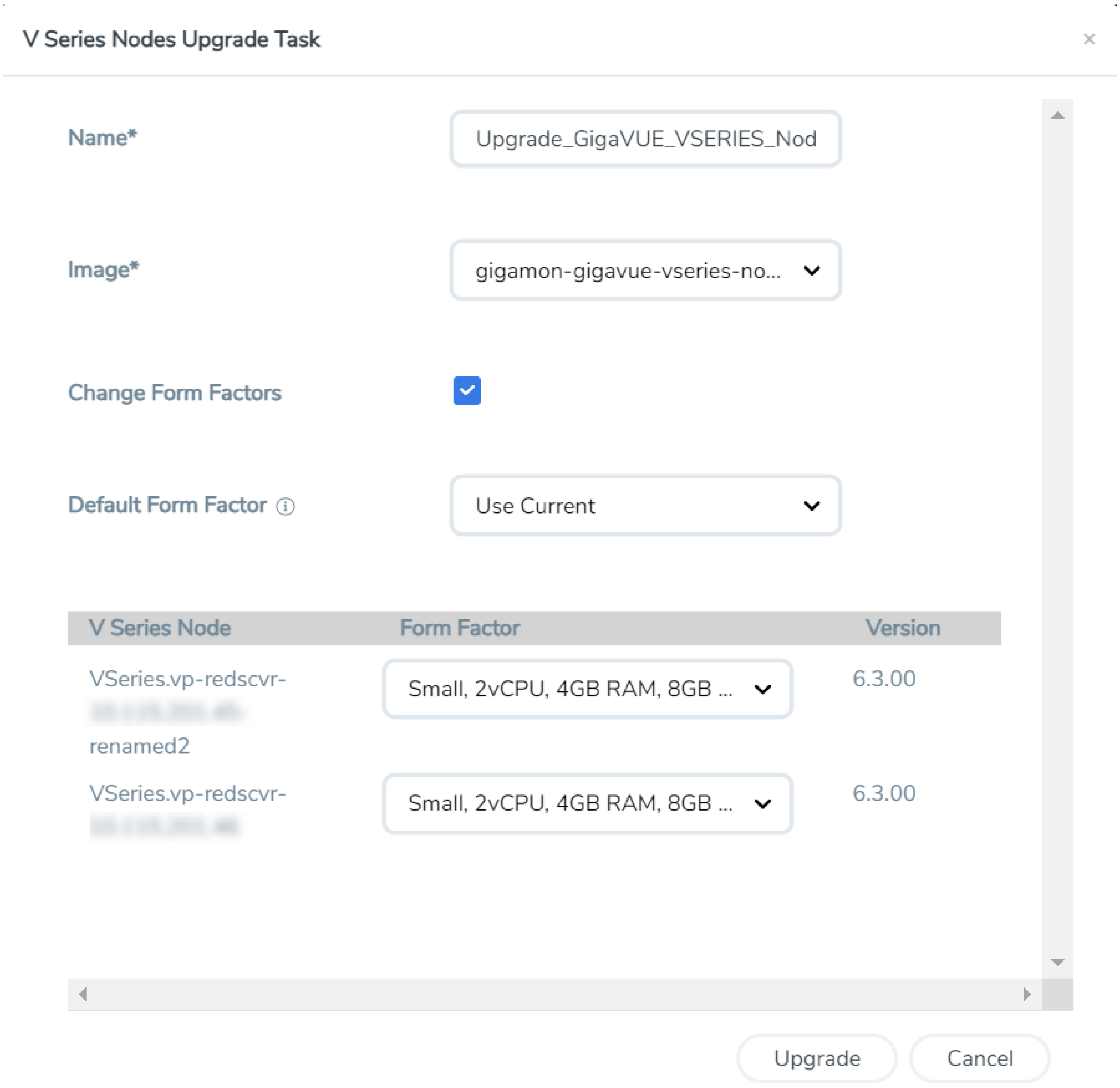
- You can select an entire monitoring domain and upgrade all the GigaVUE V Series Nodes in that particular monitoring domain, or you can select an individual GigaVUE V Series Node and upgrade it, or select multiple GigaVUE V Series Nodes in a monitoring domain and upgrade them.

- When upgrading GigaVUE V Series Nodes, if a host of a particular GigaVUE V Series Node is under maintenance mode, then the **Upgrade Fabric** button is disabled. Unselect the GigaVUE V Series Node whose host is under maintenance mode, and upgrade that GigaVUE V Series Node once the host is out of the maintenance mode.

> **NOTE:** GigaVUE-FM only supports (n-2) GigaVUE V Series Node version. Refer to GigaVUE-FM Version Compatibility Matrix in the *GigaVUE V Series Quick Start Guide* for detailed information on the supported versions.

To upgrade the GiagVUE V Series Node in GigaVUE-FM:

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



V Series Nodes Upgrade Task

Name*	Upgrade_GigaVUE_VSERIES_Nod
Image*	gigamon-gigavue-vseries-no...
Change Form Factors	☑
Default Form Factor	Use Current

V Series Node	Form Factor	Version
VSeries.vp-redscvr-[redacted]-renamed2	Small, 2vCPU, 4GB RAM, 8GB ...	6.3.00
VSeries.vp-redscvr-[redacted]	Small, 2vCPU, 4GB RAM, 8GB ...	6.3.00

3. Enter a name for the V Series Node upgrade task.
4. Select the latest GigaVUE V Series Node OVA image from the **Image** drop-down list.
5. If you want to modify the form factor (instance) size, click the **Change Form Factors** check box.

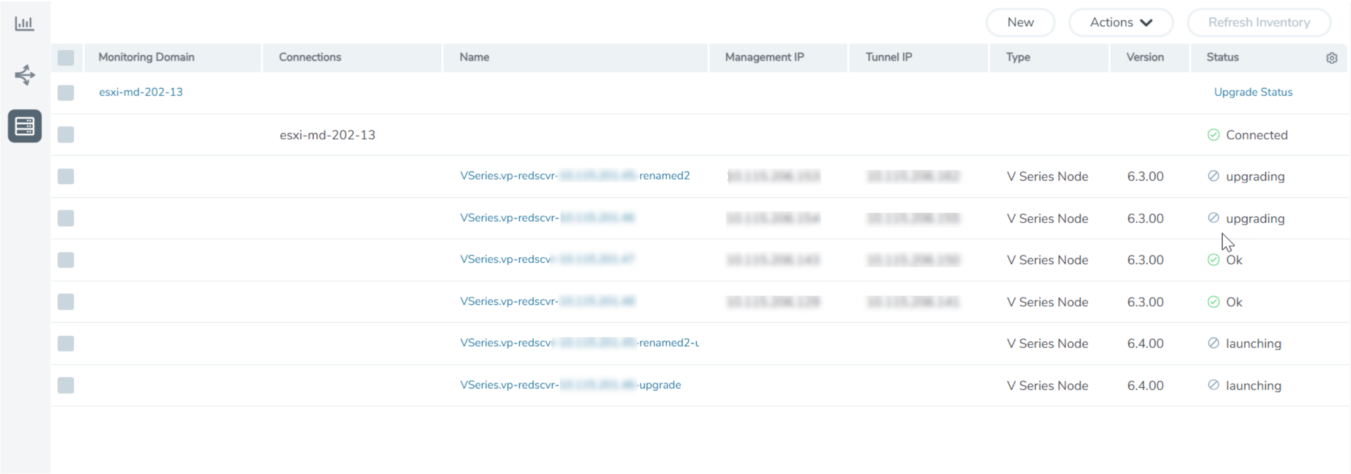
6. Select the form factor from the Default Form Factor drop-down menu to change the form factor of all the selected V Series Nodes. You can use the **Use Current** option to use the existing form factor of the individual GigaVUE V Series Node.
7. You can also change the form factor of a individual GigaVUE V Series Node from the **Form Factor** drop-down menu of the respective GigaVUE V Series Node. The form factor selected here overwrites the form factor selected in the **Default Form Factor**.

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

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

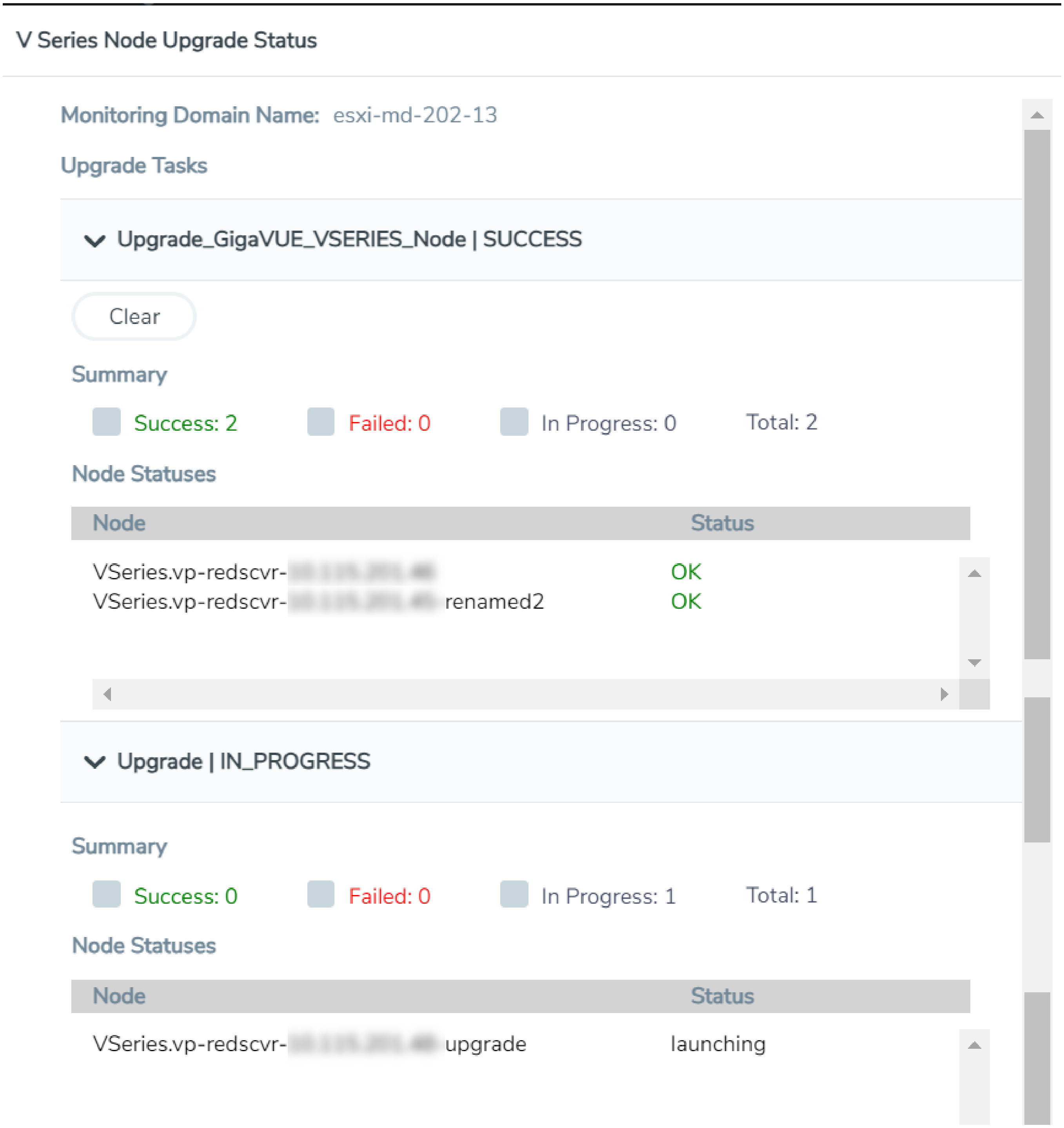
> **NOTE:** Both the new and the current V Series nodes appear in the same Monitoring Domain until the new nodes replaces the current and the status changes to **Ok**.

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



□	Monitoring Domain	Connections	Name	Management IP	Tunnel IP	Type	Version	Status
□	esxi-md-202-13							Upgrade Status
□		esxi-md-202-13						✓ Connected
□			VSeries.vp-redscvr-[redacted]-renamed2	[redacted]	[redacted]	V Series Node	6.3.00	⊘ upgrading
□			VSeries.vp-redscvr-[redacted]	[redacted]	[redacted]	V Series Node	6.3.00	⊘ upgrading
□			VSeries.vp-redscv[redacted]	[redacted]	[redacted]	V Series Node	6.3.00	✓ Ok
□			VSeries.vp-redscvr-[redacted]	[redacted]	[redacted]	V Series Node	6.3.00	✓ Ok
□			VSeries.vp-redscv[redacted]-renamed2-u			V Series Node	6.4.00	⊘ launching
□			VSeries.vp-redscvr-[redacted]-upgrade			V Series Node	6.4.00	⊘ launching

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



V Series Node Upgrade Status

Monitoring Domain Name: esxi-md-202-13

Upgrade Tasks

Upgrade_GigaVUE_VSERIES_Node | SUCCESS

Summary

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

Node Statuses

Node	Status
VSeries.vp-redscvr-[redacted]	OK
VSeries.vp-redscvr-[redacted]-renamed2	OK

Upgrade | IN_PROGRESS

Summary

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

Node Statuses

Node	Status
VSeries.vp-redscvr-[redacted]-upgrade	launching

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

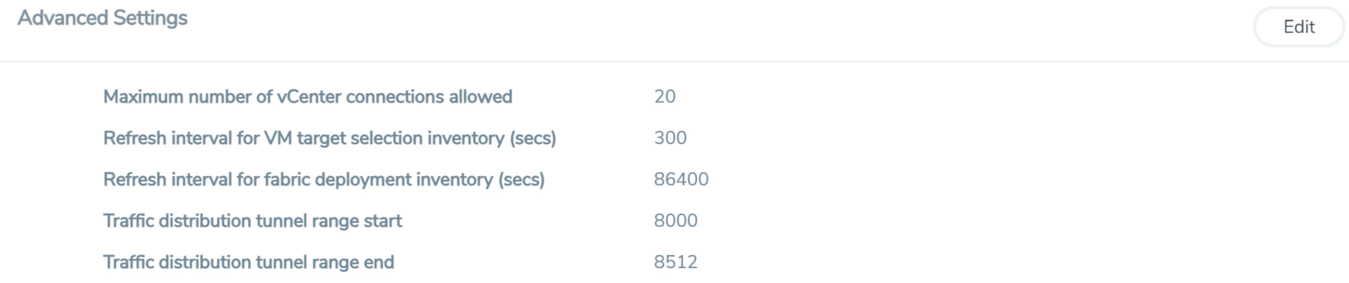
> **NOTE:** You cannot modify the node configurations when you are using **Retry** option. GigaVUE -FM uses the same values defined in the initial fabric upgrade configuration.

Configure 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 vCenter (V Series)**, and then click **Settings > Advanced Settings** to edit the VMware vCenter 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

Refer to the following table for details:

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

Configure Application Intelligence Solutions on GigaVUE V Series Nodes for VMware ESXi

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow. Refer the following topics for step by step instructions on how to configure Application Intelligence solution for GigaVUE V Series Nodes:

- Configure Environment
- Connect to VMware ESXi
- Create Source Selectors
- Create Tunnel Specifications
- User Defined Application
- Configure Application Intelligence Session
- Slicing and Masking in Application Filtering Intelligence
- Application Metadata Intelligence
- Create NetFlow Session for Virtual Environment

Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **GigaVUE V Series Proxy**) to scale and manage multiple GigaVUE V Series Nodes. Refer to the GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide for detailed information.
- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- To delete a GigaVUE V Series Node deployed in a Application Intelligence solution, you must delete the resources in the following order:
  1. Delete the Application Intelligence solution.
  2. Delete the GigaVUE V series Node and Connection.
  3. Delete the Environment.

Configure Environment

The Environments page allows you to create the following:

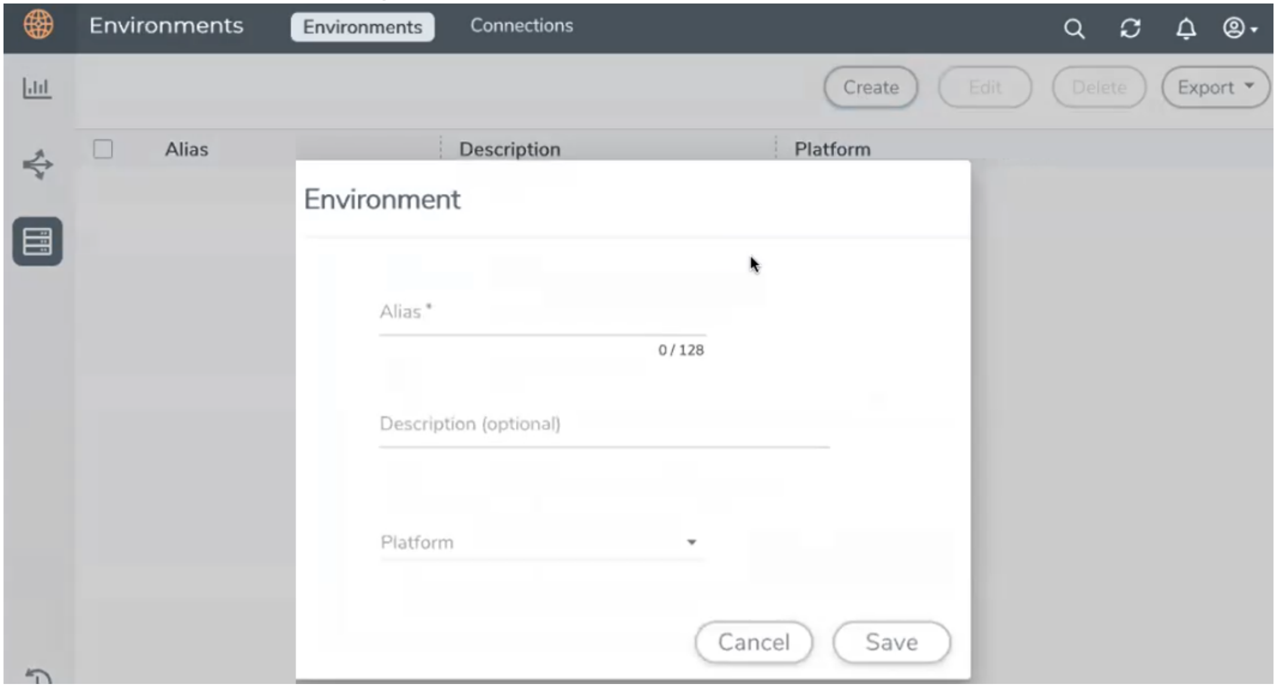
- **Environments**: The physical or the virtual environment in which the Application Intelligence solution is to be deployed.

- **Connections**: Connection between GigaVUE-FM and the cloud platform.

Create Environment

To configure the Environment:

1. Select **Inventory** > **Resources** > **Environments**.
2. On the **Environments** page, on the **Environments** tab, click **Create**.



3. Select or enter the following details:

Field	Description
Alias	Alias name used to identify the Environment.
Description	Brief description about the Environment.
Platform	Select the cloud platform.

4. Click **Save**. The environment is added to the list view.

Use the following buttons to manage your environment:

Button	Description
Delete	Use to delete an Environment.
Edit	Use to edit the details in an Environment.
Export	Export the details from the Environment page in an XLS or CSV file.

