



GigaVUE Cloud Suite for VMware— GigaVUE V Series Guide

GigaVUE Cloud Suite

Product Version: 6.0

Document Version: 1.0

(See Change Notes for document updates.)

Copyright 2022 Gigamon Inc.. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.0	1.0	08/31/2022	The original release of this document with 6.0 GA.

Contents

GigaVUE Cloud Suite for VMware–GigaVUE V Series Guide	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite for VMware–GigaVUE V Series	7
Overview of GigaVUE V Series Node	8
Volume-Based License	8
Base Bundles	8
Add-on Packages	9
How GigaVUE-FM Tracks Volume-Based License Usage	10
Manage Volume-Based License	10
Default Trial Licenses	11
Configure V Series Node on ESXi	13
VMware ESXi System Requirements	14
Network Firewall Requirements	14
Required VMware Virtual Center Privileges	15
Prerequisites for Integrating V Series Nodes with ESXi	16
Recommended Form Factor (Instance Types)	17
Integrate V Series nodes with ESXi	17
Step 1: Upload V Series node Image into GigaVUE-FM	17
Step 2: Connect to VMware vCenter	18
Step 3: Deploy GigaVUE V Series Nodes on VMware ESXi	19
Step 4: Configure Monitoring Sessions	28
Configure Application Intelligence Solutions on GigaVUE V Series Nodes for VMware ESXi	48
Configure Environment	49
Connect to VMware ESXi	50
Create Connection	51
Create Source Selectors	53
Create Tunnel Specifications	55
Configure Application Intelligence Session	57
Fabric Health Analytics for Virtual Resources (BETA)	59
Virtual Inventory Statistics and Cloud Applications Dashboard	59
Configure V Series Node on NSX-T	65
Prerequisites for Integrating V Series Nodes with NSX-T	66

Network Firewall Requirements	66
Recommended Form Factor (Instance Types)	68
Required VMware Virtual Center Privileges	68
Integrate V Series nodes with NSX-T	68
Step 1: Create Users in VMware vCenter and GigaVUE-FM	69
Step 2: Upload V Series node Image into GigaVUE-FM	70
Step 3: Connect to VMware vCenter in GigaVUE-FM	71
Step 4: Create a Service Segment in NSX-T	76
Step 5: Deploy GigaVUE V Series Nodes on VMware NSX-T	76
Step 6: Configure Monitoring Sessions	85
Step 7: Create NSX-T Group and Service Chain	100
Configure Application Intelligence Solutions on GigaVUE V Series Nodes for VMware NSX-T	101
Configure Environment	102
Connect to VMware NSX-T	103
Create Connection	104
Create NSX-T Group and Service Chain	107
Create Tunnel Specifications	107
Configure Application Intelligence Session	109
Fabric Health Analytics for Virtual Resources (BETA)	111
Virtual Inventory Statistics and Cloud Applications Dashboard	111
Remove Gigamon Service from NSX-T and GigaVUE-FM	117
Step 1: Remove the Service Chains	117
Step 2: Delete the Monitoring Session	117
Step 3: Undeploy GigaVUE Cloud Suite - V Series VMs	117
Step 4: Delete the NSX-T Manager and vCenter Connections	117
Cloud Health Monitoring	118
View Monitoring Session Configuration Health	118
Health	119
V Series Node Health	119
Target Source Health	119
View Monitoring Session Statistics	120
View Monitoring Session Diagram	120
Sharing the Same Host across Different Monitoring Domains	121
GigaVUE V Series Deployment Clean up	121
Remove Service Profiles	122
Remove Service Deployments	122
Remove Service Reference	124
Remove Service Manager	124
Remove Vendor Template and Service Definition	125

Additional Sources of Information	126
Documentation	126
How to Download Software and Release Notes from My Gigamon	128
Documentation Feedback	129
Contact Technical Support	130
Contact Sales	130
Premium Support	131
The Gigamon Community	131
Glossary	132

GigaVUE Cloud Suite for VMware–GigaVUE V Series

GigaVUE Cloud Suite GigaVUE V Series 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 V Series Node](#)
- [Configure V Series Node on ESXi](#)
- [Configure V Series Node on NSX-T](#)

Overview of GigaVUE V Series Node

A V Series node is a virtual machine running in your infrastructure that processes and distributes network traffic. It plays the same role as an H Series appliance in a physical deployment, running many of the same GigaSMART applications and feeding data to tools in a similar manner. V Series nodes reside in a virtualized environment. The outbound traffic is tunneled and the inbound traffic can be in the form of raw packets or can be tunneled (because there are no physical device ports).

Volume-Based License

All the V Series 2 nodes connected to GigaVUE-FM periodically reports statistics on the amount of traffic that flows through the V Series Nodes. The statistics give information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility into the actual amount of data, each licensed application is using on each node, and track the overuse if any. Volume-based licensing has 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

GigaVUE-FM has the following three base bundles:

- SecureVUEPlus (highest)
- NetVUE (intermediate)
- CoreVUE (lowest)

There are two types of base bundle SKUs available:

- Term Based
- Perpetual

The number in the SKU indicates the total volume allowance of the SKU. For example, VBL-250T-BN-CORE-PL has a volume allowance of 250 terabytes.

Bundle Replacement Policy

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.

There are two types of add-on SKU available:

1. **Term Based:** These add-on SKUs expire after a limited period of time.

The list of the available term based SKUs:

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

2. **Perpetual:** These add-on SKUs never expires.

The list of the available perpetual SKUs:

- VBL-250T-ADD-5GC-PL
- VBL-2500T-ADD-5GC-PL

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.
- When a license goes into grace period, you will be notified, along with a list of monitoring sessions that would be affected after the expiry of the grace period.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will be undeployed, but not deleted from the database.
- When a license is renewed or newly imported, the undeployed monitoring sessions will be redeployed.

Manage Volume-Based License

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 information like SKUs, Bundles, Start date, End date, Type, and Activation ID of the Volume-Based Licenses that are active. The expired licenses are automatically moved to the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar.

Click on the individual SKU to view the list of applications available for that particular SKU.

Use the following buttons to manage your active VBL.

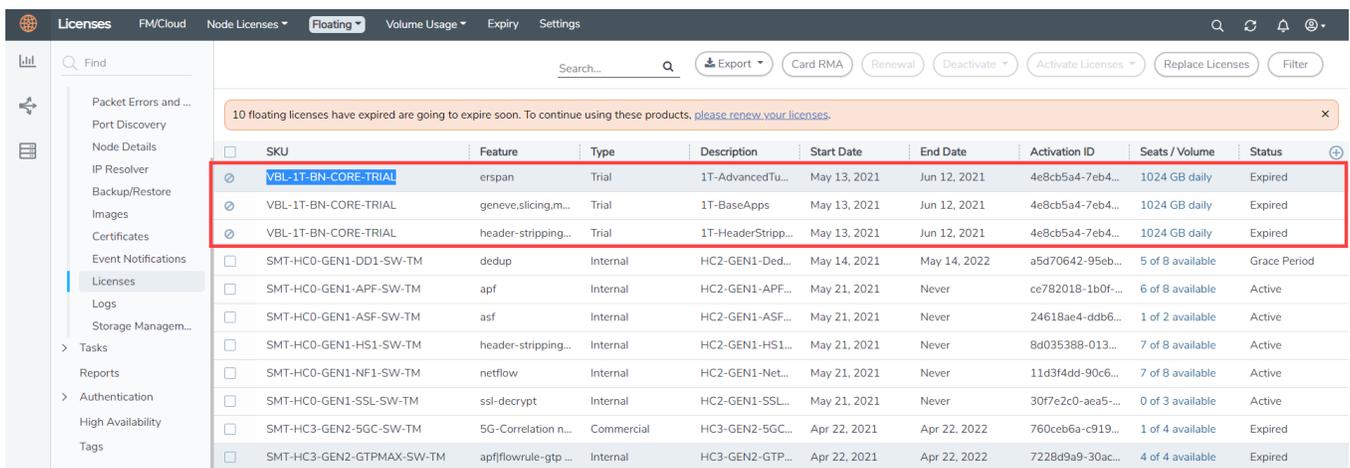
Button	Description
Activate Licenses	Use this button to activate a Volume-Based License. Refer Activate Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this option to narrow down the list of active Volume-Based Licenses 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.

For more detailed information on dashboards and reports generation for Volume-Based Licensing refer 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

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).



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	apfflowrule-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 V series 2.0 nodes.

To deactivate the trial VBL refer to [Delete Default Trial Licenses](#) section for details.

Configure V Series Node on ESXi

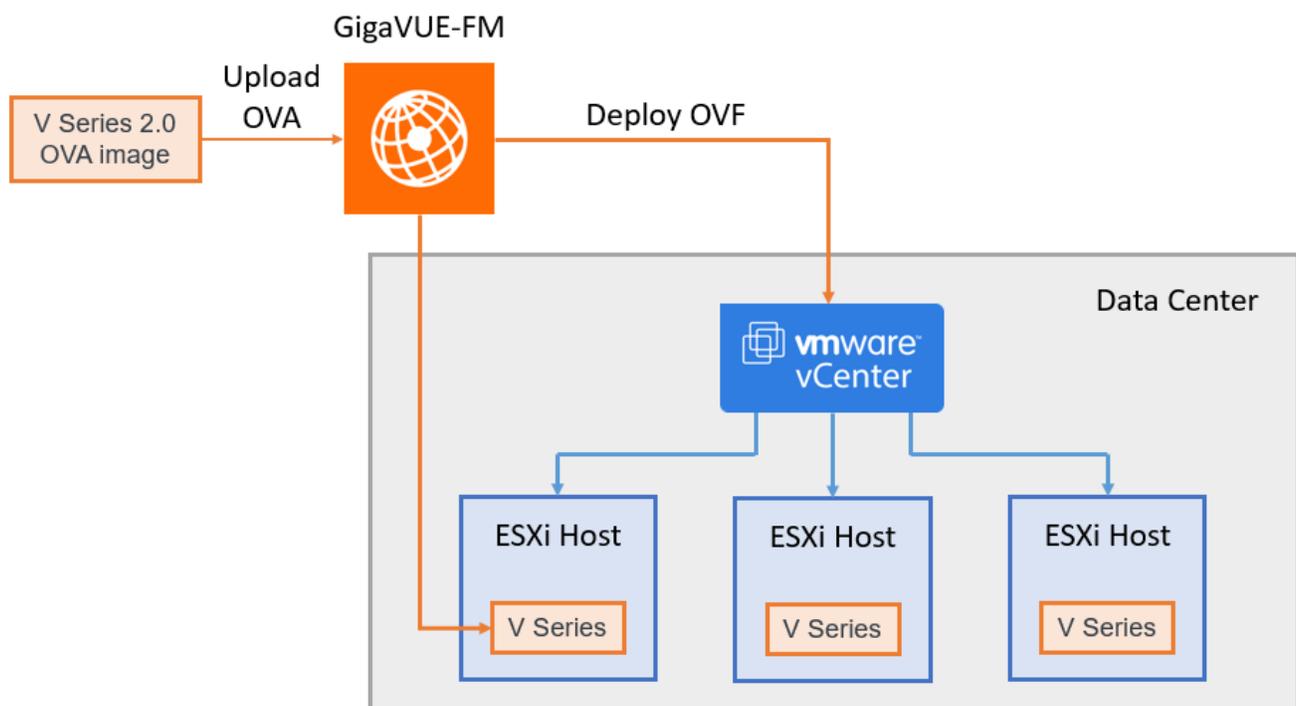
This document provides an overview of the V Series fabric node deployment on the VMware ESXi platforms and describes the procedure for setting up the traffic monitoring sessions using the V Series fabric nodes. The V Series fabric nodes support traffic visibility on the following VMware networking elements:

- vSphere standard switch
- vSphere distributed switch

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

NOTE: 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.

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



The chapter includes the following major sections:

- [Prerequisites for Integrating V Series Nodes with ESXi](#)
- [Integrate V Series nodes with ESXi](#)

NOTE: These steps assume that VMware ESXi is installed and configured.

Refer [Deploying GigaVUE Cloud Suite on VMware vCenter in a multi-tier DC Environment](#) for more detailed information.

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 V Series 2 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	V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with V Series node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	

Remote Source	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 V Series nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
V Series Nodes	Tool/ HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows V Series node to communicate and tunnel traffic to the Tool
			N/A	IP 47	GRE	
V Series Nodes	Tool/ HC Series instance	N/A	N/A	ICMP	Echo Request	Allows V Series node to health check tunnel destination traffic (Optional)
					Echo Response	

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 <ul style="list-style-type: none"> Network Configuration 	VSS Tapping
	Inventory	Pin V Series Node to the host in cluster

Category	Required Privilege	Purpose
	<ul style="list-style-type: none"> Modify 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 resource pool	V Series Node Deployment
vApp	Import vApp instance configuration	V Series Node Deployment V Series Node Deployment
Virtual machine	Configuration <ul style="list-style-type: none"> Add new disk Add or remove device Modify device settings Rename 	V Series Node Deployment V Series Node Deployment/VSS Tapping
	Interaction <ul style="list-style-type: none"> Connect devices Power on Power Off 	V Series Node Deployment V Series Node Deployment V Series Node Deployment
	Inventory <ul style="list-style-type: none"> Create from existing Remove 	V Series Node Deployment V Series Node Deployment
	Provisioning <ul style="list-style-type: none"> 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:

- VMware vCenter ESXi Standard Version must be 6.7 u3, and 7.0.
- 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.
- V Series 2 device OVA image file.
- All the target VMs must have VMware guest tools or Open VM tools if you use IP based filtering.
- Port 8889 must be available for GigaVUE-FM to access V Series nodes.

- TCP Port 443 must be open between the GigaVUE-FM instance and the ESXi host to upload the OVA files.

The V Series 2 Node OVA image files can be downloaded from [Gigamon Customer Portal](#).

Recommended Form Factor (Instance Types)

The form factor (instance) size of the V Series 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 V series node. Instance sizes can be different for 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		

Integrate V Series nodes with ESXi

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

- [Step 1: Upload V Series node Image into GigaVUE-FM](#)
- [Step 2: Deploy V Series nodes on VMware ESXi](#)
- [Step 4: Configure Monitoring Sessions](#)

Step 1: Upload V Series node Image into GigaVUE-FM

To upload the V Series image into GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > Settings**. The **Settings** page appears.
2. In the Settings page, click **OVA Files** tab.

Settings Advanced OVA Files Delete

Select an OVA file to upload Browse Upload to Server

<input type="checkbox"/>	Name	Type	Version
<input type="checkbox"/>	gigamon-gigavue-vseries-node-2.1.0-237319_am...	V SERIES_NODE	2.1.0
<input type="checkbox"/>	gigamon-gigavue-vseries-node-2.1.1-238809_am...	V SERIES_NODE	2.1.1
<input type="checkbox"/>	gigamon-gigavue-vseries-node-2.1.1-239018_am...	V SERIES_NODE	2.1.1

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

Step 2: Connect to VMware vCenter

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 V Series node.

To configure VMware vCenter in GigaVUE-FM:

1. In GigaVUE-FM, from the left navigation pane, select **Inventory > VIRTUAL > VMware > Monitoring Domain**. The Monitoring Domain page appears.
2. On the **Monitoring Domain** page, click **New**. The **VMware Configuration** page appears.