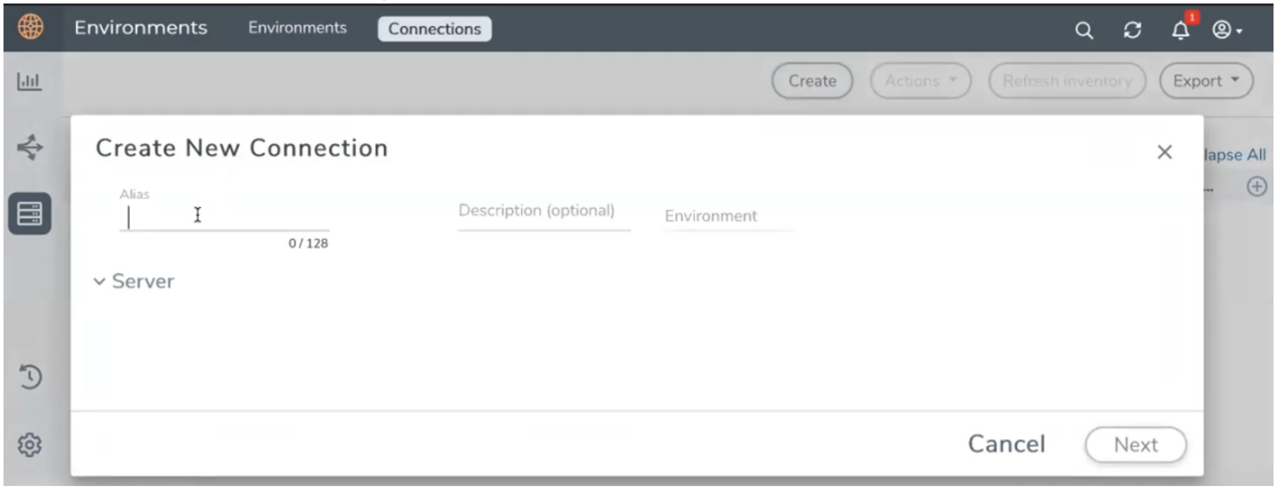
Connect to VMware ESXi

After creating a environment create a connection between the VMware ESXi and GigaVUE-FM. Refer to the following step given below for detailed information on how to create a new connection.

Create Connection

To create a new Connection:

1. Select **Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Connections** tab, click **Create**.



3. The **Create New Connection** dialog box opens. Enter the details as mentioned in the below section.

> **NOTE:** When creating a connection in the connections page, the corresponding monitoring domain created for internal use in GigaVUE-FM will not be displayed in the Monitoring Domain list page.

To establish a connection to the VMware ESXi, select or enter the following details:

Field	Description
Alias	Alias name used to identify the connection.
Description	Brief description about the connection.
Environment	Select the required environment. Refer to Connect to VMware ESXi
Server	The IP address of the virtual server.
vCenterUserName	Valid user name
vCenterPassword	Password for the user

After the connection is established, select or enter the following details in the fabric launch configuration page and click **Next**:

> **NOTE:** During V Series Node upgrade, the old node gets deleted and the new V Series Node is deployed. However, when the node upgrade fails due to deployment issues, the old node gets deleted and the new node is not deployed on the **Connection** page. This may led to loss of traffic. To avoid this you will have to redeploy the nodes again.

Field	Description
Datacenter	vCenter Data Center with the ESXi hosts to be provisioned with V Series nodes
Cluster	The Cluster on which the V Series nodes are to be deployed. From the drop-down list, select the required cluster or click **All** to select all the available clusters.
V Series Node Image	Web Server URL of the directory where V Series node ova files are available. **NOTE:** Before VMware Configuration, the V Series OVA files must be extracted as OVF files and placed in the same directory.
Form Factor	Instance size of the V Series node. Refer Prerequisites for Integrating V Series Nodes with ESXi for more information.
Hosts	Select the ESXi host for V Series deployment. Click **Select All** or **Select None** to select or unselect multiple hosts. **NOTE:** You can configure multiple hosts in a single connection (GigaVUE V Series Node). Select the Datastore and enter the required values. Click **Apply**.
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.

Field	Description
V Series Node Name	Name of the V Series Node
Datastore	Network datastore of the selected host
Management Network	Management network for V Series nodes

Field	Description
IP Type	IP type, can be IPv4 or IPv6.
Tunnel Network	Tunnel Network for the V Series nodes
IP Type	IP type of the tunnel, can be IPv4 or IPv6.
Tunnel Gateway IP	IP address of the Tunnel Gateway
Netmask Length	CIDR value of the Tunnel
User Password: (gigamon)	SSH Password of the V Series node
Form Factor	Instance size of the V Series node
IPv6	Use the toggle option to configure IPv6 tunnels. Provide the IPv6 prefix length value. The value must be greater than zero. **NOTE:** Ensure to enable this option before deploying the solution with IPv6 address as tool address.

Use the following buttons to manage your VMware ESXi connections :

Button	Description
Create	Use to create new connection.
Actions	Provides the following options: • **Edit Connection** - Use to edit a connection. • **Deploy Node** - Use to deploy a node. **NOTE:** You cannot add new V Series Nodes to a **Connection** which already has nodes. To add new V Series Nodes you will have to delete the existing V Series Node and the related Monitoring Session, and deploy all the V Series Nodes again. • **Delete Connection** - Use to delete a connection. • **Delete Node** - Use to delete a node. • **Force Delete** - This option is enabled when an upgrade fails due to infrastructure issues. Use this option to force delete the connection. • **Upgrade Fabric** - Use to upgrade fabric components. • **Continue Upgrade Fabric** - If the upgrade is failed or interrupted for any reason, use this option to continue the upgrade process.
Refresh Inventory	Use to refresh the selected connection.
Export	Use to export the details from the Connections page into an XLS or a CSV file.

To create Application Intelligence sessions, refer to Create an Application Intelligence Session in Virtual Environment.

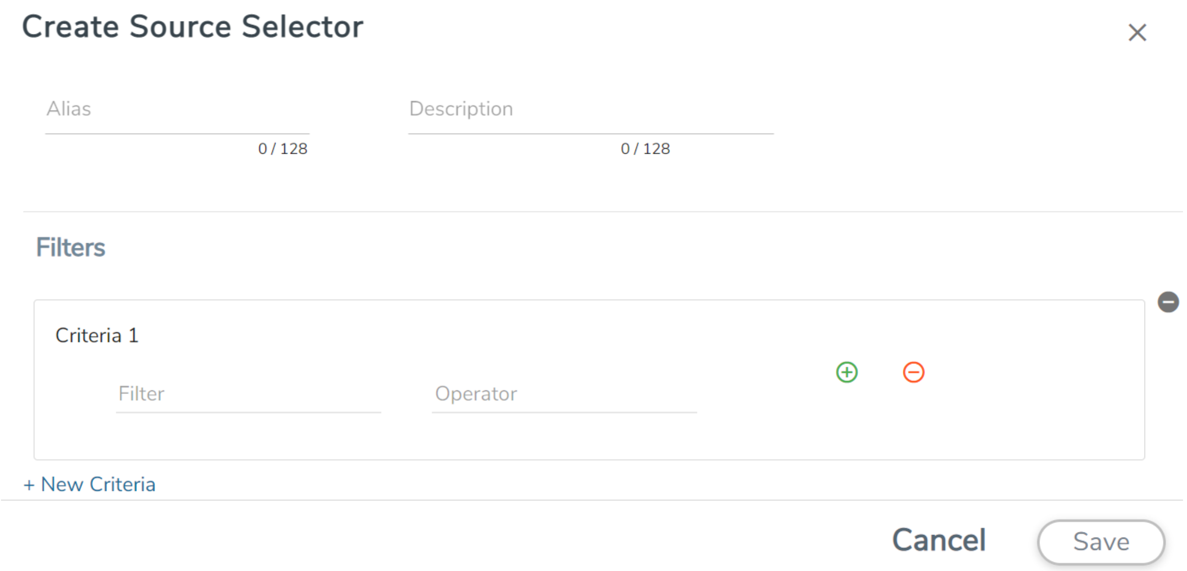
Create Source Selectors

When setting up a traffic flow, it is important to define the selection criteria for the source of traffic. Use the Source Selectors page for configuring the source of traffic to the GigaVUE V Series nodes.

> **NOTE:** When deploying the Application Intelligence using Source Selector, if the GigaVUE V Series Node is down, you will not be able to view the Selected Targets and UCT-Vs.

To configure the Source Selectors:

1. Select **Inventory** > **Resources> Source Selectors**.
2. On the **Source Selectors** page, on the **VM** tab, click **Create**. The **Create Source Selector** wizard appears.



Create Source Selector

Alias 0 / 128

Description 0 / 128

Filters

Criteria 1

Filter

Operator

3. Enter or select the required information:

Field	Description
Alias	Name of the source
Description	Description of the source
Filters	You can create a filter template from the Filters option
Criteria 1	Criteria to filter the traffic source. **NOTE:** You can create multiple criteria.
Filter	The criteria based on which the traffic is filtered. Select from the list of available filters. **NOTE:** Ensure that the registered traffic agents match the filter criteria.
Operator	Select the required operator based on the filter selected. Options are: • Starts with • Ends with • excludes • equals • between
Values	The values for the filter.

4. Click Save to save the source selector.

> **Note:** You can create multiple filter criteria. Within each criterion, you can configure multiple filters.

- If you have configured multiple filters in a criterion, then the traffic will be filtered only if all the filter rules are true.
- If you have configured multiple criteria, then the traffic will be filtered even if one of the criteria is true.
- A maximum of 25 inclusion rulesets and 25 exclusion rulesets can be added.

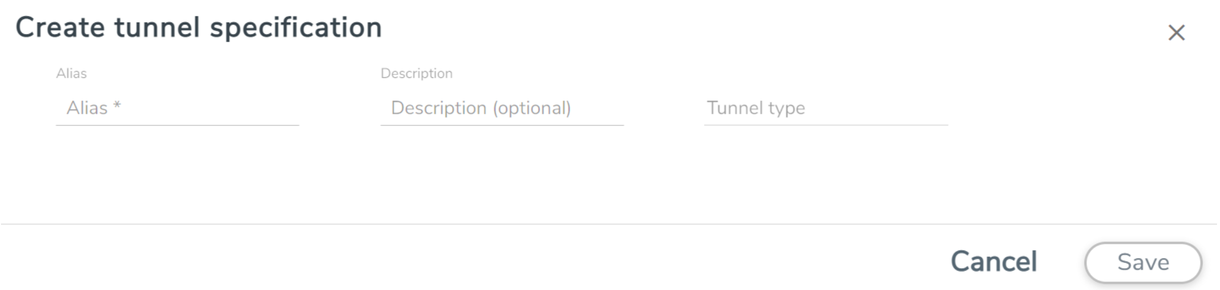
Create Tunnel Specifications

A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel. The tunnel can be an ingress tunnel or an egress tunnel.

NOTE: VXLAN is the only supported tunnel type for Azure.

To configure the tunnels:

1. Select **Inventory** > **Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **VM** tab and click **Create**. The Create Tunnel Specification wizard appears.



Create tunnel specification

Alias: Alias *

Description: Description (optional)

Tunnel type

3. Enter or select the following information:

Field	Description
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Tunnel Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN to create a tunnel. Do not select UDPGRE tunnel type. **NOTE:** VXLAN is the only supported tunnel type for Azure.
Traffic Direction	The direction of the traffic flowing through the V Series node. • Choose **In** (Decapsulation) for creating an Ingress tunnel, Tunnel Spec for the Source should always have the Traffic Direction as IN, signifying an ingress tunnel. Enter values for the Key. • Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key. • ERSPAN, L2GRE, and VXLAN are the supported **Ingress tunnel** types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session. • L2GRE and VXLAN are the supported **Egress tunnel** types. • For Azure connection, VXLAN is the supported Ingress and Egress tunnel type.
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.

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

User Defined Application

This feature gives you the ability to classify the applications by the DPI engine. This allows unclassified TCP, UDP, HTTP, and HTTPS applications to be identified and named with the help of user defined application signatures.

To configure User Defined Application signatures :

Step Number	Task	Refer the following
1	Create rules under User Defined Application Section	Create rules under User Defined Application
2	Configure Application Intelligence Session	For Physical: Application Intelligence Session For Virtual: Configure Application Intelligence Session
3	Monitor User Defined Application	View the Application Intelligence Dashboard

Create Rules under User Defined Application

1. Click **Inventory**.

2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.

3. Click **New** in the **User Defined Applications** screen to create a new rule.

4. Enter **Application Name**.

5. Enter **Priority**. The value must be between 1 and 120.

Note: The least value will have the highest priority.

6. In the created rule:

   a. Choose the **Protocol** from the list of protocols.

   b. Choose the **Attributes** from the list of attributes.

   c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.

8. Click the application listed under the **Applications** column.

9. Click the **Rule** tab.

10. Select a rule to view its protocol details.

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regex patterns, refer Supported RegExp Syntax

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file|new_slice|upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-	Referer	Source	Client	REGEXP	http:\/\/gigamon.com\/

	referer	URI	address where client got the URI	to Server Only		
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\/football\/.*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
ssl	common_name	Domain Name	Domain name from Client Hello message or the certificate		REGEXP	(.*\.)?gigamon\.com
	stc-	Subjec	List of	Server	REGEXP	(.*\.)?gigamon\.com

	subject_alt_name	t Alt Name (s)	host names which belong to the same certificate	to Client Only		
rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http:\/\/www.music.tv\/recorded\/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a packet, excluding the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata
	port	Server Port	Server (listen)		UINT16 RANGE	80-4350

			port number		as REGEXP String	
sip	user_agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Message Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Message Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Address	IP address of the server		IPV4 as REGEXP String	62.132.12.30\/24
	dscp	DSCP Value	DSCP from Differentia ted Service (DS) Field in IP header		UINT8 as REGEXP String	33

	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentia ted Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
( )	Groups a series of expressions together

[ ]	Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
| [<start>-<end>]	Separates values contained in ( ). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog | cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_ number>	Matches for a direct binary with octal input
\x<hexadecimal-number>\x	Matches for a direct binary with hexadecimal input
\[<character-set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Configure Application Intelligence Session

Application Intelligence provides a comprehensive solution that:

- identifies the applications contributing to the network traffic.
- isolates preferred application-specific traffic and directs it to the appropriate tools.
- exports relevant application metadata for further analytics and analysis.

Application Intelligence provides the following capabilities for both physical devices and virtual nodes:

- **Application Visualization (earlier known as Application Monitoring)** - Identifies and monitors all applications contributing to the network traffic, and reports on the total applications and the total bandwidth they consume over a select period. Able to identify more than 3,200 applications. It displays the traffic statistics in bytes, packet and flows.

- **Application Filtering Intelligence**- Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.
- **Application Metadata Intelligence** - Supports exporting over 5000 attributes of metadata that provide relevant usage context on over 3,200 applications, thus enabling you to rapidly identify indicators of compromise (IoC) for security analytics and forensics tools.

Prerequisites

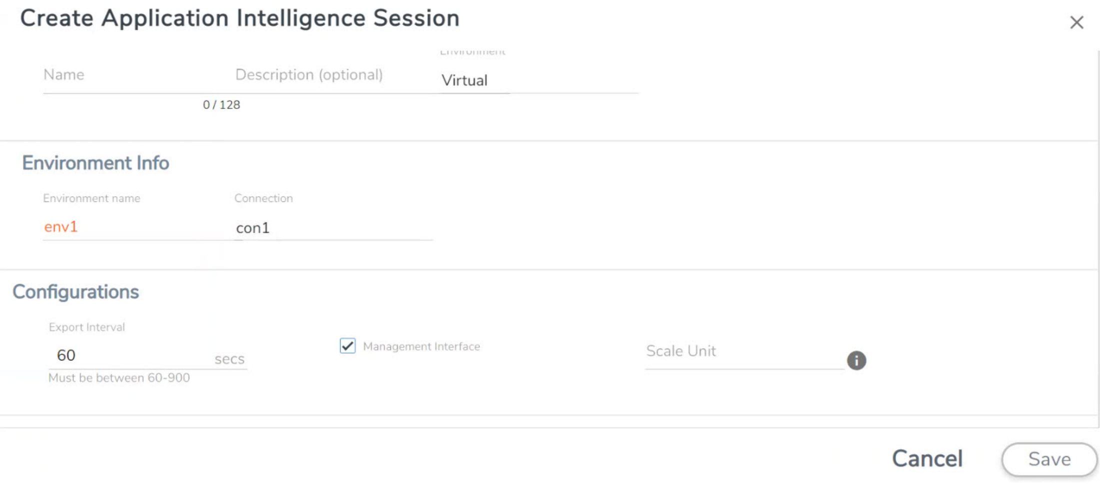
- The environment on which the Application Intelligence solution is to be deployed must already be created and the nodes must be deployed on it.
- In virtual environment, the destination tunnels for the Application Filtering Intelligence Map must already be created.

> **NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

To create an Application Intelligence Session:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create New**. The **Create Application Intelligence Session** page appears.



Create Application Intelligence Session

Name:

Description (optional): 0 / 128

Environment: Virtual

Environment Info

Environment name: env1

Connection: con1

Configurations

Export Interval: 60 secs (Must be between 60-900)

☑ Management Interface

Scale Unit:

3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created:
   - Virtual- connects to the specific environment.
4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides..

5. In the **Configurations** section, complete the following:
    a. Select an **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization. The valid range is 60–900 seconds.
    b. Select the required interface. By default, **Management Interface** is enabled. To export the data through tunnel interface, uncheck the Management Interface check box.
    c. Enter a value for the **Scale Unit**. The scale unit represents the number of flows supported by the application. If the scale unit value is 1, the maximum active flow limit will be 100k.
    Refer to the following table for the maximum scale unit supported for VMware, AWS, and Azure platforms.

Cloud Platform	Instance Size	Maximum Scale Unit without using Secure Tunnels	Maximum Scale Unit when using Secure Tunnels
VMware	Large (8 vCPU and 16 GB RAM)	3	2
AWS	Large (c5n.2xlarge)	3	3
Azure	Large (Standard_D8s_V4)	5	5

> **NOTE:** If the Application Intelligence Session deployment fails, due to using a scale unit other than the recommended scale unit, then reload the GigaVUE V Series Node.

6. In the **Source Traffic** section, select anyone of the following:

- **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to Create Source Selectors.
    - **Prefilter** - Enable the mirroring option, select the prefilter checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.
    - **Precryption**: Select the Precryption checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.

> **NOTE:** You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using the Third Party Orchestration in VMware ESXi host.

- **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to Create Tunnel Specifications.

> **NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration.

- **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will trap the traffic for application monitoring.

> **NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

> - Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel.
> - For Azure Connection, VXLAN is the only supported Tunnel Type.

7. Click **Save**. The session created is added in the list view.
8. In the **User Defined Applications** section, select the template from the list.For information on **Supported protocols and Attributes** and **Limitations** refer **User Defined Application** topic.

The total applications participating in the network traffic are displayed in the Application Intelligence Dashboard. For more information about the dashboard, refer to the View the Application Intelligence Dashboard.

Select the session from the Application Intelligence Sessions pane and click on the ⋮ icon and select **View Details** from the drop-down menu, to view the deployed UCT-V, their status and more information about source selectors, selected target.

If the session configuration is unsuccessful, troubleshoot the error notified (refer to View the Health Status of a Solution). Click the **Reapply all pending solutions** button ⟲ in the dashboard to redeploy the configuration.

> **NOTE:** GigaVUE-FM takes few minutes to display the application statistics.

> **NOTE:** The option **Reapply all pending solutions** is applicable for physical solution only.

When the Application Intelligence solution is in suspended state, you cannot delete the session. You can click on the ⋮ icon and select **View Details** from the drop-down menu, to view the details.

You can also filter the traffic based on the applications. For more information, see Create Application Filtering Intelligence.

Slicing and Masking in Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. With the addition of slicing and masking parameters to the existing application filtering functionality, you will be able to slice, mask, or slice and mask the filtered packets before sending them to the destination tunnel endpoint.

For step-by-step instructions on how to configure Application Filtering Intelligence refer to Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard topic from *GigaVUE Fabric Management Guide*.

Configuring Application Filtering Intelligence with Slicing

You can enable the slicing configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be sliced.

The filtered traffic will be sliced before forwarding it to the destination tunnel endpoint.

Refer to Slicing section in the *GigaVUE V Series Applications Guide* for more detailed information on Slicing.

Configuring Application Filtering Intelligence with Masking

You can enable the masking configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be masked.
3. In the Pattern field, enter the pattern for masking the packet.
4. In the Length field, enter the length of the packet that must be masked.

The filtered traffic will be masked before forwarding it to the destination tunnel endpoint.

Refer to Masking section in the *GigaVUE V Series Applications Guide* for more detailed information on Masking.