The screenshot shows the 'VMware Configuration' page in GigaVUE-FM. The page has a dark header with 'VMware > Monitoring Domain' and search, refresh, and notification icons. Below the header is a light gray sidebar with a navigation menu. The main content area contains a form with the following fields:

- Monitoring Domain***: Enter a monitoring domain name
- Connection Alias***: Alias
- Virtual Center***: Virtual Center
- Username***: Username
- Password***: Password
- Traffic Acquisition Method**: Select traffic acquisition method type...
- Setup NSX-T**: No (toggle switch)

Buttons for 'Save' and 'Cancel' are located in the top right corner of the form area.

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. NOTE: When using OGW application select the traffic acquisition Method as None.
Setup NSX-T	Enable to setup NSX-T and the fields of NSX-T to appear. Refer to Configure V Series Node on NSX-T for detailed information.

4. Click **Save**.

Step 3: Deploy GigaVUE V Series Nodes on VMware ESXi

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

GigaVUE V Series Nodes can be deployed on VMware ESXi in two ways. You can either directly use VMware ESXi host system to deploy your GigaVUE 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 ESXi Host](#)

Deploy GigaVUE V Series Nodes using GigaVUE-FM

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 **Fabric** and then select **Deploy Fabric** from the drop-down. The **VMware Fabric Launch Configuration** page appears.

The screenshot shows the VMware Fabric Launch Configuration interface. The breadcrumb navigation at the top reads "VMware > Monitoring Domain". The page title is "VMware Fabric Launch Configuration". On the right side of the header, there are icons for search, refresh, notifications, and user profile. Below the header, there are "Deploy" and "Cancel" buttons. The main configuration area includes the following fields:

- Datacenter***: A dropdown menu with "Systest_DC" selected.
- Cluster**: A dropdown menu with "Select a cluster..." selected.
- V Series Node Image***: A dropdown menu with "gigamon-gigavue-vseries-node-2.5.0-314690_amd64.ova" selected.
- Form Factor***: A dropdown menu with "Small, 2vCPU, 4GB RAM, 8GB Disk" selected.
- Hosts***: Two radio buttons: "Import Host Info from File" (selected) and "Add Host Info Manually". Below these are instructions: "a) Download this csv file as a template. Fill in the information for your hosts." and "b) After you've filled out csv file above, go ahead and import that file." A "Browse" button is located below the instructions.

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

Field	Description
Datacenter	vCenter Data Center with the ESXi hosts to be provisioned with V Series nodes
Cluster	Cluster where you want to deploy V Series nodes
Hosts	<p>Select the ESXi hosts for V Series deployment.</p> <p>Select Import Host Info from file or Add Host Info Manually.</p> <p>Import Host Info from file:</p> <p>To import host details from a .csv file:</p> <ol style="list-style-type: none"> Download the .csv template file. Enter the required values in the Excel sheet and save the file. Click Browse and select the .csv file saved in the previous step. <p>Add Host Info Manually:</p> <p>Select the ESXi hosts for V Series deployment.</p> <p>The Common Configuration drop-down wizard appears. Select the Datastores or Datastore Clusters and enter the required values. Click Apply to all to apply the selected values to all the selected hosts.</p> <p>Select the IP type as Static if you wish to deploy a node using a Static IP address.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: The Tunnel Gateway IP field is optional.</p> </div>

Field	Description
	<div style="border: 1px solid #ccc; padding: 10px;"> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <p>▼ Common Configuration</p> </div> <div style="display: flex; justify-content: flex-end; margin-bottom: 10px;"> <input checked="" type="radio"/> Datastores <input type="radio"/> Datastore Clusters </div> <div style="margin-bottom: 10px;"> <p>Datastore Select a datastore... ▾</p> </div> <div style="margin-bottom: 10px;"> <p>V Series Node Name Prefix V Series -</p> </div> <div style="margin-bottom: 10px;"> <p>V Series Node Name Suffix _____</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Management</p> <p>Network* Select a switch or port group... ▾</p> <p>IP Type Select IP type... ▾</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p>Tunnel</p> <p>Network* Select a switch or port group... ▾</p> <p>IP Type DHCP ▾</p> <p>Gateway IP* _____</p> <p>CIDR* _____</p> <p>Use IPv6 <input type="checkbox"/> No</p> </div> <div style="margin-bottom: 10px;"> <p>Virtual Disk Format Thin Provision ▾</p> </div> <div style="margin-bottom: 10px;"> <p>Deployment Folder /</p> </div> <div style="margin-bottom: 10px;"> <p>User Password* (<i>gigamon</i>) _____</p> </div> </div>
V Series Node Image	Select the OVA file uploaded in the Step 1: Upload V Series node Image into GigaVUE-FM , from the drop-down menu.
Form Factor	Instance size of the V Series node. Refer Prerequisites for Integrating V Series Nodes with ESXi for more information.

- 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.