Configuring Application Filtering Intelligence with Slicing and Masking

You can enable both slicing and masking configurations, and provide inputs for each **Application Filtering** rule set.

The filtered traffic will be sent to the slicing application, the sliced traffic will be sent to masking application and then to the destination tunnel Endpoint.

NOTE: When combining slicing and masking operations, the offset range of the masking must be lesser than the offset value entered for the slicing operation, as the slicing operation is performed first.

Application Metadata Intelligence

Application Metadata Intelligence generates more than 5000 attributes for more than 3200 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

Application Metadata Intelligence (AMI) is enabled to multi-collect protocols with more than one metadata attribute of the same type. The multi-collect feature supports additional protocols such as DNS, GTP,GTPV2, DHCP, HTTP, HTTPS, SSL, HTTP_PROXY, HTTP2, KERBEROS5, and DHCP6.

The generated metadata is exported in IPFIX (IP Flow Information Export) format and CEF (Common Even Format) to security analytics and forensics tools thereby providing greater visibility to enforce corporate compliance.

The output from the Application Metadata Intelligence in CEF format can also be converted to JSON format using Application Metadata Exporter (AMX) application. To learn more about AMX application refer to Application Intelligence—Application Metadata Exporter

Application Metadata Intelligence generates metadata only if the application is allowed to be passed in Application Filtering Intelligence. For example, Application Metadata Intelligence has the capability to generate metadata for HTTP traffic only if Application Filtering Intelligence filters in the HTTP traffic.

Refer to Create Application Metadata Intelligence Session for Virtual Environment topic for step-by-step instructions on how to configure Application Metadata Intelligence on Virtual Environment.

Create Application Metadata Intelligence Session for Virtual Environment

You can create an Application Metadata Intelligence session for virtual environment.

To create an Application Metadata Intelligence session, follow these steps:

1. Go to **Traffic > Solutions > Application Intelligence**.
2. From the Sessions pane, click ⋮ and select **Edit**. The **Edit Application Intelligence Session** window appears.

3. In the **Edit Application Intelligence Session** window, click **Application Metadata**.

   > **NOTE:** If Application Filtering Intelligence License is available, you must create Application Filtering to create Application Metadata Intelligence. For more information, refer to Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard

4. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can also create multiple exporters.
   a. Enter the following details:

Field	Description
Tool Name	Enter the tool Name
Tool IP Address	Enter the tool IP address
Template	Select the tool template. Refer to Tool Templates for more details on what are tool templates and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow or CEF
NetFlow: Select this option to use Netflow	
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
CEF: Select this option to use CEF	
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.

   b. Click **App Editor**, to select the applications and its attributes. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFLow V5 Template in the above **Template** drop-down menu.) The Application Editor screen appears as shown:

   c. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. You can also select **Add All Applications in Family** or **Delete All Applications in Family**. The selected applications and their families appear in the **Selected Applications** section.

   > **NOTE:** You can select the required applications without selecting the application family.

5. In the **Advanced Settings** > **Collects** section, you can select the following packet attributes:
   - Counter - Select the Bytes, and Packets.
   - IPv4 - Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
   - IPv6 - Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
   - Transport -Select the required attributes. By default, Source Port, Destination Port are enabled.

   a. By default, the above collect types are displayed. Click ⊕ to add the following collect types:
      - Data Link - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
      - Timestamp - Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
      - Flow - Select the parameter as End Reason if required.
      - Interface - Select any one of the parameter such as Input Physical, Output Physical and Input Name.

6. In the **Application Metadata Settings** section:
   a. Select the Flow Behavior as any one of the following:
      - Uni-Directional
      - Bi-Directional. The default value is Bi-Directional.

   b. Enter the Timeout and Cache Size.

   c. You can enable or disable the **Multi-Collect** option to perform the following:
      - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
      - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.

   d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

> **NOTE:** You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

   e. You can enable or disable the **Advance Hash** option to perform the following:
      - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
      - **Disable** — Disables the metadata cache advance-hash for flows.

   f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.

   g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.

7. Click **Save**.

The metrics of the Application Metadata traffic appear on the dashboard.

Create NetFlow Session for Virtual Environment

Note: This configuration is applicable only when using NetVUE Base Bundle.

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

To create an NetFlow session, follow these steps:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create** . The **Create Application Intelligence Session** page appears.
3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created.
4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides.
5. In the **Configurations** section, complete the following:
   a. The **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization is 5 seconds
   b. By default, **Management Interface** is enabled.

6. In the **Source Traffic** section, select anyone of the following:
   a. **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to Create Source Selectors

      > **NOTE:** You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using Third Party Orchestration in VMware ESXi Host

   b. **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to Create Tunnel Specifications.

      > **NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration. Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel. For Azure Connection, VXLAN is the only supported Tunnel Type.

   c. **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will tap the traffic for application monitoring.

      > **NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

7. Click on the **Application Metadata** tab.

8. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can only create a maximum of 5 exporters. Enter the following details:

Field	Description
Tool Name	Enter the tool name.
Tool IP Address	Enter the tool IP address.
Template	Select the tool template. Refer to Tool Templates for more details on what tool templates are and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	NetFlow
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds.

9. In the **Advanced Settings** > **Collects** section, the following details are already configured.

> **NOTE:** When the template is NetFlow v5 or when the format is NetFlow and the version as V5 you cannot modify the **Collects**.

- TimeStamp
- Counter
- Interface
- IPv4
- Transport

10. In the **Application Metadata Settings** section:
    a. Select the Flow Behavior as any one of the following:
       - Uni-Directional
       - Bi-Directional. The default value is Bi-Directional.

    b. Enter the Timeout and Cache Size.

    c. You can enable or disable the **Multi-Collect** option to perform the following:
       - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
       - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.

    d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

> **NOTE:** You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

e. You can enable or disable the **Advance Hash** option to perform the following:
   - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
   - **Disable** — Disables the metadata cache advance-hash for flows.

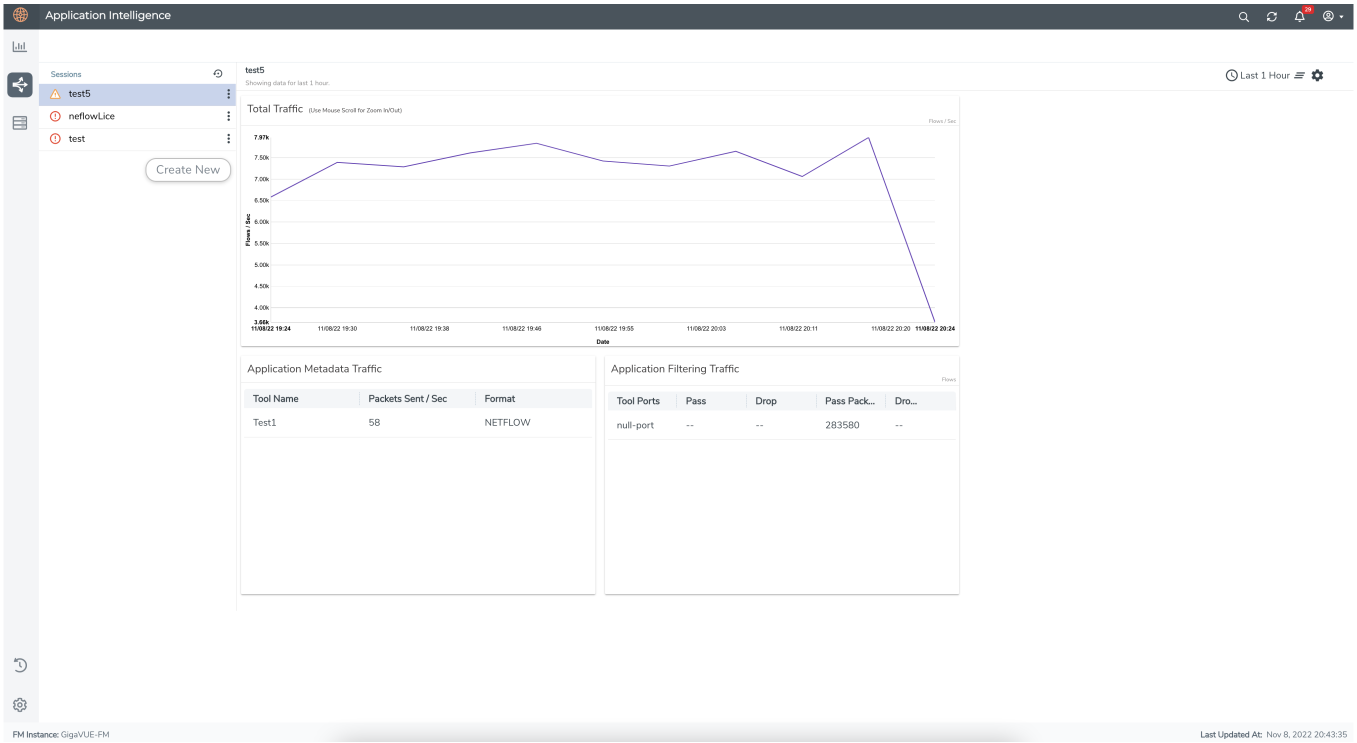
f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.

g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.

11. Click **Save**.

NetFlow Dashboard

In Appviz, only the traffic statistics are displayed as applications cannot be configured and used in the NetFlow configuration



Tool Name	Packets Sent / Sec	Format
Test1	58	NETFLOW

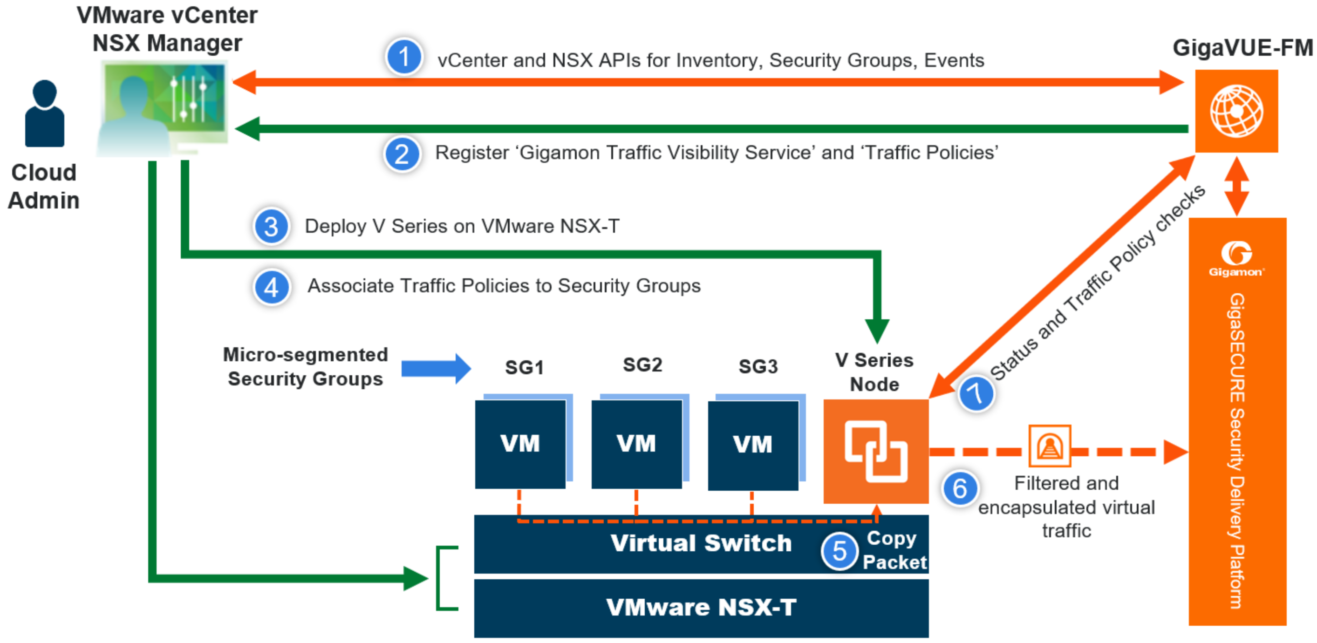
Tool Ports	Pass	Drop	Pass Pack...	Dro...
null-port	--	--	283580	--

Configure GigaVUE V Series Node on VMware NSX-T

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

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

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


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

> **NOTE:** If a V Series Node is restarted, then the existing flows that is received by that V Series node will not be forwarded to the other available V Series Nodes (if any). However, the new flows will be forwarded to any available V Series Node.

The chapter includes the following major sections:

- Prerequisites for Integrating V Series Nodes with NSX-T
- Integrate GigaVUE V Series Nodes with VMware NSX-T

- Configure Application Intelligence Solutions on GigaVUE V Series Nodes for VMware NSX-T
- Remove Gigamon Service from NSX-T and GigaVUE-FM

NOTE: These steps assume that VMware NSX-T is installed and configured. Refer to VMware Documentation for configuration details.

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 V Series node host-based deployment will be unsuccessful.

Refer to the following Gigamon Validated Designs for more detailed information:

- Deploying GigaVUE Cloud Suite for VMware NSX-T 3.1.2 using V Series
- Deploying GigaVUE Cloud Suite for VMware NSX-T using V Series
- Deploying GigaVUE Cloud Suite for VMware NSX-T 3.0 using V Series
- Deploying GigaVUE Cloud Suite for VMware NSX-T 2.5.1 using V Series

Prerequisites for Integrating 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.
- 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 Recommended Form Factor (Instance Types) 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.
- GigaVUE-VM and GigaVUE V Series Node visibility solutions cannot be deployed on the same NSX-T manager.
- 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 vCenter Privileges
- Required Roles 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	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter, NSX-T and all ESXi hosts.
	NSX-T Manager					
	vCenter					
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM

						to communicate with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to communicate 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/ 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/ 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-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						
ESXi host						
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						
ESXi host						

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 vCenter Privileges

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

The following table lists the minimum required permissions for GigaVUE-FM to manage the vCenter user.

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.

GigaVUE-FM Deployment

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

NSX-T Deployment

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

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!

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 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 Monitoring Domain	Create Monitoring Domain for VMware NSX-T
4	Create a service segment in NSX-T	Create a Service Segment in 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
7	Create a Ingress and Egress Tunnels to tunnel traffic	Create Ingress and Egress Tunnel
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 NSX-T Group and Service Chain

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 Monitoring Domain	Create Monitoring Domain for VMware NSX-T
4	Create a service segment in NSX-T	Create a Service Segment in 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
7	Create a Ingress and Egress Tunnels to tunnel traffic	Create Ingress and Egress Tunnel
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 NSX-T Group and Service Chain

Integrate GigaVUE V Series Nodes with 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
- Upload GigaVUE V Series Node Image into GigaVUE-FM
- Create Monitoring Domain for VMware NSX-T
- Create a Service Segment in VMware NSX-T
- Configure GigaVUE V Series Nodes for VMware NSX-T
- Configure Monitoring Session
- Create NSX-T Group and Service Chain
- Upgrade GigaVUE V Series Nodes for VMware NSX-T
- Configure VMware Settings

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. For NSX-T and GigaVUE Cloud Suite FM to communicate, users with the proper permissions must be created in both GigaVUE-FM and VMware NSX-T. Refer to Required VMware vCenter Privileges and Required Roles in VMware NSX-T for more information on user roles and privileges.

> **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.

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** and then from the drop-down list,
   - for **NSX-T version 3.2.x**, select LDAP with the following Role combination:
     - NETX Partner Admin and Security Admin
   - for **NSX-T version 3.1.x**, select LDAP with one of the following Role combinations:
     - NETX Partner Admin and Security Operator
     - NETX Partner Admin and Network Operator

   > **NOTE:** When you deploy V Series Nodes using VMware NSX-T manager, you can select NETX Partner Admin alone as Role instead of these combinations.
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.

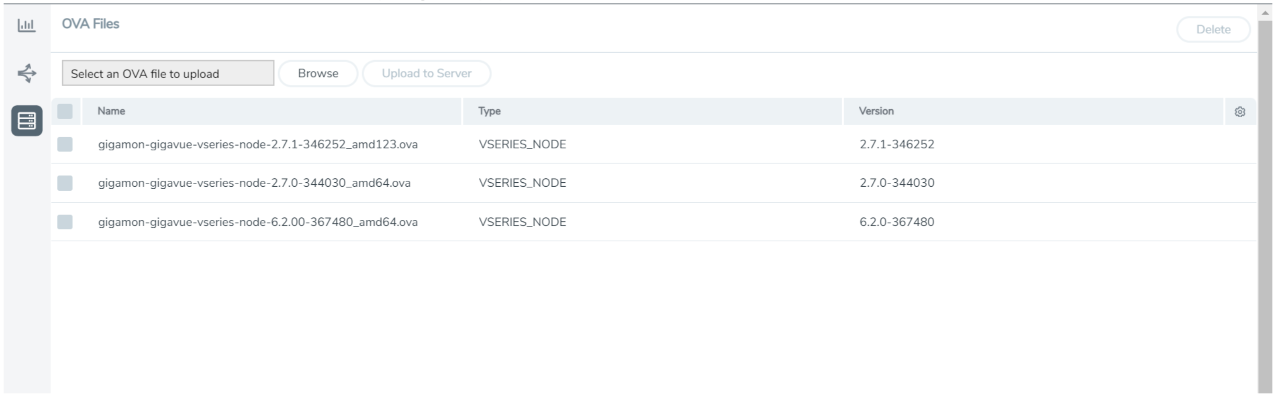
The username and password created for vCenter, NSX-T Manager, and GigaVUE-FM in this section will be used when creating Monitoring Domain in GigaVUE-FM. Refer to Create Monitoring Domain for VMware NSX-T section for step-by-step instructions on how to create monitoring domain.

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 is three.

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**.

NOTE: Due to certificate validation requirement in NSX-T manager nodes, V Series node deployment may fail. Before deploying the V Series nodes, disable the certificate validation as follows.

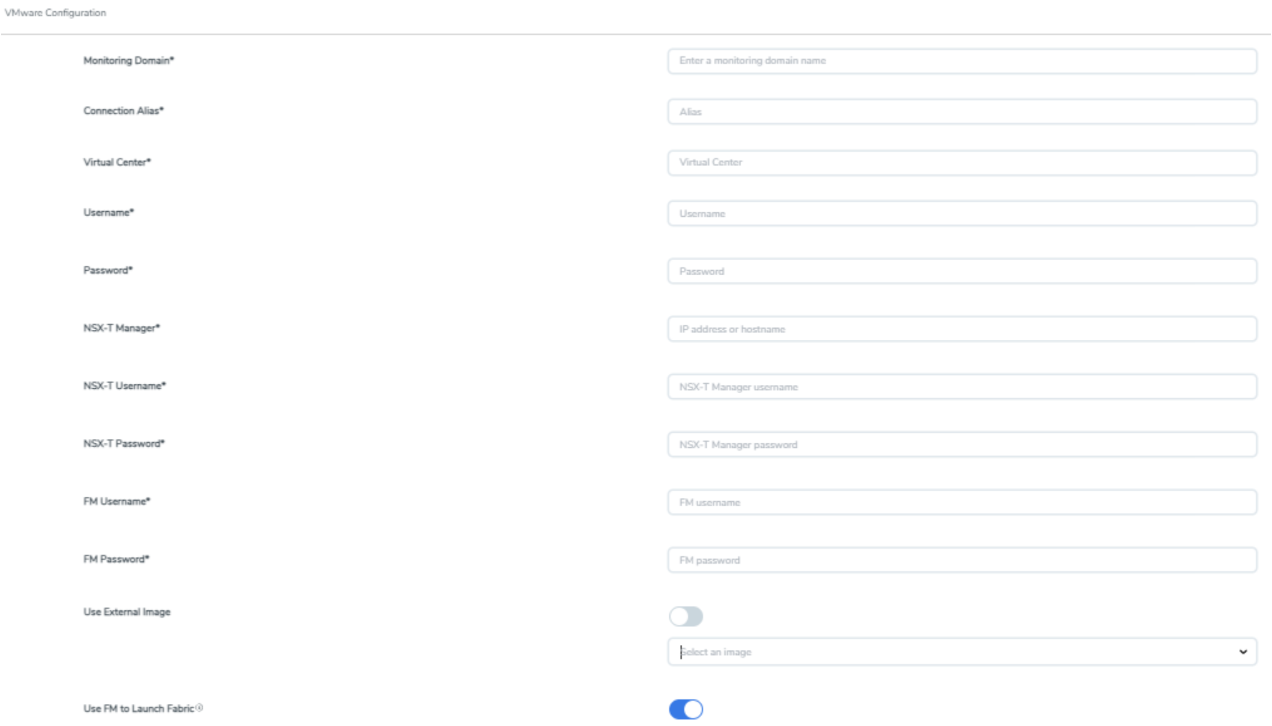
1. Login to each NSX-T manager using CLI with root credentials.
2. Open **/config/vmware/auth/ovf_validation.properties** file
3. Set a value for **THIRD_PARTY_OVFS_VALIDATION_FLAG** as **2**. The definition of the legends are as follows:
   - 0: only VMware-signed OVFs are allowed for deployment
  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

Create Monitoring Domain for VMware NSX-T

This chapter describes how to create a monitoring domain for deploying V Series nodes in VMware NSX-T environment through GigaVUE-FM. You must establish a connection between GigaVUE-FM and your vCenter environment before you can perform the configuration steps for V Series node.