Deploy GigaVUE V Series Nodes using VMware ESXi Host

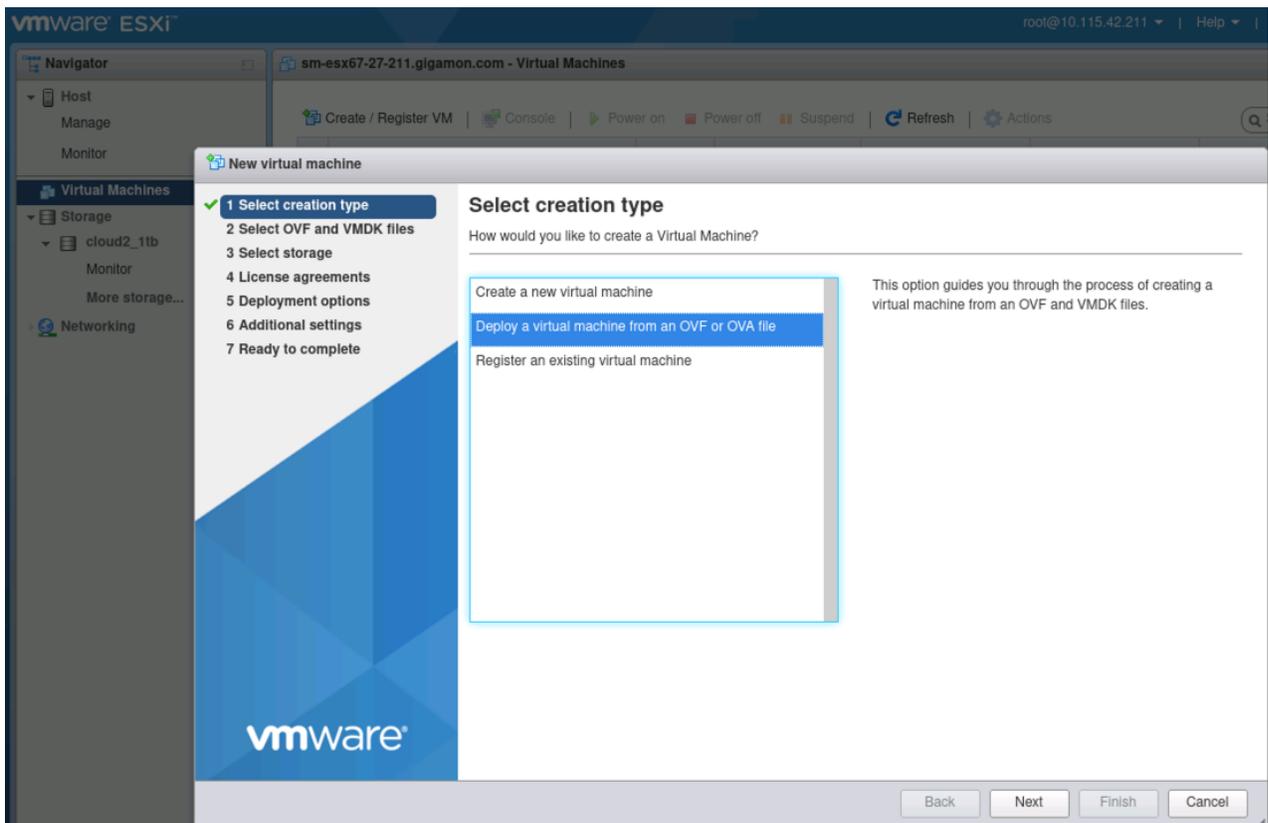
You can use your own VMware ESXi host system to deploy GigaVUE V Series nodes and use GigaVUE-FM to configure the advanced features supported by these nodes. These nodes register themselves with GigaVUE-FM using the information provided by the user in the virtual machine creation wizard. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

This section describes how to deploy GigaVUE V Series Nodes under AnyCloud Monitoring Domain using VMware ESXi Host.



- The nodes will be deployed under the Monitoring Domain created in AnyCloud.
- When registering GigaVUE V Series nodes in GigaVUE-FM, the connection name under each monitoring domain must be unique.

1. Login to VMware ESXi host using your web browser.
2. On the left navigation pane, select Virtual Machines and click **Create/Register VM**. The New Virtual Machine dialog box appears.



3. On the **Select Creation Type** page, select **Deploy a Virtual Machine from an OVF or OVA file**.
4. The **Select OVF and VMDK files or Select OVA file** page appears. Provide a name for the Virtual machine. Upload the OVF and VMDK files. Click Next.



When deploying GigaVUE V Series Nodes using VMware ESXi,

- you cannot use OVA files.
- you must only select any of the following OVF files:
 - a. files vseries-node-file7.ovf (Small form factor)
 - b. files vseries-node-file8.ovf (Medium form factor)
 - c. files vseries-node-file9.ovf (Large form factor)

5. Then, the **Select Storage** page appears, select the storage type and data store. Click Next.
6. Under the **Deployment Options**, provide the necessary details given below.
 - a. Select the network port group associated with the host, network ports and tunneling port details from the **Network Mappings** drop-down.
 - b. Select Thick/Thin from the **Disk provisioning** field.
 - c. Select **Management Port DHCP** from the **Deployment type** drop-down.
 - d. (optional) Enable the **Power on automatically** check-box to power on the Virtual Machine automatically.