To configure VMware vCenter in GigaVUE-FM:

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 of the vCenter
Username	Username of the vCenter user with admin role privilege
Password	vCenter password 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. • The NSX-T user account must have admin privileges. • Each NSX-T manager can support a maximum of one monitoring domain.
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 image or internal image. If you wish to use the **Use External Image** option, you use an external server to place all the OVA files and provide the URL of the web server. Else you can upload the OVA files to GigaVUE-FM and use it as an internal image server. a. **Yes** to use an external image. To use an external image, enter the web server URL of the directory where V Series node OVA, VMDK, and OVF files are available. The Web Server URL must be in the following format: *http://<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. **NOTE:** When using an external image, before VMware Configuration ensure all the contents of the OVA file are extracted and placed in the directory which represents the Image URL. b. **No** to use an internal image. To use an internal image, select the uploaded OVA files from the **Select an image** drop-down menu. **NOTE:** When using an internal image, before VMware Configuration save the OVA files to the dedicated directory.
Use FM to Launch Fabric	Enable this toggle button if you wish to deploy GigaVUE V Series Nodes using GigaVUE-FM.

4. Click **Save** and you are navigated to the **VMware NSX-T Fabric Deployment** page.

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

NOTE: When editing a Monitoring domain that has nodes deployed, then the **Use External Image** toggle button is disabled. However, for a monitoring domain which does not have any nodes deployed the **Use External Image** toggle button is enabled.

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 on VMware NSX-T in two ways. You can either directly use VMware NSX-T manager to deploy your V Series nodes or use GigaVUE-FM to deploy your V Series nodes.

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

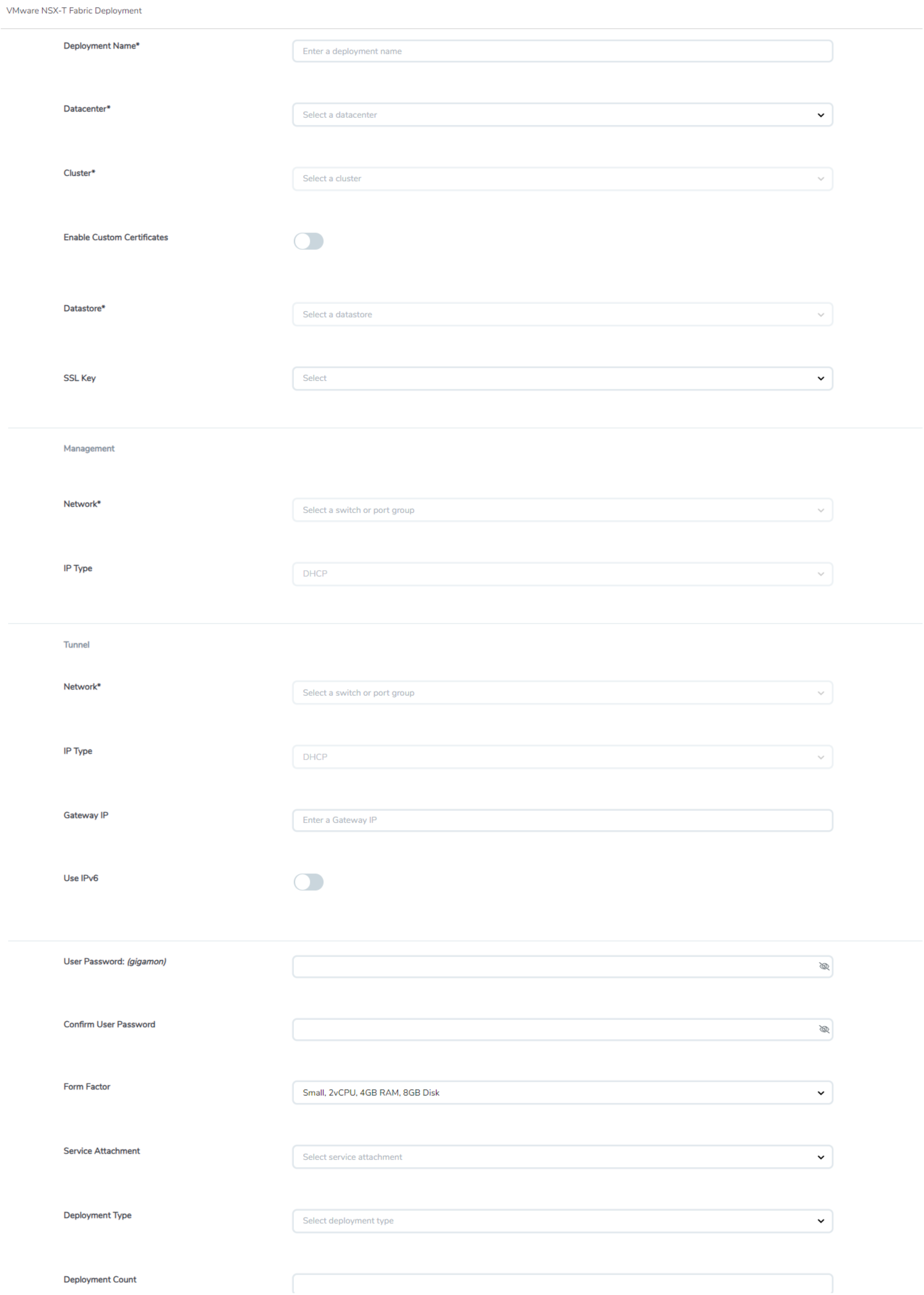
After establishing a connection between GigaVUE-FM and VMware NSX-T, GigaVUE-FM launches the configuration for the GigaVUE V Series Node.

Refer to the following sections for details:

- Deploy GigaVUE V Series Node from GigaVUE-FM
- Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM

Deploy GigaVUE V Series Node from GigaVUE-FM

1. In the **VMware NSX-T Fabric Deployment** page, enter or select the following details.



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

Management

Network*	Select a switch or port group
IP Type	DHCP

Tunnel

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

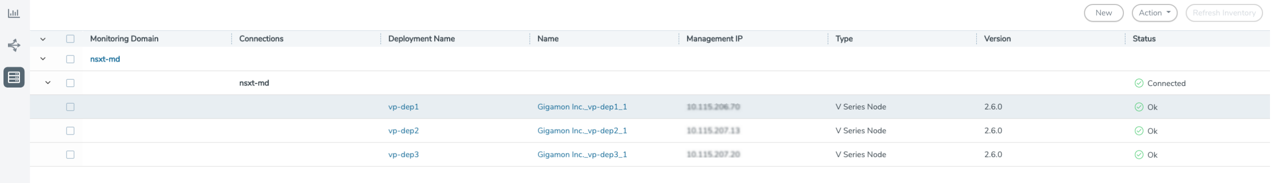
User Password: *(gigamon)*	
Confirm User Password	
Form Factor	Small, 2vCPU, 4GB RAM, 8GB Disk
Service Attachment	Select service attachment
Deployment Type	Select deployment type
Deployment Count	

2.

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	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.
Datastore	Network datastore shared among all NSX-T hosts.
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 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 **NOTE:** This field appears only when the Tunnel **IP type** is Static.	Select the IP Pool
MTU	The Maximum Transmission Unit (MTU) is the maximum size of

Field	Description
	each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000.
User Password: (gigamon)	SSH Password for the built-in user, '**gigamon**' on the V Series node
Confirm Password	Confirm the SSH Password of the V Series node
Form Factor	Instance size of the V Series node. (eg: Small, Medium or Large)
Service Attachment	Service segment created on NSX-T
Deployment Type	Type of 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 Increase or Decrease 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

3. Click **Deploy**. After the 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 node, click on a GigaVUE V Series Node, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

> **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.

Increase or Decrease 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.

You can add more nodes or remove nodes from an existing monitoring domain using GigaVUE-FM.

Add V Series Nodes to Existing Monitoring Domain

To increase the number of 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 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 Deploy GigaVUE V Series Node from 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 V Series Nodes you wish to add in the **Deployment Count** column.
5. Click Deploy.

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

Decrease 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 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 V Series Nodes under that deployment will be deleted.

    The number of 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 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 V Series node to the existing monitoring domain instead of undeploying and redeploying the monitoring domain every time you wish to add more V Series nodes to the monitoring domain.

Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

You can deploy your 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 sessions and related services in GigaVUE-FM.

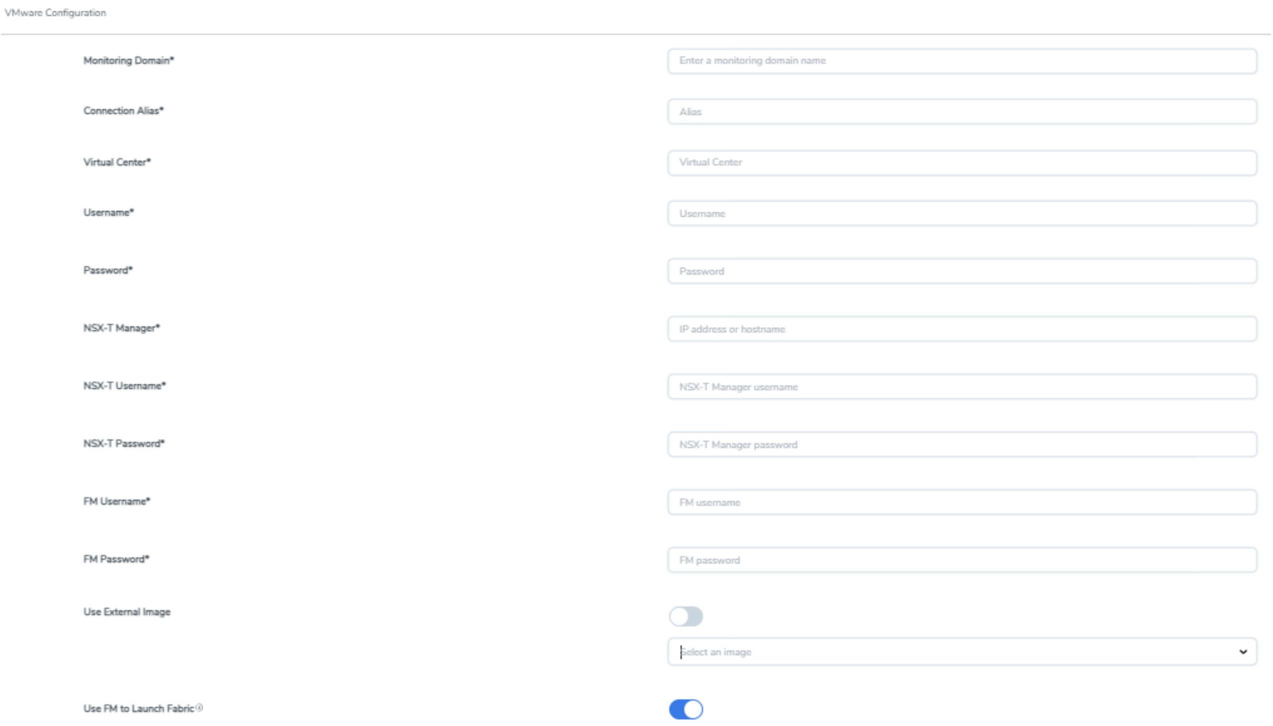
Refer to the following sections for details:

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

Getting Started

To register your 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 V Series Nodes using VMware NSX-T manager.



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

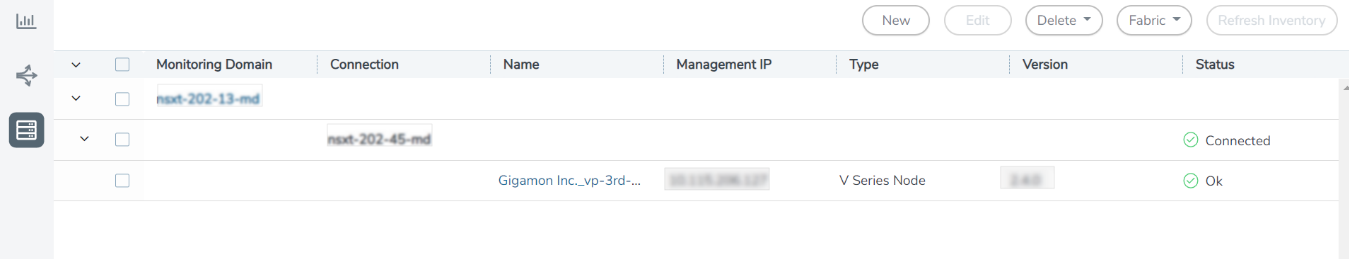
3. After creating your monitoring domain, you can use VMware NSX-T manager to deploy your nodes.

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 GigaVUE Cloud Suite from the **Partner Service** drop-down. 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 Install Custom Certificate topic for more detailed information on Custom Certificates.

4. Once the 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 V Series Nodes are of same version. GigaVUE-FM does not support V Series Nodes with different version in the Monitoring Domain.

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 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 VMware NSX-T Manager

You can now add more nodes or remove nodes from an existing monitoring domain using VMware NSX-T Manager.

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 V Series nodes that are part of that service deployment will be deleted from the host. These 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.

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
- Interface Mapping
- Create Ingress and Egress Tunnel
- Create a New Map
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics

Create a Monitoring Session

Create a Monitoring Session

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

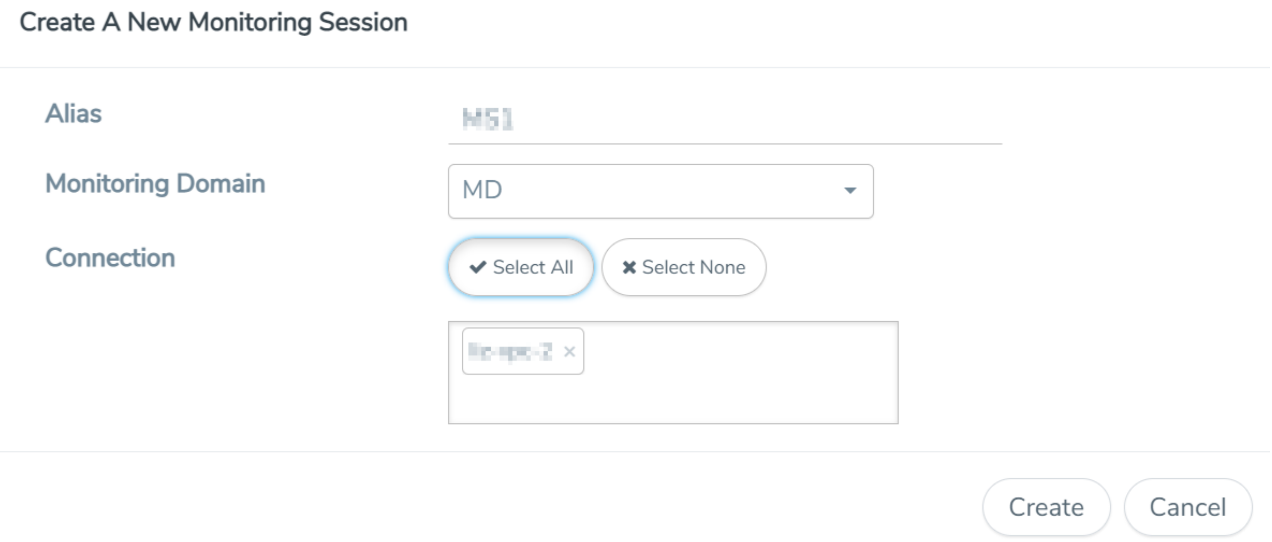
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

> **NOTE:** You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows > VMware**. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.



Create A New Monitoring Session

Alias: [redacted]

Monitoring Domain: MD

Connection: [redacted]

3. Enter the appropriate information for the monitoring session as described in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain that you want to select.
Connection	The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.

4. Click **Create**. The Monitoring Session details page appears displaying the specified session information and target VMs.

> **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.

The Monitoring Session page also has the following buttons:

Button	Description
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
Delete	Deletes the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Deploy	Deploys the selected monitoring session.
Undeploy	Undeploys the selected monitoring session.
Apply Threshold	You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates and how to apply threshold templates.

Edit Monitoring Session

In the edit monitoring session canvas page, you can add and configure applications, tunnel endpoints, raw endpoints, and maps.

Refer to the following topics for detailed information:

- Create Ingress and Egress Tunnels
- Add Applications to Monitoring Session
- Create Raw Endpoint
- Create a New Map

The **Edit Monitoring Session** page has the following buttons:

Button	Description
Show Targets	Use to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
Interface mapping	Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping topic for more details.
Deploy	Deploys the selected monitoring session. Refer to Deploy Monitoring Session topic for more details.

Interface Mapping

You can change the interface of individual GigaVUE V Series Nodes deployed in a monitoring session. After deploying the monitoring session, if you wish to change the interfaces mapped to an individual GigaVUE V Series Node, you can use the **Interface Mapping** button to map the interface to the respective GigaVUE V Series Nodes. To perform interface mapping:

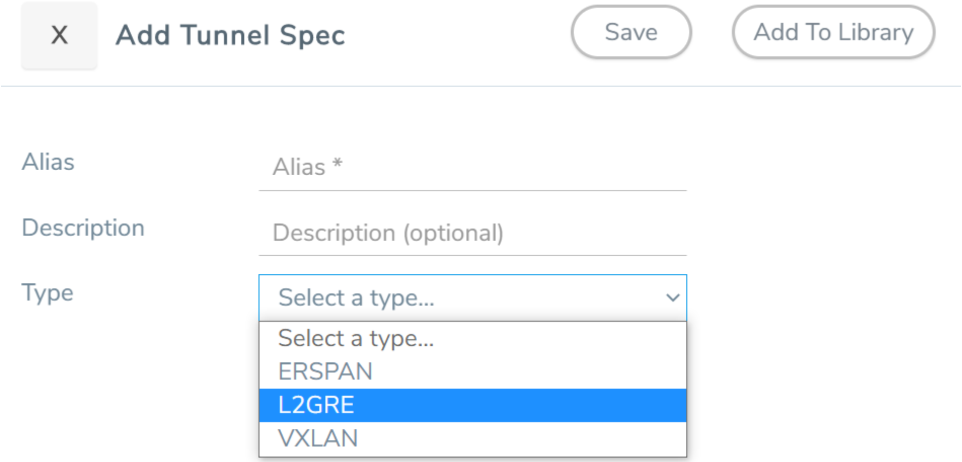
1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.
3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.
4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.
5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

Create Ingress and Egress Tunnel

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.

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.


X
Add Tunnel Spec
Save
Add To Library
Alias
Alias *
Description
Description (optional)
Type
Select a type...
Select a type...
ERSPAN
L2GRE
VXLAN

3. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description	
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.	
Description	The description of the tunnel endpoint.	
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN, or UDPGRE to create a tunnel.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint.	
	Remote Tunnel IP	For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled

Field	Description	
		with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the	

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

Field	Description	
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

Field	Description	
Out	**IP Version**	The version of the Internet Protocol. only IPv4 is supported.
	Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575
	Source L4 Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments when there is a delay.