7. Under the additional settings page, provide the user data as shown in the figure.

Additional settings	
Additional properties for the VM	
Options	
Hostname	vseries-node-51301
Administrative Login Password	*****
Administrative Login Password confirm	*****
Administrative Login Public Key	
Oauth Login Public Key	
Management Port DHCP	<input checked="" type="checkbox"/>
Management Port IP Address	
Management Port IP Netmask	
Management Port IP Gateway	
Tool Port DHCP	<input type="checkbox"/>
Tool Port IP Address	
Tool Port IP Netmask	
Tool Port IP Gateway	
GroupName	ssi-md
SubGroupName	ssi-vpc
User	orchestration
Password	*****
Password confirm	*****
RemoteIP	10.10.10.10
RemotePort	443

Enter the following values in the additional settings:

- Hostname: <Host Name>
- Administration Password: <Your Password>
- GroupName: <Monitoring domain name>
- SubGroupName: < Connection name>
- User: Description: orchestration
- Password: orchestration123A!
- remoteIP: <IP address of the GigaVUE-FM>
- remotePort: 443

8. Review the setting selection in the **Ready to Complete page**, then click Finish.

The V Series Node deployed in VMware ESXi host appears in AnyCloud Monitoring Domain page of GigaVUE-FM.

Monitoring Domain	Connections	Name	Management IP	Type	Version	Status
MD1	Connection1		10.115.182.94	V Series Node	2.6.0	Connected
			10.115.182.94	V Series Node	2.6.0	Ok
MD2	Connection2		10.115.182.23	V Series Node	2.6.0	Connected
			10.115.182.23	V Series Node	2.6.0	Ok

Upgrade V Series Node in GigaVUE-FM

To upgrade V Series Node in GigaVUE-FM:



Before upgrading the V Series Nodes, ensure the following:

- All the current V Series nodes are of same version.
- Latest V Series Node OVA image must be uploaded to GigaVUE-FM. Refer to [Step 1: Upload V Series node Image into GigaVUE-FM](#) for detailed information.

1. In GigaVUE-FM, on the left navigation pane, select **Inventory > VIRTUAL > VMware > Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select a deployed monitoring domain and click **Fabric**. From the drop-down list, select **Upgrade Fabric**, the **V Series Node Upgrade** dialog box appears.
The V Series Node Upgrade dialog box displays the current version of the V Series Node image. Select the latest V Series Node OVA image from the Image drop-down list. If you want to modify the form factor (instance) size, click the **Change Form Factors** check box. When you are upgrading more than one V Series node, you can modify the form factors of each V Series nodes individually using the drop-down list.

V Series Node Upgrade

Current Version	2.3.0
Image	Select an Image... ▾
Change Form Factors	<input checked="" type="checkbox"/>
V Series Node	Form Factor
VSeries-vp-ind-node-10-115-41-76	Medium, 4vCPU, 8GB RAM, 8GB Disk ▾
VSeries-vp-ind-node-10-115-41-77	Small, 2vCPU, 4GB RAM, 8GB Disk ▾

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

3. Enter the required information for all the available V Series nodes and click **Upgrade** to launch the 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	Connection	Name	Management IP	Type	Version	Status
iron-md						Upgrade in progress
		iron-md				Connected
		VSeries-up-demo-static-10-115-41-77	10.115.44.232	V Series Node	2.3.1	upgrading
		VSeries-up-demo-static-10-115-41-76	10.115.44.234	V Series Node	2.3.1	upgrading
		VSeries-up-demo-static-10-115-41-77-upgrade		V Series Node	2.3.2	launching
		VSeries-up-demo-static-10-115-41-76-upgrade		V Series Node	2.3.2	launching

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:

Summary

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

Node Statuses

Node	Status
VSeries-up-demo-static-10-115-41-77-upgrade	launching
VSeries-up-demo-static-10-115-41-76-upgrade	launching

Close

- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.
- If the V Series Node Upgrade failed or interrupted for any reason, under **Fabric** drop-down click **Continue Fabric Upgrade** to continue the V Series Node upgrade process.

NOTE: You cannot modify the form factor or the V Series image when you are using the **Continue Fabric Upgrade** option. GigaVUE-FM uses the same values defined in the initial fabric upgrade configuration.

Step 4: Configure Monitoring Sessions

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:

- 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](#)
- [Create a New Map](#)
- [Add Applications to Monitoring Session](#)
- [To deploy the 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

Monitoring Domain

Connection Select All Select None

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.

Create Ingress and Egress Tunnel

Traffic from the V Series 2 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 **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table.

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.
Traffic Direction	The direction of the traffic flowing through the V Series node. <ul style="list-style-type: none"> • Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node. 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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> • ERSPAN, L2GRE, UDPGRE, 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. </div>
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**.

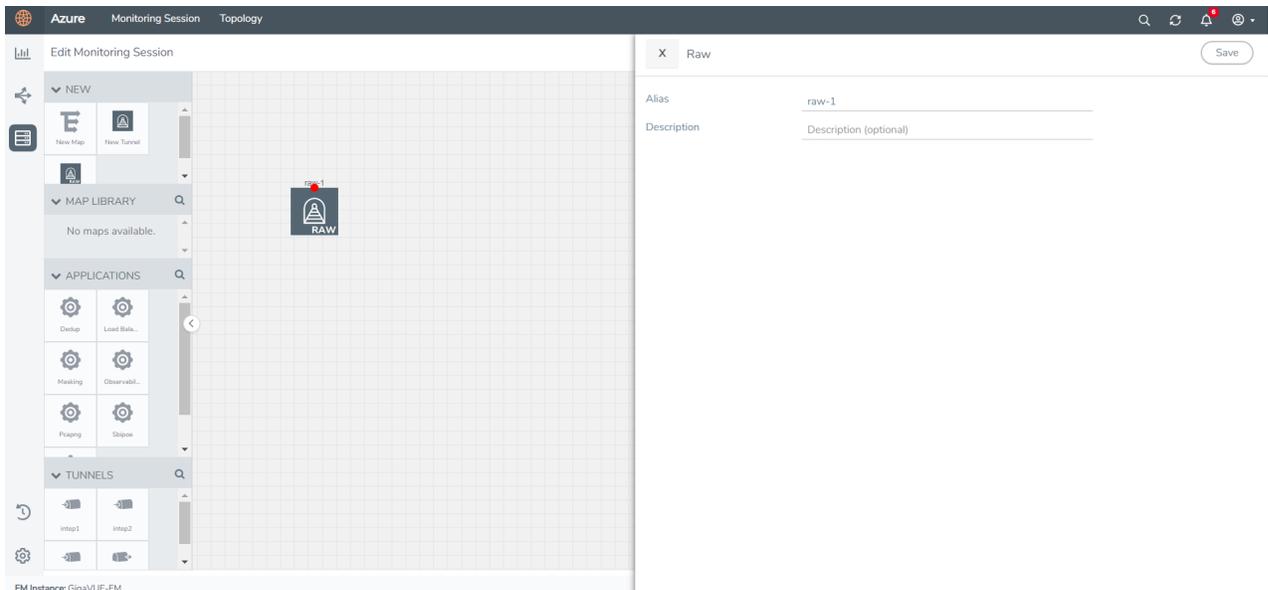
To delete a tunnel, select the required tunnel and click **Delete**.

Create Raw Endpoint

Raw End Point (REP) is used to pass traffic from an interface. 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**.



4. To deploy the monitoring session after adding the Raw Endpoint click the **Deploy** button in 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**.

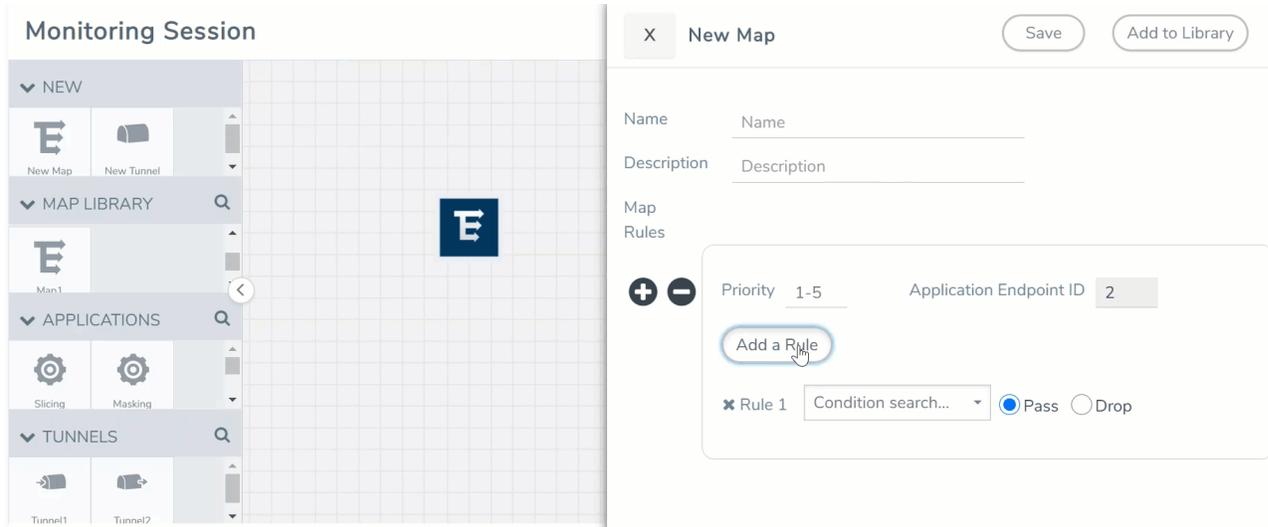
Create a New Map

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 detailed information on GigaVUE-FM licenses, refer to "Licenses" section in the *GigaVUE Administration Guide*.