4. Click **Save**.

To delete a tunnel, select the required tunnel and click **Delete**.

To apply threshold template to Tunnel End Points, select the required tunnel end point on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold template, refer to *Monitor Cloud Health* topic.

After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

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 a New Map

You must have the flow map license to deploy a map in the monitoring session.

For new users, the free trial bundle will expire after 30 days, and the GigaVUE-FM prompts you to buy a new license. For licensing information, refer to *GigaVUE Licensing Guide*.

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

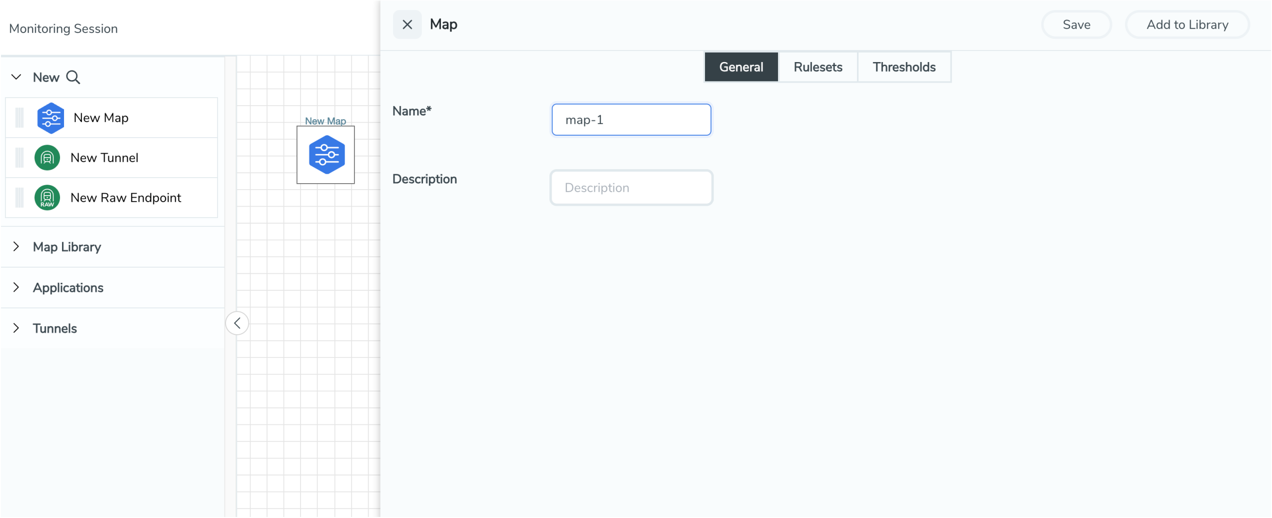
Keep in mind the following when creating a map:

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

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the monitoring session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: - mac Source - mac Destination - ipv4 Source - ipv4 Destination - ipv6 Source - ipv6 Destination - VM Name Destination - VM Name Source - VM Tag Destination - Not applicable to Nutanix. - VM Tag Source - Not applicable to Nutanix. - VM Category Source - Applicable only to Nutanix - VM Category Destination - Applicable only to Nutanix. - Host Name -Applicable only to Nutanix and VMware. The traffic direction is as follow: - For any rule type as Source - the traffic direction is egress. - For Destination rule type - the traffic direction is ingress. - For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **NOTE:** If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

To create a new map:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Map**, drag and drop a new map template to sthe workspace. The New Map quick view appears.



Name* map-1

Description Description

3. On the New Map quick view, click on **General** tab and enter the required information as described in the following table:

Field	Description
Name	Name of the new map
Description	Description of the map

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

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

4. Click on **Rule Sets** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to Example- Create a New Map using Inclusion and Exclusion Maps for more detailed information on how to configure Inclusion and Exclusion maps using ATS.
    a. **To create a new rule set:**
        i. Click **Actions > New Rule Set**.
        ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
        iii. Enter the Application Endpoint in the Application EndPoint ID field.
        iv. Select a required condition from the drop-down list.
        v. Select the rule to **Pass** or **Drop** through the map.
    b. **To create a new rule:**
        i. Click **Actions > New Rule**.
        ii. Select a required condition from the drop-down list. Click ... and select **Add Condition** to add more conditions.
        iii. Select the rule to **Pass** or **Drop** through the map.
5. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
    a. Select an existing group from the **Select Group** list or create a **New Group** with a name.
    b. Enter a description in the **Description** field, and click **Save**.
6. Click **Save**.

> **NOTE:** If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Map Statistics" section in *GigaVUE Fabric Management Guide* for detailed information.

To edit a map, select the map and click **Details**, or click **Delete** to delete the map.

To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.

Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.

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

- Click a map and select **Details** to edit the map
- Click a map and select **Delete** to delete the map.
- Click the **Show Targets** button to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.
- Click ⤢ to expand the **Targets** dialog box. To view details about a GigaVUE V Series Node, click the arrow next to the VM.
- In the Instances window, click ▼ to filter the list of instances.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a monitoring session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

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

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

Add Applications to Monitoring Session

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

- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- Header Stripping
- 5G-Service Based Interface Application
- Application Metadata Exporter
- SSL Decrypt

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

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

- Application Metadata Intelligence
- Application Filtering Intelligence

For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

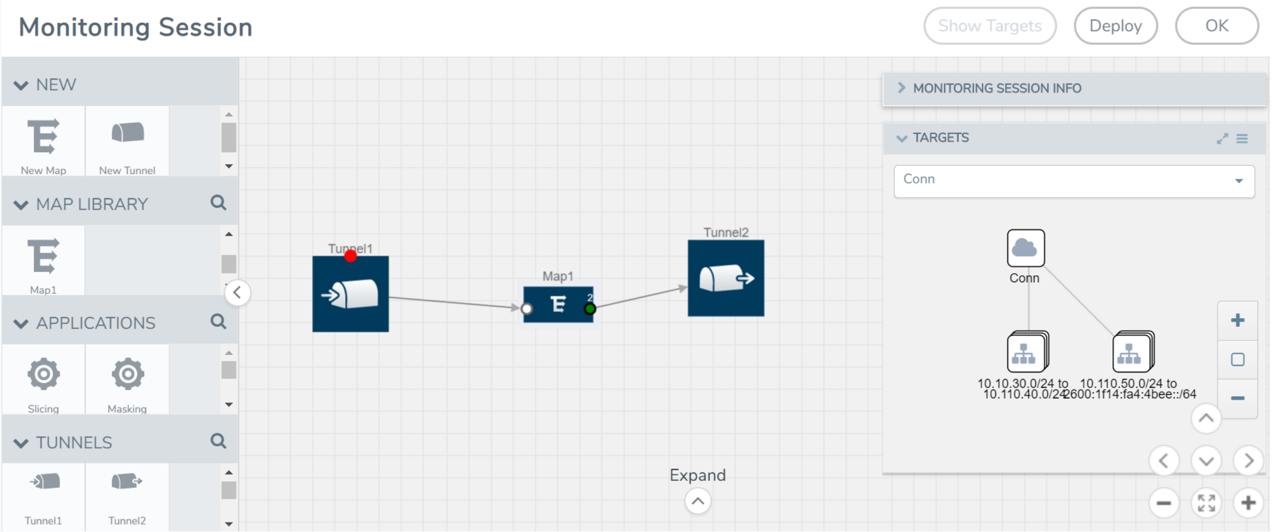
Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
   - Maps from the **MAP LIBRARY** section
   - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART apps from the **APPLICATIONS** section
   - Egress tunnels from the **TUNNELS** section

2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

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



3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
4. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.

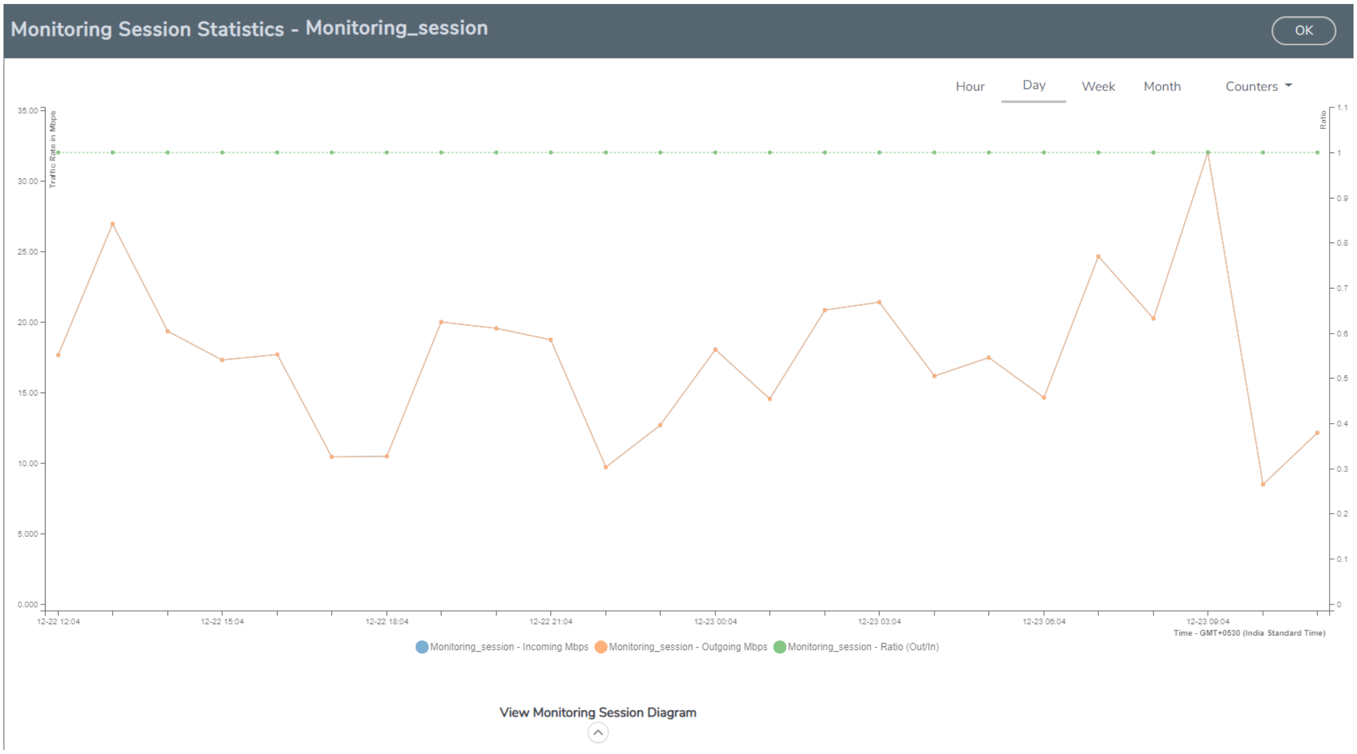
   The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

View Monitoring Session Statistics

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. The traffic can be viewed based on kilobits/second, megabits/second or gigabits/second.

On the Monitoring Sessions page, click **View** in the Statistics column to view the Monitoring Session Statistics page. The **Monitoring Session Statistics** page appears where you can analyze incoming and outgoing traffic.

> **NOTE:** If there are multiple monitoring sessions with different target selection, then the incoming maps will not show true statistics and it shows the aggregate traffic from all the targets.


Monitoring Session Statistics - Monitoring_session
OK
Hour
Day
Week
Month
Counters
Traffic Rate in Mbps
35.00
30.00
25.00
20.00
15.00
10.00
5.000
0.000
Ratio
1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
12-22 12:04
12-22 15:04
12-22 18:04
12-22 21:04
12-23 00:04
12-23 03:04
12-23 06:04
12-23 09:04
Time - GMT+0530 (India Standard Time)
Monitoring_session - Incoming Mbps
Monitoring_session - Outgoing Mbps
Monitoring_session - Ratio (Out/In)
View Monitoring Session Diagram

You can also perform the following actions on the Monitoring Session Statistics page:

- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.
- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.
- Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

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.

View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page. Refer to Monitor Cloud Health for more detailed information on how to configure cloud health and view health status.

The following columns in the monitoring session page are used to convey the health status:

Health

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy then the health status is moved to unhealthy.

V Series Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

You can view the health status of the individual V Series Nodes by clicking on the V Series Node Health column.

NOTE: V Series Node health only displays the health status therefore even if the V Series Node is down it will not be reflected in the monitoring session page.

Target Source Health

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

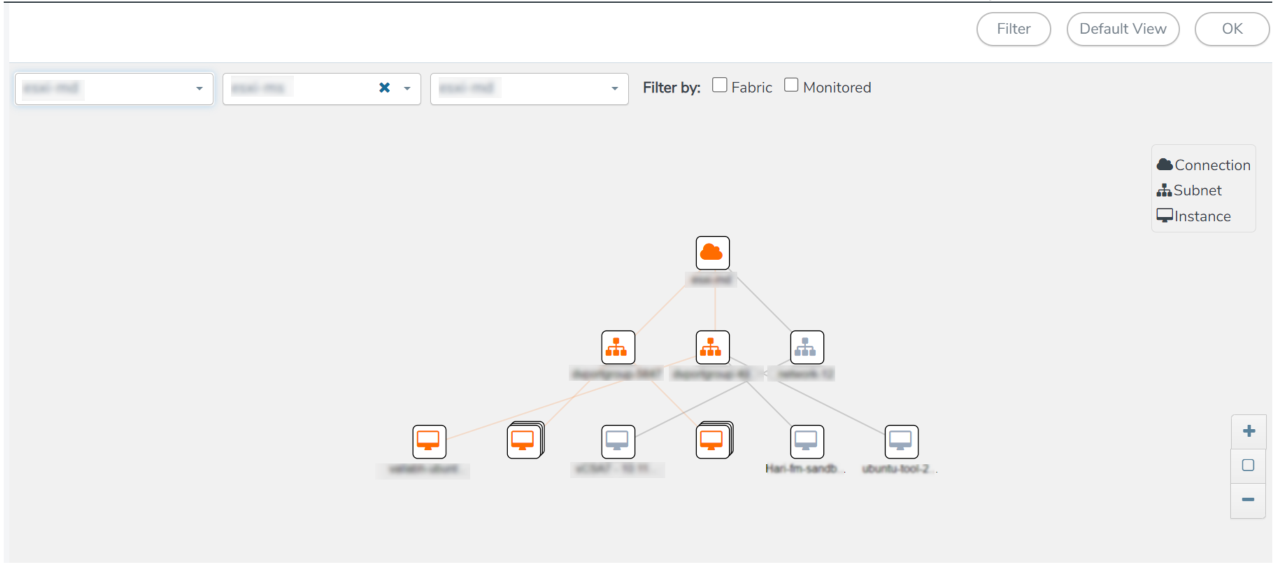
You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

Visualize the Network Topology

You can have multiple connections in GigaVUE-FM. Each connection can have multiple monitoring sessions configured within them. You can select the connection and the monitoring session to view the selected subnets and instances in the topology view.

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.
4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



5. (Optional) Hover over or click the subnet or VM Group icons to view the subnets or instances present within the group.

In the topology page, you can also do the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the right-bottom corner to move the topology page up, down, left, or right. Click the **Fit-to-Width** icon to fit the topology diagram according to the width of the page.
- Use **+** or **-** icons to zoom in and zoom out the topology view.

Create NSX-T Group and Service Chain

An NSX-T group and service chain must be created to redirect network traffic to the GigaVUE Cloud Suite. An NSX-T group defines which VMs are to be monitored. The service chain associates the GigaVUE Cloud Suite and map 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*.

To create the service chain in 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 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 **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.

The new Service Chain is then updated in the **NSX-T Virtual Maps** page of GigaVUE-FM.

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 NSX-T, 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.
        - Add or select Membership Criteria, Members, IP/MAC Addresses, and AD Groups.
    c. Enter the description for the group.
4. Click **Save** and then a group is created and appears on the **Groups** page.

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. 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 **Applied To** field, select the appropriate groups.
    f. On **Action** field, specify whether to redirect the traffic or not.
4. Click **Publish**. On publishing the rule/policy you can view the traffic flow from the V Series nodes to the tunnel endpoint.

Upgrade GigaVUE V Series Nodes for VMware NSX-T

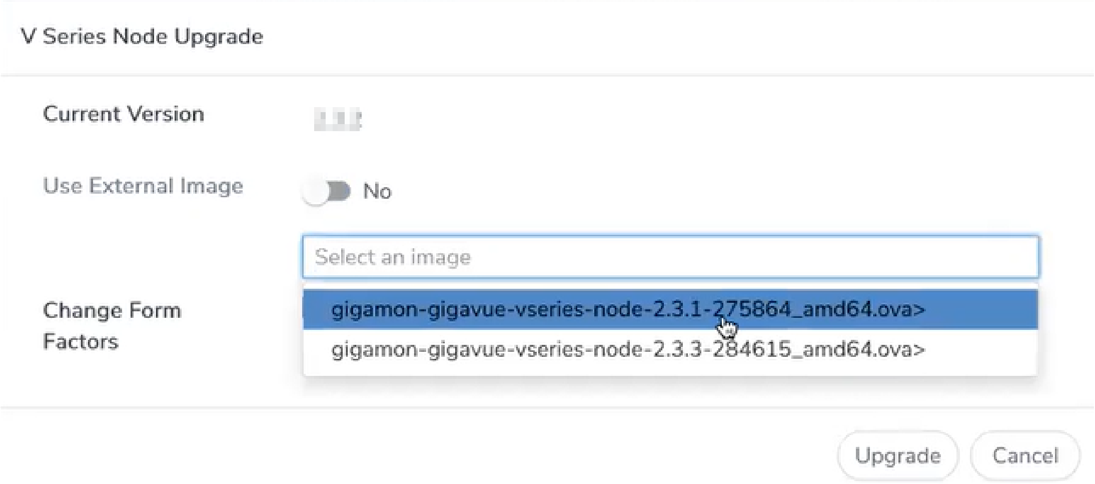
GigaVUE V Series Nodes can be deployed on VMware NSX-T in two ways. You can either directly use VMware NSX-T manager to deploy your V Series nodes or use GigaVUE-FM to deploy your V Series nodes. Based on the method in which you deploy GigaVUE V Series Nodes, you can upgrade them in two ways. Refer to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

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

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 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

Use External Image: No

Change Form Factors

Select an image
gigamon-gigavue-vseries-node-2.3.1-275864_amd64.ova>
gigamon-gigavue-vseries-node-2.3.3-284615_amd64.ova>
Upgrade
Cancel

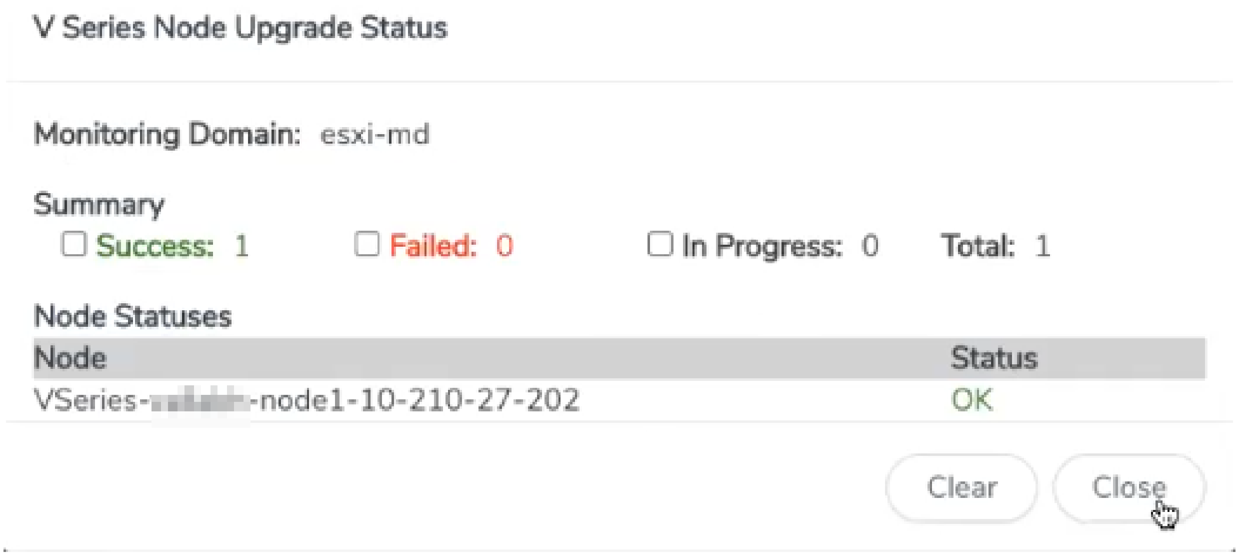
3. Use the **Use External Image** toggle button to choose between internal and external image.
   - **Yes** to use an external image. Enter the Image URL of the latest V Series Node OVA image
   - **No** to use an internal image. To use an internal image, select the uploaded OVA files from the **Select 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

> **NOTE:** 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.

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

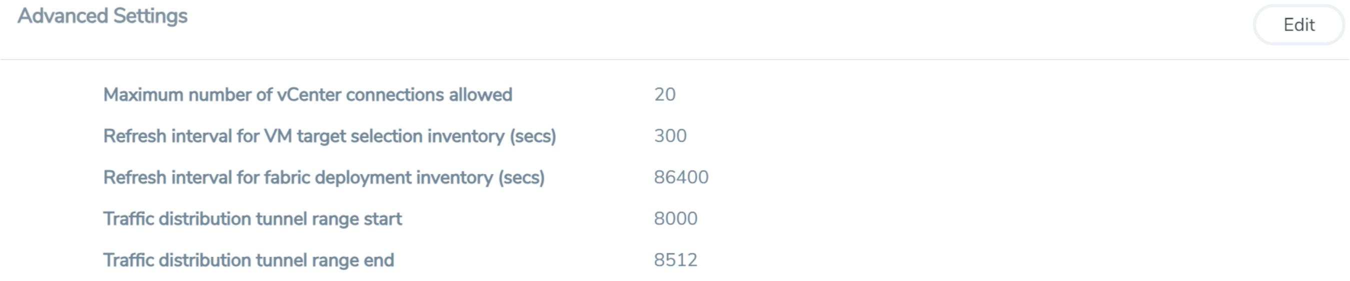
1. Delete the existing V Series Node in VMware NSX-T Manager.
2. Click **Actions > Edit** in the Monitoring Domain page. The **VMware Configuration** page appears.
3. Enter the new **Image URL** or select a new image if **Use External Image** toggle button is disabled.
4. Then, deploy the new V Series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

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

Refer to the following table for details:

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

Configure Application Intelligence Solutions on GigaVUE V Series Nodes for VMware NSX-T

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow. Refer the following topics for step by step instructions on how to configure Application Intelligence solution for GigaVUE V Series Nodes:

- Configure Environment
- Connect to VMware NSX-T
- Create NSX-T Group and Service Chain
- Create Tunnel Specifications
- User Defined Application
- Configure Application Intelligence Session

- Slicing and Masking in Application Filtering Intelligence
- Application Metadata Intelligence
- Create NetFlow Session for Virtual Environment

Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **GigaVUE V Series Proxy** to scale and manage multiple GigaVUE V Series Nodes. Refer to the GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide for detailed information.
- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- To delete a GigaVUE V Series Node deployed in a Application Intelligence solution, you must delete the resources in the following order:
    1. Delete the Application Intelligence solution.
    2. Delete the GigaVUE V series Node and Connection.
    3. Delete the Environment.

Configure Environment

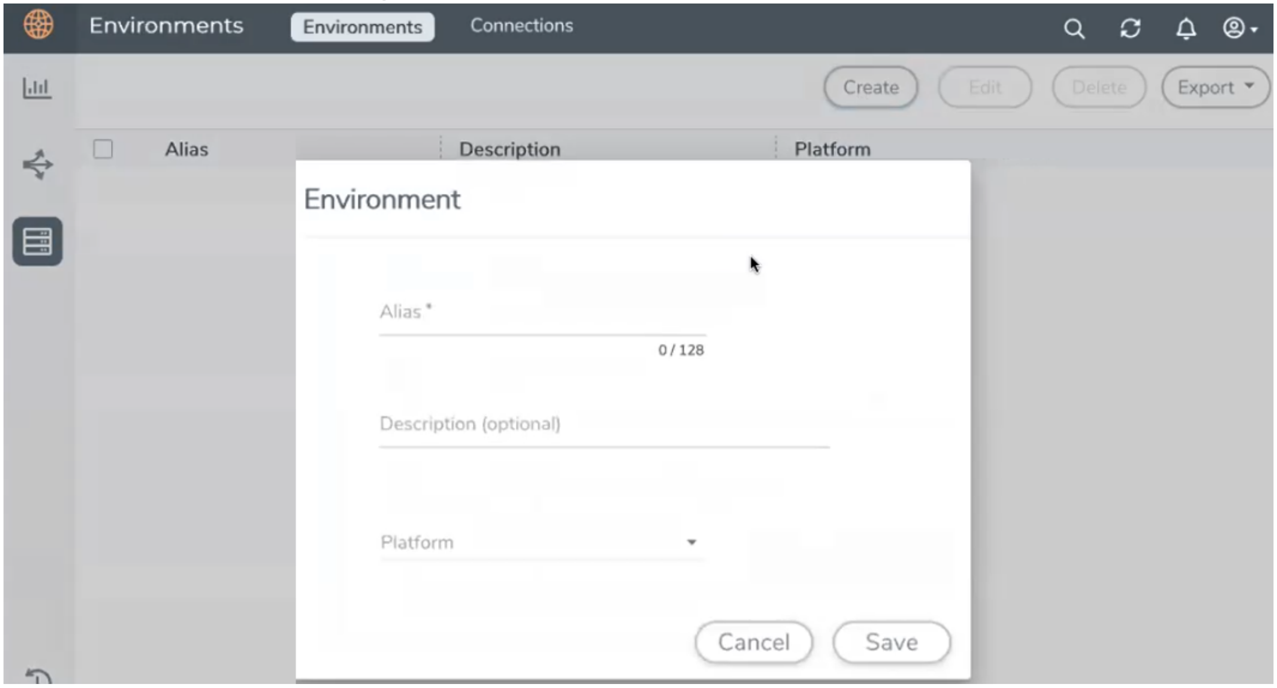
The Environments page allows you to create the following:

- **Environments**: The physical or the virtual environment in which the Application Intelligence solution is to be deployed.
- **Connections**: Connection between GigaVUE-FM and the cloud platform.

Create Environment

To configure the Environment:

1. Select **Inventory** > **Resources** > **Environments**.
2. On the **Environments** page, on the **Environments** tab, click **Create**.



3. Select or enter the following details:

Field	Description
Alias	Alias name used to identify the Environment.
Description	Brief description about the Environment.
Platform	Select the cloud platform.

4. Click **Save**. The environment is added to the list view.

Use the following buttons to manage your environment:

Button	Description
Delete	Use to delete an Environment.
Edit	Use to edit the details in an Environment.
Export	Export the details from the Environment page in an XLS or CSV file.

Connect to VMware NSX-T

After creating a environment create a connection between the VMware NSX-T and GigaVUE-FM.

Refer to the following sections for details:

- Rules and Notes
- Steps

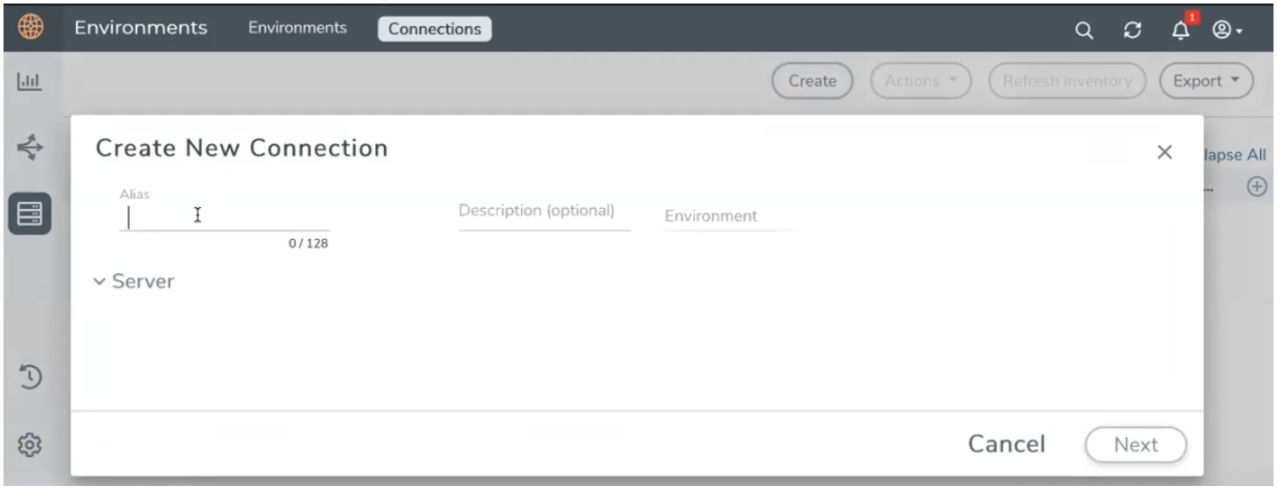
Rules and Notes

- NSXT- manager version must be 3.1.3. Otherwise after editing the solution, the packets will not reach the GigaVUE V Series Node.
- NSX-T manager cannot be registered for more than one GigaVUE-FM.
- For GigaVUE-FM software version 5.13.00, you cannot deploy more than one GigaVUE V Series Node.
- **For GigaVUE-FM software version 5.13.00**: If you configure a GigaVUE V Series Node with the Application intelligence solution, then you must not configure other basic GigaSMART applications, such as slicing, masking, and vice-e-versa. These GigaSMART applications cannot work in parallel.

Create Connection

To create a new Connection:

1. Select **Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Connections** tab, click **Create**.



3. The **Create New Connection** dialog box opens. Enter the details as mentioned in the below section.

> **NOTE:** When creating a connection in the connections page, the corresponding monitoring domain created for internal use in GigaVUE-FM will not be displayed in the Monitoring Domain list page.

To connect to VMware NSX-T, select or enter the following details:

Field	Description
Alias	Alias name used to identify the connection.
Description	Brief description about the connection.
Environment	Select the environment configured in the Connect to VMware NSX-T
Server	The IP address or the DNS name of the virtual server.
vCenterUserName	Valid user name
vCenterPassword	Password for the user
NSX-T Manager IP Address	IP address or Hostname of your VMware NSX-T.
NSX-T User Name	Username of your NSX-T account.
NSX-T Password	Password of your NSX-T account.
Image URL	Web Server URL of the directory where V Series node OVA, VMDK, and OVF files are available. The Web Server URL must be in the follwoing format: *http://<server-IP:port>/<path to where the OVF files are saved>* and the port can be any valid number.
GigaVUE-FM User Name	GigaVUE-FM username.
GigaVUE-FM Password	GigaVUE-FM password
Enable Custom Certificates	Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs. **NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate.

Once the connection is established, enter the following details in the fabric launch configuration page, and click **Save**:

Field	Description
Datacenter	vCenter Data Center with the ESXi hosts to be provisioned with V Series nodes
Cluster	Cluster where you want to deploy V Series nodes
Datastore	Network datastore shared among all ESXi hosts.
Management Network	Management network for V Series nodes
IP Type	Select the management network IP type as Static or DHCP

Field	Description
Tunnel Network	Tunnel Network for the V Series nodes
IP Type	Select the tunnel network IP address type as Static or DHCP
Tunnel Gateway IP	Gateway IP address of the Tunnel Network
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry.
Netmask Length	CIDR value of the Tunnel.
User Password: (gigamon)	SSH Password for the built-in user, '**gigamon**' on the V Series node
Confirm User Password	Confirm the SSH Password of the V Series node
Form Factor	Instance size of the V Series node
Service Attachment	Service segment created on NSX-T
Deployment Type **Deployment Count** (for Clustered deployment type)	Deployment type is clustered. **NOTE:** Host-based deployment option is disabled, as there can be one V series node per ESXi host. Deployment count is restricted to one V Series nodes (Service Instances).

Use the following buttons to manage your VMware NSX-T connections :

Button	Description
Create	Use to create new connection.
Actions	Provides the following options: • **Edit Connection** - Use to edit a connection. You can only edit the following fields in the Edit Connection page: ▪ vCenter Username ▪ vCenter Password ▪ NSX-T Username ▪ NSX-T password ▪ Image URL • **Deploy Node** - Use to deploy a node. • **Delete Connection** - Use to delete a connection. • **Delete Node** - Use to delete a node. • **Force Delete** -This option is enabled when an upgrade fails due to infrastructure issues. Use this option to force delete the connection. • **Upgrade Fabric** - Use to upgrade the fabric components. • **Continue Upgrade Fabric** - If the upgrade failed or interrupted for any reason, use this optionto continue the upgrade process.
Refresh Inventory	Use to refresh the entire connections page.
Export	Use to export the details from the Connections page into an XLS or a CSV file.

To create Application Intelligence sessions, refer to Create an Application Intelligence Session in Virtual Environment.

Refer Deploying Application Intelligence Solution at Scale on VMware NSX-T 3.1.3 for more detailed information.

Create NSX-T Group and Service Chain

After creating connection to NSX-T, VMware NSX-T NSX-T manager is responsible for configuring the sources. In order for VMware NSX-T manager to configure the source, you must create groups and service chains in NSX-T manager. Refer Create NSX-T Group and Service Chain for step-by-step instructions.

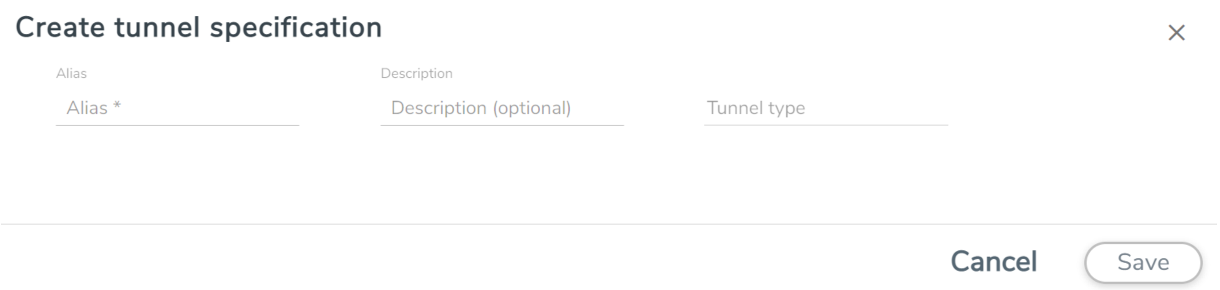
Create Tunnel Specifications

A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel. The tunnel can be an ingress tunnel or an egress tunnel.

NOTE: VXLAN is the only supported tunnel type for Azure.

To configure the tunnels:

1. Select **Inventory** > **Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **VM** tab and click **Create**. The Create Tunnel Specification wizard appears.



Create tunnel specification

Alias: Alias *

Description: Description (optional)

Tunnel type

3. Enter or select the following information:

Field	Description
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Tunnel Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN to create a tunnel. Do not select UDPGRE tunnel type. **NOTE:** VXLAN is the only supported tunnel type for Azure.
Traffic Direction	The direction of the traffic flowing through the V Series node. • Choose **In** (Decapsulation) for creating an Ingress tunnel, Tunnel Spec for the Source should always have the Traffic Direction as IN, signifying an ingress tunnel. Enter values for the Key. • Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key. • ERSPAN, L2GRE, and VXLAN are the supported **Ingress tunnel** types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session. • L2GRE and VXLAN are the supported **Egress tunnel** types. • For Azure connection, VXLAN is the supported Ingress and Egress tunnel type.
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.

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

User Defined Application

This feature gives you the ability to classify the applications by the DPI engine. This allows unclassified TCP, UDP, HTTP, and HTTPS applications to be identified and named with the help of user defined application signatures.

To configure User Defined Application signatures :

Step Number	Task	Refer the following
1	Create rules under User Defined Application Section	Create rules under User Defined Application
2	Configure Application Intelligence Session	For Physical: Application Intelligence Session For Virtual: Configure Application Intelligence Session
3	Monitor User Defined Application	View the Application Intelligence Dashboard

Create Rules under User Defined Application

1. Click **Inventory**.

2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.

3. Click **New** in the **User Defined Applications** screen to create a new rule.

4. Enter **Application Name**.

5. Enter **Priority**. The value must be between 1 and 120.

Note: The least value will have the highest priority.

6. In the created rule:

   a. Choose the **Protocol** from the list of protocols.

   b. Choose the **Attributes** from the list of attributes.

   c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.

8. Click the application listed under the **Applications** column.

9. Click the **Rule** tab.

10. Select a rule to view its protocol details.

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regex patterns, refer Supported RegExp Syntax

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file|new_slice|upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-	Referer	Source	Client	REGEXP	http:\/\/gigamon.com\/

	referer	URI	address where client got the URI	to Server Only		
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\/football\/.*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
ssl	common_name	Domain Name	Domain name from Client Hello message or the certificate		REGEXP	(.*\.)?gigamon\.com
	stc-	Subjec	List of	Server	REGEXP	(.*\.)?gigamon\.com

	subject_alt_name	t Alt Name(s)	host names which belong to the same certificate	to Client Only		
rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http:\/\/www.music.tv\/recorded\/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a packet, excluding the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata
	port	Server Port	Server (listen)		UINT16 RANGE	80-4350

			port number		as REGEXP String	
sip	user_agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Message Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Message Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Address	IP address of the server		IPV4 as REGEXP String	62.132.12.30\/24
	dscp	DSCP Value	DSCP from Differentia ted Service (DS) Field in IP header		UINT8 as REGEXP String	33

	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentiated Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
( )	Groups a series of expressions together

[ ]	Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
| [<start>-<end>]	Separates values contained in ( ). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog | cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_number>	Matches for a direct binary with octal input
\x<hexadecimal-number>\x	Matches for a direct binary with hexadecimal input
\[<character-set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Configure Application Intelligence Session

Application Intelligence provides a comprehensive solution that:

- identifies the applications contributing to the network traffic.
- isolates preferred application-specific traffic and directs it to the appropriate tools.
- exports relevant application metadata for further analytics and analysis.

Application Intelligence provides the following capabilities for both physical devices and virtual nodes:

- **Application Visualization (earlier known as Application Monitoring)** - Identifies and monitors all applications contributing to the network traffic, and reports on the total applications and the total bandwidth they consume over a select period. Able to identify more than 3,200 applications. It displays the traffic statistics in bytes, packet and flows.

- **Application Filtering Intelligence**- Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.
- **Application Metadata Intelligence** - Supports exporting over 5000 attributes of metadata that provide relevant usage context on over 3,200 applications, thus enabling you to rapidly identify indicators of compromise (IoC) for security analytics and forensics tools.

Prerequisites

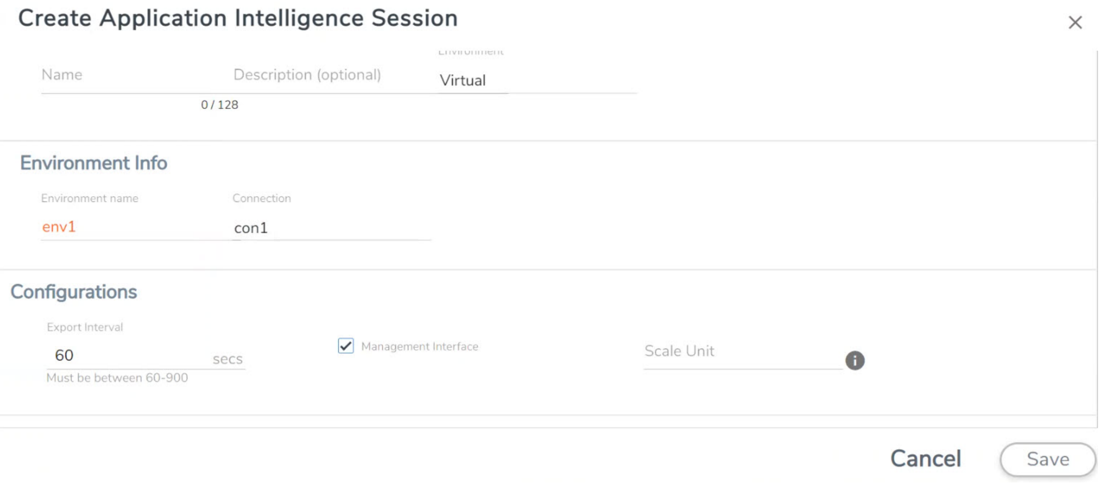
- The environment on which the Application Intelligence solution is to be deployed must already be created and the nodes must be deployed on it.
- In virtual environment, the destination tunnels for the Application Filtering Intelligence Map must already be created.

> **NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

To create an Application Intelligence Session:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create New**. The **Create Application Intelligence Session** page appears.



Create Application Intelligence Session

Name

Description (optional)

0 / 128

Environment

Virtual

Environment Info

Environment name

env1

Connection

con1

Configurations

Export Interval

60 secs

Must be between 60-900

☑ Management Interface

Scale Unit

3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created:
   - Virtual- connects to the specific environment.
4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides..

5. In the **Configurations** section, complete the following:
    a. Select an **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization. The valid range is 60–900 seconds.
    b. Select the required interface. By default, **Management Interface** is enabled. To export the data through tunnel interface, uncheck the Management Interface check box.
    c. Enter a value for the **Scale Unit**. The scale unit represents the number of flows supported by the application. If the scale unit value is 1, the maximum active flow limit will be 100k.
    Refer to the following table for the maximum scale unit supported for VMware, AWS, and Azure platforms.

Cloud Platform	Instance Size	Maximum Scale Unit without using Secure Tunnels	Maximum Scale Unit when using Secure Tunnels
VMware	Large (8 vCPU and 16 GB RAM)	3	2
AWS	Large (c5n.2xlarge)	3	3
Azure	Large (Standard_D8s_V4)	5	5

> **NOTE:** If the Application Intelligence Session deployment fails, due to using a scale unit other than the recommended scale unit, then reload the GigaVUE V Series Node.

6. In the **Source Traffic** section, select anyone of the following:

- **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to Create Source Selectors.
    - **Prefilter** - Enable the mirroring option, select the prefilter checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.
    - **Precryption**: Select the Precryption checkbox and then select the policy. If you want to enable Secure tunnel, then select the secure tunnel checkbox.

> **NOTE:** You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using the Third Party Orchestration in VMware ESXi host.

- **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to Create Tunnel Specifications.

> **NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration.

- **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will trap the traffic for application monitoring.

  > **NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

> - Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel.
> - For Azure Connection, VXLAN is the only supported Tunnel Type.

7. Click **Save**. The session created is added in the list view.
8. In the **User Defined Applications** section, select the template from the list.For information on **Supported protocols and Attributes** and **Limitations** refer **User Defined Application** topic.

The total applications participating in the network traffic are displayed in the Application Intelligence Dashboard. For more information about the dashboard, refer to the View the Application Intelligence Dashboard.

Select the session from the Application Intelligence Sessions pane and click on the ⋮ icon and select **View Details** from the drop-down menu, to view the deployed UCT-V, their status and more information about source selectors, selected target.

If the session configuration is unsuccessful, troubleshoot the error notified (refer to View the Health Status of a Solution). Click the **Reapply all pending solutions** button ⟲ in the dashboard to redeploy the configuration.

> **NOTE:** GigaVUE-FM takes few minutes to display the application statistics.

> **NOTE:** The option **Reapply all pending solutions** is applicable for physical solution only.

When the Application Intelligence solution is in suspended state, you cannot delete the session. You can click on the ⋮ icon and select **View Details** from the drop-down menu, to view the details.

You can also filter the traffic based on the applications. For more information, see Create Application Filtering Intelligence.

Slicing and Masking in Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. With the addition of slicing and masking parameters to the existing application filtering functionality, you will be able to slice, mask, or slice and mask the filtered packets before sending them to the destination tunnel endpoint.

For step-by-step instructions on how to configure Application Filtering Intelligence refer to Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard topic from *GigaVUE Fabric Management Guide*.

Configuring Application Filtering Intelligence with Slicing

You can enable the slicing configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be sliced.

The filtered traffic will be sliced before forwarding it to the destination tunnel endpoint.

Refer to Slicing section in the *GigaVUE V Series Applications Guide* for more detailed information on Slicing.

Configuring Application Filtering Intelligence with Masking

You can enable the masking configuration and provide inputs for each **Application Filtering** rule set:

1. From the **Select a Protocol** drop-down list, choose a protocol.
2. In the **Offset** field, specify the length of the packet that must be masked.
3. In the Pattern field, enter the pattern for masking the packet.
4. In the Length field, enter the length of the packet that must be masked.

The filtered traffic will be masked before forwarding it to the destination tunnel endpoint.

Refer to Masking section in the *GigaVUE V Series Applications Guide* for more detailed information on Masking.

Configuring Application Filtering Intelligence with Slicing and Masking

You can enable both slicing and masking configurations, and provide inputs for each **Application Filtering** rule set.

The filtered traffic will be sent to the slicing application, the sliced traffic will be sent to masking application and then to the destination tunnel Endpoint.

> **NOTE:** When combining slicing and masking operations, the offset range of the masking must be lesser than the offset value entered for the slicing operation, as the slicing operation is performed first.

Application Metadata Intelligence

Application Metadata Intelligence generates more than 5000 attributes for more than 3200 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

Application Metadata Intelligence (AMI) is enabled to multi-collect protocols with more than one metadata attribute of the same type. The multi-collect feature supports additional protocols such as DNS, GTP,GTPV2, DHCP, HTTP, HTTPS, SSL, HTTP_PROXY, HTTP2, KERBEROS5, and DHCP6.

The generated metadata is exported in IPFIX (IP Flow Information Export) format and CEF (Common Even Format) to security analytics and forensics tools thereby providing greater visibility to enforce corporate compliance.

The output from the Application Metadata Intelligence in CEF format can also be converted to JSON format using Application Metadata Exporter (AMX) application. To learn more about AMX application refer to Application Intelligence—Application Metadata Exporter

Application Metadata Intelligence generates metadata only if the application is allowed to be passed in Application Filtering Intelligence. For example, Application Metadata Intelligence has the capability to generate metadata for HTTP traffic only if Application Filtering Intelligence filters in the HTTP traffic.

Refer to Create Application Metadata Intelligence Session for Virtual Environment topic for step-by-step instructions on how to configure Application Metadata Intelligence on Virtual Environment.

Create Application Metadata Intelligence Session for Virtual Environment

You can create an Application Metadata Intelligence session for virtual environment.

To create an Application Metadata Intelligence session, follow these steps:

1. Go to **Traffic > Solutions > Application Intelligence**.
2. From the Sessions pane, click ⋮ and select **Edit**. The **Edit Application Intelligence Session** window appears.

3. In the **Edit Application Intelligence Session** window, click **Application Metadata**.

   > **NOTE:** If Application Filtering Intelligence License is available, you must create Application Filtering to create Application Metadata Intelligence. For more information, refer to Create Application Filtering Intelligence by Editing Monitoring Session from Dashboard

4. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can also create multiple exporters.
   a. Enter the following details:

Field	Description
Tool Name	Enter the tool Name
Tool IP Address	Enter the tool IP address
Template	Select the tool template. Refer to Tool Templates for more details on what are tool templates and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow or CEF
NetFlow: Select this option to use Netflow	
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
CEF: Select this option to use CEF	
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.

   b. Click **App Editor**, to select the applications and its attributes. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFLow V5 Template in the above **Template** drop-down menu.) The Application Editor screen appears as shown:

c. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. You can also select **Add All Applications in Family** or **Delete All Applications in Family**. The selected applications and their families appear in the **Selected Applications** section.

> **NOTE:** You can select the required applications without selecting the application family.

5. In the **Advanced Settings** > **Collects** section, you can select the following packet attributes:
   - Counter - Select the Bytes, and Packets.
   - IPv4 - Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
   - IPv6 - Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
   - Transport -Select the required attributes. By default, Source Port, Destination Port are enabled.

   a. By default, the above collect types are displayed. Click ⊕ to add the following collect types:
      - Data Link - Select any one of the parameters such as Source Mac, Destination Mac and VLAN.
      - Timestamp - Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
      - Flow - Select the parameter as End Reason if required.
      - Interface - Select any one of the parameter such as Input Physical, Output Physical and Input Name.

6. In the **Application Metadata Settings** section:
   a. Select the Flow Behavior as any one of the following:
      - Uni-Directional
      - Bi-Directional. The default value is Bi-Directional.

   b. Enter the Timeout and Cache Size.

   c. You can enable or disable the **Multi-Collect** option to perform the following:
      - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
      - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.

   d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

> **NOTE:** You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

   e. You can enable or disable the **Advance Hash** option to perform the following:
      - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
      - **Disable** — Disables the metadata cache advance-hash for flows.

   f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.

   g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.

7. Click **Save**.

The metrics of the Application Metadata traffic appear on the dashboard.

Create NetFlow Session for Virtual Environment

Note: This configuration is applicable only when using NetVUE Base Bundle.

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

To create an NetFlow session, follow these steps:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create** . The **Create Application Intelligence Session** page appears.
3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created.
4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to *Configure Environment* section in the respective cloud guides.
5. In the **Configurations** section, complete the following:
   a. The **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization is 5 seconds
   b. By default, **Management Interface** is enabled.

6. In the **Source Traffic** section, select anyone of the following:
   a. **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to Create Source Selectors

      > **NOTE:** You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using Third Party Orchestration in VMware ESXi Host

   b. **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to Create Tunnel Specifications.

      > **NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration. Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel. For Azure Connection, VXLAN is the only supported Tunnel Type.

   c. **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will tap the traffic for application monitoring.

      > **NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

7. Click on the **Application Metadata** tab.

8. In the **Destination Traffic** section, click **+ Add New** to create an exporter to receive application-specific traffic. You can only create a maximum of 5 exporters. Enter the following details:

Field	Description
Tool Name	Enter the tool name.
Tool IP Address	Enter the tool IP address.
Template	Select the tool template. Refer to Tool Templates for more details on what tool templates are and to create custom tool templates.
L4 Source Port	Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A.
L4 Destination Port	Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B.
APPLICATION ID	Enable to export the data with Application Id.
Format	NetFlow
Record / Template type	● Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. ● Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active timeout value in seconds.
Inactive Timeout	Enter the inactive timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds.

9. In the **Advanced Settings** > **Collects** section, the following details are already configured.

> **NOTE:** When the template is NetFlow v5 or when the format is NetFlow and the version as V5 you cannot modify the **Collects**.

- TimeStamp
- Counter
- Interface
- IPv4
- Transport

10. In the **Application Metadata Settings** section:
    a. Select the Flow Behavior as any one of the following:
        - Uni-Directional
        - Bi-Directional. The default value is Bi-Directional.

    b. Enter the Timeout and Cache Size.

    c. You can enable or disable the **Multi-Collect** option to perform the following:
        - **Enable** — Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. By default, when a new cache is created, multi-collect is enabled. When upgraded from an older release, the multi-collect option is enabled.
        - **Disable** — Disables the multi-collect of attributes within a given Metadata Store cache.

    d. You can use the toggle button to enable or disable the **Aggregate Mode**, which is disabled by default. You need to delete the existing solution and recreate the solution to enable the **Aggregate Mode**. The **Aggregate Mode** option is applicable only for Gen 3 devices. Only one exporter is supported with the **Aggregate Mode** enabled.

Protocol Name	Attribute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

> **NOTE:** You need to enable the **Aggregate Mode** option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

e. You can enable or disable the **Advance Hash** option to perform the following:
   - **Enable** — Configures metadata cache advance-hash for encapsulated flows . This feature improves the efficiency of scheduling the distribution of encapsulated flows. It also improves the distribution of flows in service provider deployment cases. By default, when a new cache is created, advance hash is enabled. When upgraded from an older release, the advance hash is enabled.
   - **Disable** — Disables the metadata cache advance-hash for flows.

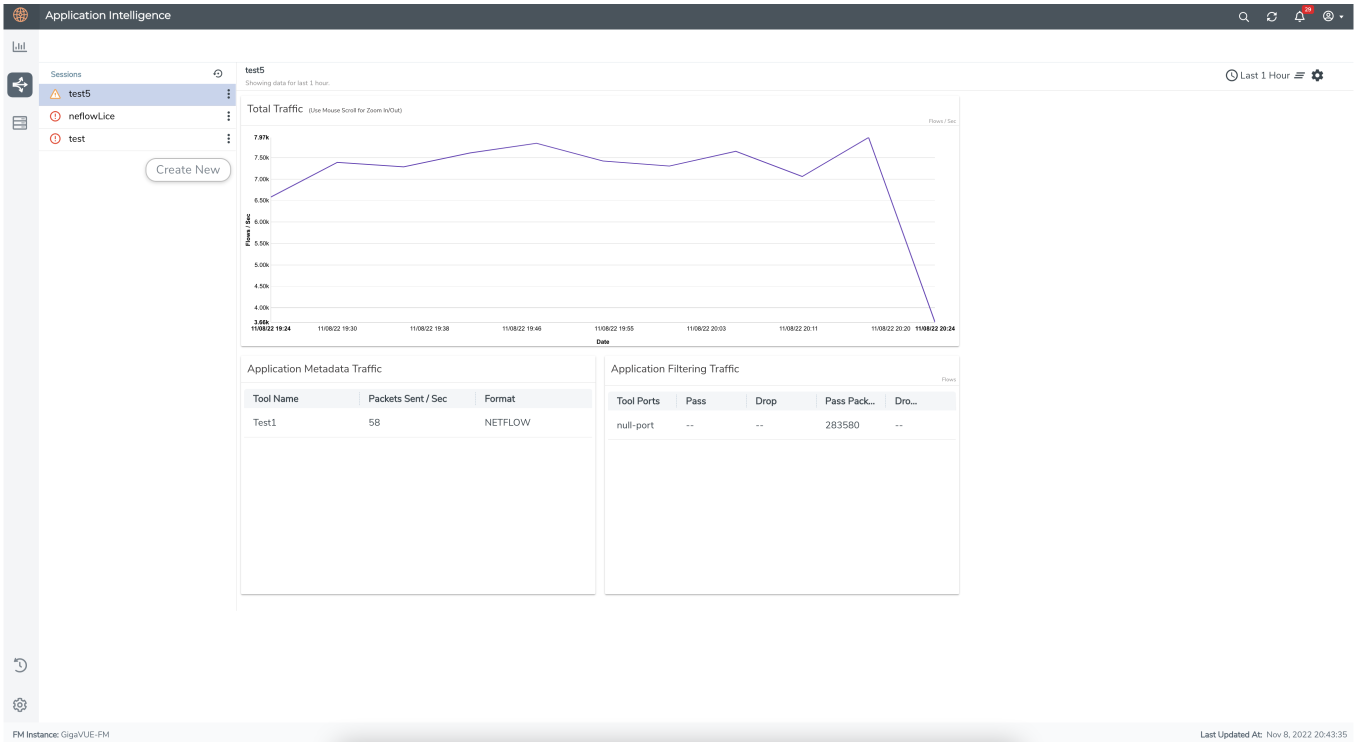
f. If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.

g. In the **Observation Domain ID** field, enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.

11. Click **Save**.

NetFlow Dashboard

In Appviz, only the traffic statistics are displayed as applications cannot be configured and used in the NetFlow configuration



Tool Name	Packets Sent / Sec	Format
Test1	58	NETFLOW

Tool Ports	Pass	Drop	Pass Pack...	Dro...
null-port	--	--	283580	--

FM Instance: GigaVUE-FM

Last Updated At: Nov 8, 2022 20:43:35

Remove Gigamon Service from NSX-T and GigaVUE-FM

To clean up the Gigamon Visibility Platform from NSX-T and GigaVUE-FM, perform the following steps:

- Step 1: Remove the Service Chains
- Step 2: Delete the Monitoring Session
- Step 3: Undeploy GigaVUE Cloud Suite - V Series VMs
- Step 4: Delete the NSX-T Manager and vCenter Connections

Step 1: Remove the Service Chains

To delete the network monitoring services:

1. Select **Security > Settings >Network Introspection** and then click **SERVICE CHAINS** tab.
2. On the appropriate Service Chain, click ⋮ and then select **Delete** to delete the selected Service Chain.

Step 2: 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 **Delete**. The service profile and the profile that corresponds to the map is deleted on NSX-T manager console.

Step 3: Undeploy GigaVUE Cloud Suite - V Series VMs

To undeploy GigaVUE Cloud Suite-Fabric VMs from GigaVUE-FM:

1. From the left navigation pane, select **Inventory** > **VIRTUAL** > **VMware** > **Monitoring Domain**. The Monitoring domain page appears along with the deployed V Series nodes.
2. Select the appropriate **Monitoring Domain** for NSX-T, click on the dropdown option for Delete and then click **Delete Fabric Nodes**.

Step 4: Delete the NSX-T Manager and vCenter Connections

To delete the NSX-T Manager from GigaVUE-FM:

1. From the left navigation pane, select **Inventory** > **VIRTUAL** > **VMware** > **Monitoring Domain**. The monitoring domain page appears.
2. Select the appropriate NSX-T monitoring domain that you wish to delete and then click **Delete Monitoring Domain** option from the **Delete** dropdown.

Monitor Cloud Health

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

- Configuration Health Monitoring
- Traffic Health Monitoring
- View Health Status

Configuration Health Monitoring

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

This feature is supported for the following fabric components and features on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For UCT-Vs:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

To view the configuration health status, refer to the Configuration Health Monitoring section.

Traffic Health Monitoring

GigaVUE-FM allows you to monitor the traffic health status of the entire monitoring session and also the individual V Series Nodes for which the monitoring session is configured. Traffic health monitoring focuses on identifying any discrepancies (packet drop or overflow etc) in the traffic flow. When any such discrepancies are identified, GigaVUE-FM propagates the health status to corresponding monitoring session. GigaVUE-FM monitors the traffic health status in near real-time. GigaVUE V Series Node monitors the traffic, when the traffic limit goes beyond the upper or lower threshold values that is configured, it notifies GigaVUE-FM, based on which traffic health is computed.

> **NOTE:** When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to Configuration Settings section in the *GigaVUE Administration Guide* for configuration details.

This feature is supported for GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware

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

- Create Threshold Template
- Apply Threshold Template
- Edit Threshold Template
- Clear Thresholds
- Supported Resources and Metrics

Keep in mind the following points when configuring a threshold template:

- By default Threshold Template is not configured to any monitoring session. If you wish to monitor the traffic health status, then create and apply threshold template to the monitoring session.
- Editing or redeploying the monitoring session will reapply all the threshold policies associated with that monitoring session.
- Deleting or undeploying the monitoring session will clear all the threshold policies associated with that monitoring session.
- After applying threshold template to a particular application, you need not deploy the monitoring session again.

Create Threshold Template

To create threshold templates:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
2. The **Threshold Template** page appears. Click **Create** to open the **New Threshold Template** page.
3. Enter the appropriate information for the threshold template as described in the following table.

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Monitored Objects	Select the resource for which you wish to apply the threshold template. Eg: TEP, REP, Maps, Applications like Slicing, Dedup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that needs to be monitored. For example: Tx Packets, Rx Packets.
Type	**Difference**: The difference between the stats counter at the start and end time of an interval, for a given metric. **Derivative**: Average value of the statistics counter in a time interval, for a given metric.
Condition	**Over**: Checks if the statistics counter value is greater than the 'Set Trigger Value'. **Under**: Checks if the statistics counter value is lower than the 'Set Trigger Value'.
Set Trigger Value	Value at which a traffic health event is raised, if statistics counter goes below or above this value, based on the condition configured.
Clear Trigger Value	Value at which a traffic health event is cleared, if statistics counter goes below or above this value, based on the condition configured.

4. Click **Save**. The newly created threshold template is saved, and it appears on the **Threshold Template** page.

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

To apply the threshold template across a monitoring session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. To apply a threshold template across a monitoring session, select the template you wish to apply across the monitoring session from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Done**.

Apply Threshold Template to Applications

To apply the threshold template to a particular application in the monitoring session follow the steps given below:

> **NOTE:** Applying threshold template across monitoring session will not over write the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it over writes the existing threshold value for that particular application.

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

Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appear.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

> **NOTE:** Editing a threshold template does not automatically apply the template to monitoring session. You must apply the edited template to monitoring session for the changes to take effect.

Clear Thresholds

You can clear the thresholds across the entire monitoring session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the monitoring session follow the steps given below:

1. On the **Monitoring Session** page. Click**Actions > Edit**. The Edit Monitoring Session page with canvas page appears.
2. Click on the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Click **Clear All** and then Click **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a monitoring session follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds page appears**. Click **Clear**.

> **NOTE:** Clearing thresholds at monitoring session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application refer to Clear Thresholds for Applications

Supported Resources and Metrics

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

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

	2. Rx Packets 3. Packets Dropped	2. Derivative	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

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 the Entire Monitoring Session

To view the health status of a monitoring session:

1. On the Monitoring Session details page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed, click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

This displays the configuration health and traffic health of the monitoring session and also the thresholds applied to that monitoring session.

View Health Status of an Application

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

1. On the Monitoring Session page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

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

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

View Health Status for Individual V Series Nodes

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

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu and then click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session. If the traffic health is not configured for monitoring session or a particular application, the traffic health is displayed as **Not Applicable**.

You can also view the cloud health Status in the Monitoring Session Page, refer to View Health Status on the Monitoring Session Page topic for more detailed information on how to view cloud health status in the Monitoring Session page.

Fabric Health Analytics for Virtual Resources

Fabric Health Analytics (FHA) in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using FHA[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 FHA. Dashboards, Visualizations and Search Objects are called FHA objects. Refer to Fabric Health Analytics topic in *GigaVUE Fabric Management Guide* for more detailed information on Fabric Health Analytics.

Rules and Notes:

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

[1] FHA uses the Kibana front-end application to visualize and analyze the data in the Elasticsearch database of GigaVUE-FM. Kibana is an open source data visualization plugin for Elasticsearch.

Virtual Inventory Statistics and Cloud Applications Dashboard

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

To access the dashboards:

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

The following table lists the various virtual dashboards:

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

Dashboard	Displays	*Visualizations*	Displays
	filters: - Platform - Connection - V Series Node		**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.
		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.

Dashboard	Displays	*Visualizations*	Displays
		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 • VSeries Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the dedup packets received against the dedup application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session**: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V-series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • **V series node**: Management IP of the V Series node. Choose the required V-series node from the drop-down. • **Tunnel:** Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. The following statistics are	*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
	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. By default, the following statistics are displayed: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
		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 Elasticsearch database, which are available only from software version 5.14.00 and beyond.

Sharing the Same Host across Different Monitoring Domains

GigaVUE-FM has the ability to share a host between VMware ESXi and VMware NSX-T monitoring domain. 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. This way the workload virtual machines connected to NSX segments can be monitored using the V Series nodes deployed in NSX-T monitoring domain and workload virtual machines connected to regular VSS / VDS networks can be monitored using the V Series node deployed in the ESXi monitoring domain.

NOTE: If a Virtual Machine has NICs attached to both VMware NSX-T segments and ESXi VDS or VSS port groups then GigaVUE-FM cannot provide visibility to those virtual machines in ESXi platform.

GigaVUE V Series Deployment Clean up

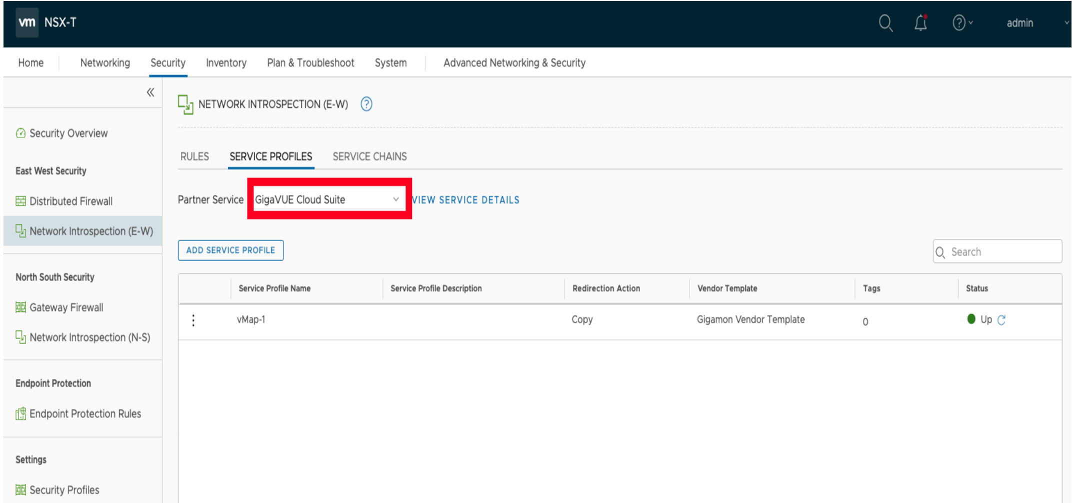
On installation failure or incomplete service removal, you must clean up V Series nodes before reattempting the installation. To clean up the V Series deployments from NSX-T and GigaVUE-FM, perform the following steps:

- Remove Service Profiles
- Remove Service Deployments
- Remove Service Reference
- Remove Service Manager
- Remove Vendor Template and Service Definition

Remove Service Profiles

To remove Service Profiles:

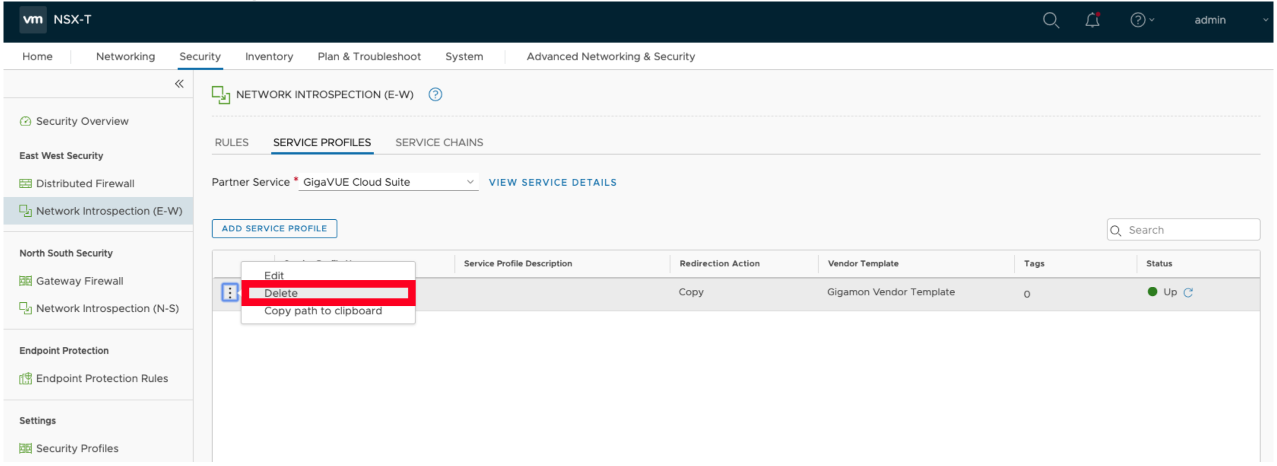
1. From NSX-T Manager, navigate to **Security > Network Introspection (E-W)**.
2. In the **SERVICE PROFILES** tab, select the **GigaVUE Cloud Suite** partner service.



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.



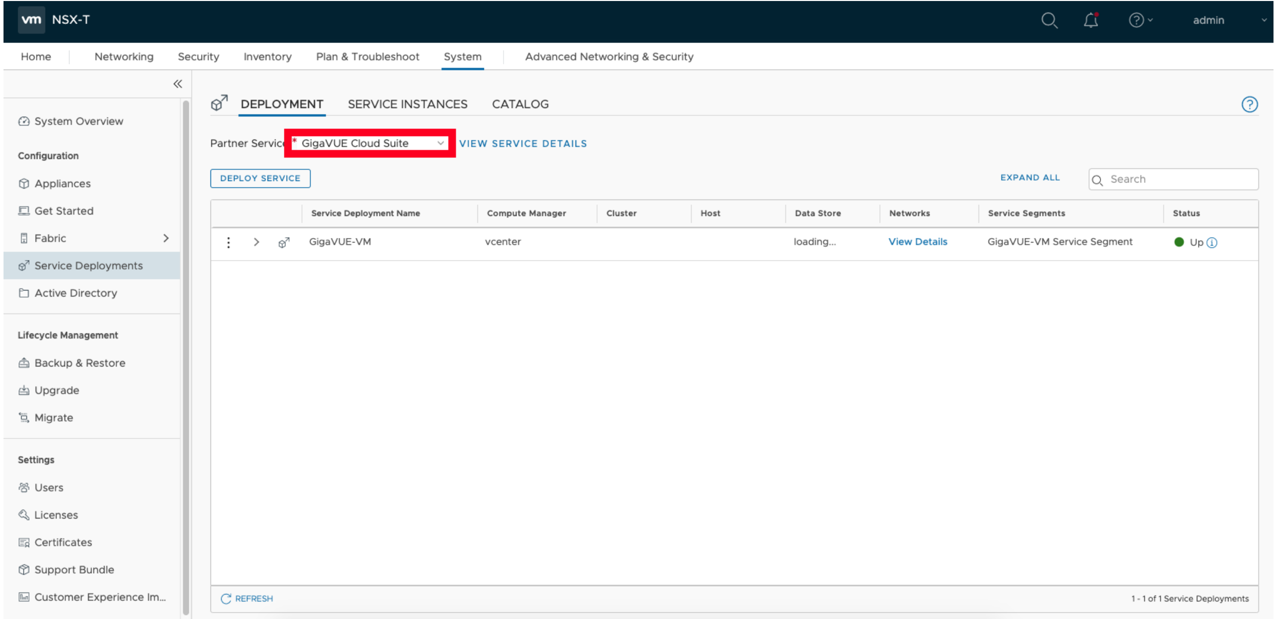
Partner Service * GigaVUE Cloud Suite

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

Remove Service Deployments

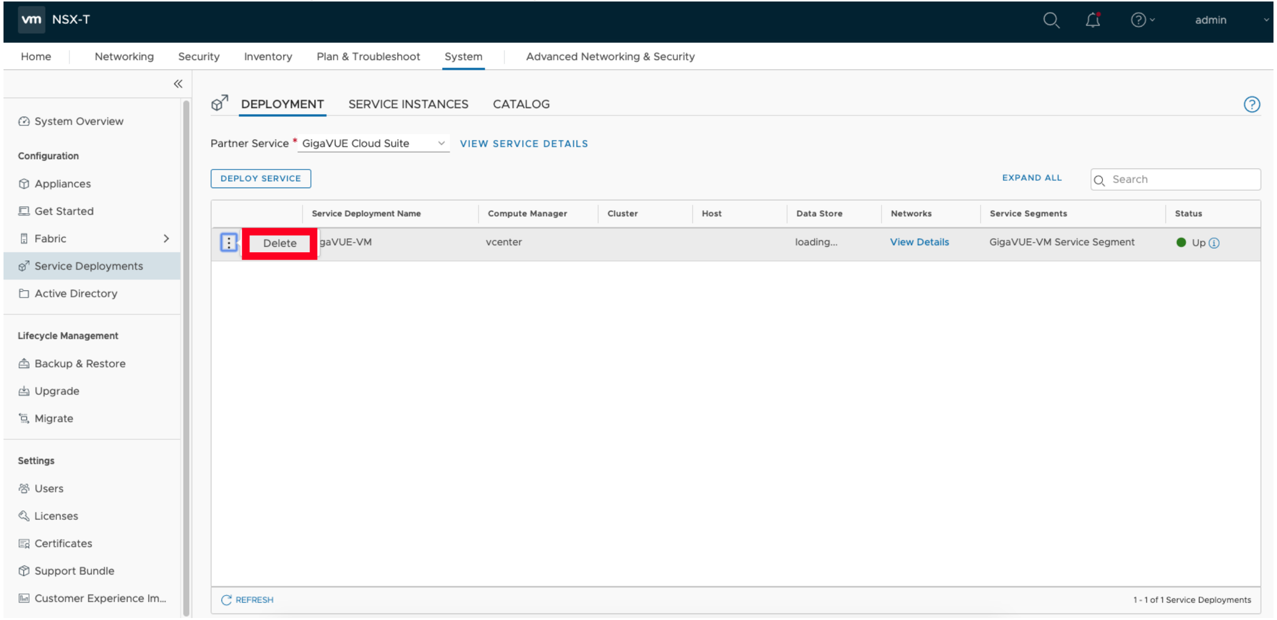
To remove Service Profiles:

1. From NSX-T Manager, navigate to **System > Service Deployments**.
2. In the **DEPLOYMENT** tab, Select the **GigaVUE Cloud Suite** partner service.



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

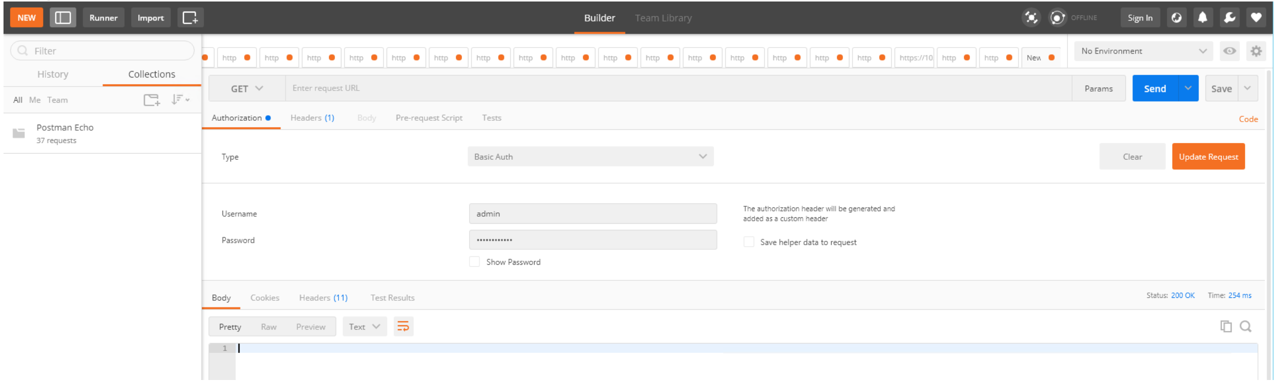
3. Delete all the existing Service Deployments.



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

□ Save helper data to request

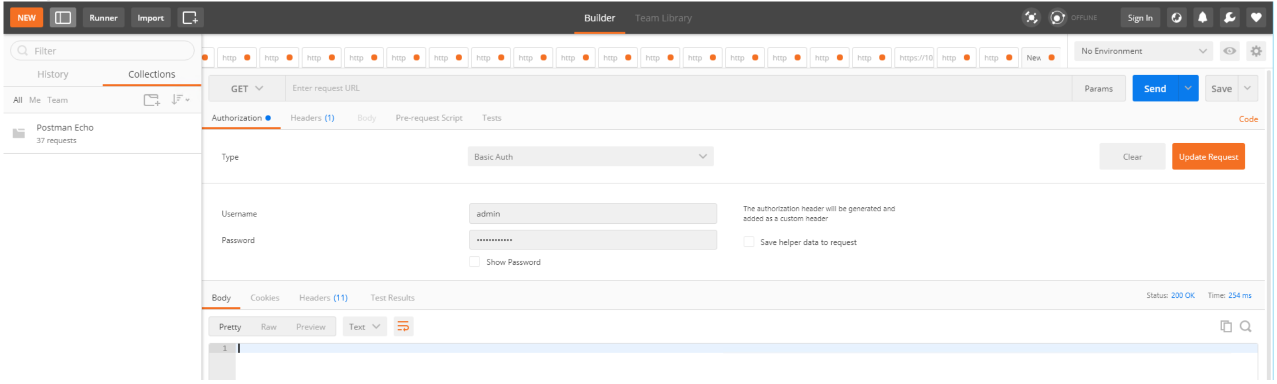
Status: 200 OK Time: 254 ms

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

□ Save helper data to request

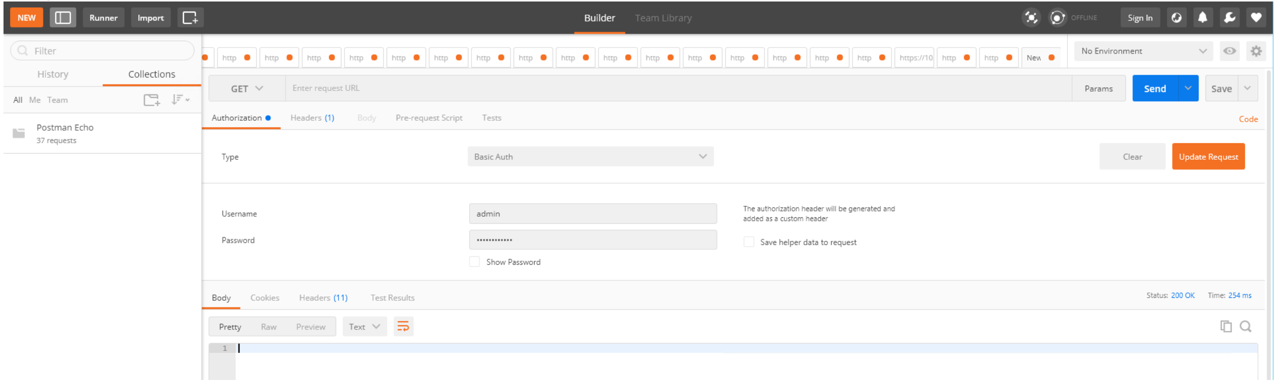
Status: 200 OK Time: 254 ms

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: ••••••••••••

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

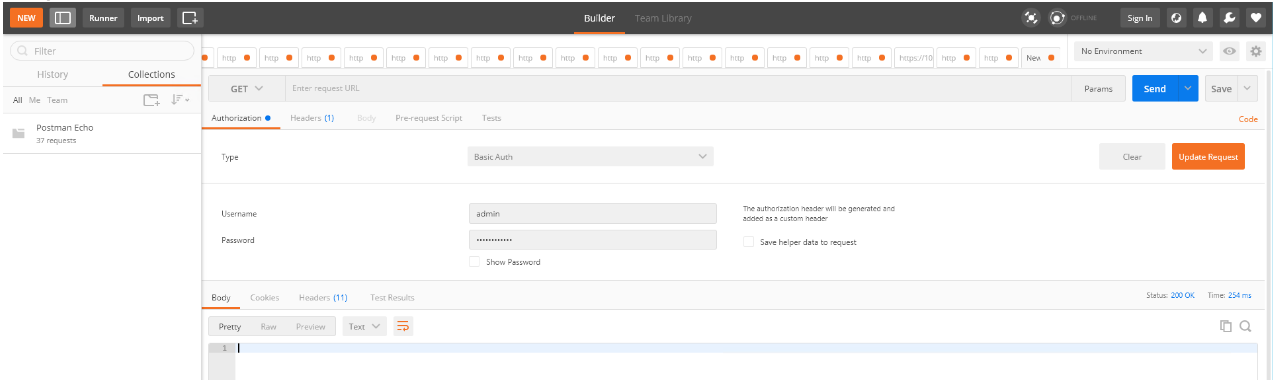
Status: 200 OK Time: 254 ms

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: ••••••••••••

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 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>

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 6.4 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud Tap - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite Deployment Guide - AWS 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 TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & 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 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 site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)