To create a new map:

1. After creating a new monitoring session, or click **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.



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
Comments	Description of the map
Map Rules	<p>The rules for filtering the traffic in the map. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add multiple rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. A rule set can have only 5 rules per map and 25 conditions per map. To add ATS rules for an Inclusion/Exclusion map, you must select atleast one rule condition.</p> <p>To add a map rule:</p> <ol style="list-style-type: none"> Enter a Priority value from 1 to 5 for the rule with 5 being the highest and 1 is the lowest priority. Click Add a Rule. The new rule field appear for the Application Endpoint. Select a required condition from the drop-down list. Select the rule to Pass or Drop through the map. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> If two rules with same condition are configured as pass and drop,</p> <ul style="list-style-type: none"> on a same tunnel endpoint, the traffic filtering precedence will be based on the priority value. on two different tunnel endpoints, the traffic will be passed or dropped to the respective tunnel endpoints. <p>For detailed information on filtering fragmented and unfragmented packets, refer to "GigaSMART Adaptive Packet Filtering (APF)" section on the <i>GigaVUE Fabric Management Guide</i>.</p> </div>



- 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. 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**.
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.

Add Applications to Monitoring Session

GigaVUE Cloud Suite with GigaVUE V Series 2 node supports the following GigaSMART applications in the GigaVUE-FM canvas:

- [Slicing](#)
- [Masking](#)
- [Dedup](#)
- [Load Balancing](#)
- [PCAPng](#)
- [Observability Gateway Application](#)

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*.

For the detailed list of GigaSMART Operation supported for V Series 2 nodes, refer to "Supported GigaSMART Operation" topic in the *GigaVUE Fabric Management Guide*.

You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools. Refer to the [Volume Based License \(VBL\)](#) section for more information on Licenses for using V Series 2 Nodes.

To add a GigaSMART application:

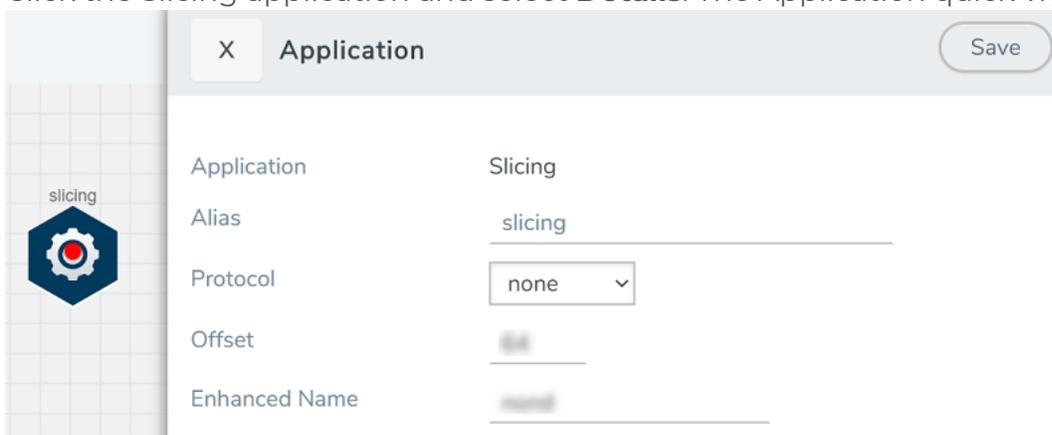
1. Drag and drop an application from **APPLICATIONS** to the canvas.
2. In the canvas, click the application and select **Details**.
3. Enter or select the required values for the selected application and click **Save**.

Slicing

Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. For detailed information on Slicing, refer to [GigaSMART Packet Slicing](#)"GigaSMART Packet Slicing" topic in the *GigaVUE Fabric Management Guide*.

To add a slicing application:

1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.
2. Click the Slicing application and select **Details**. The Application quick view appears.



Application	Slicing
Alias	slicing
Protocol	none
Offset	0
Enhanced Name	none

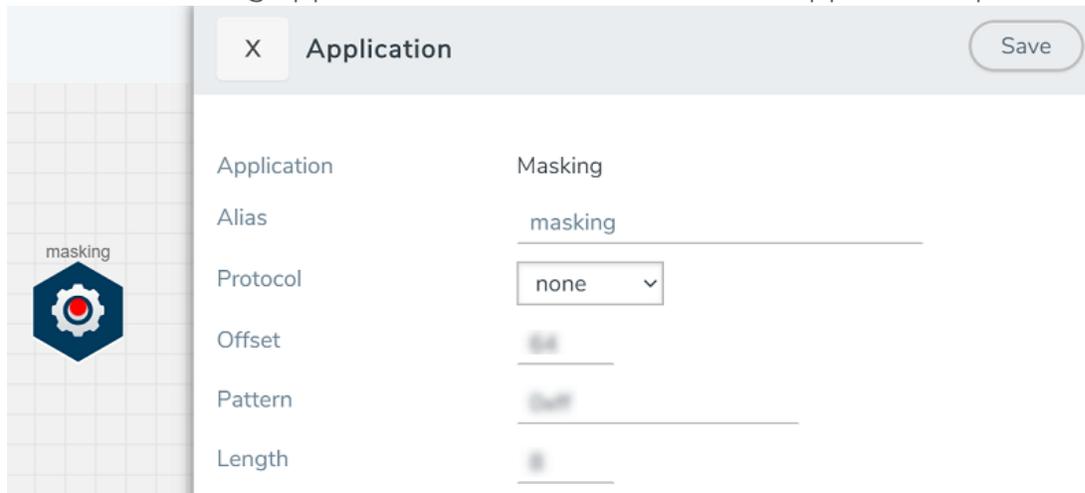
3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the slicing.
 - From the **Protocol** drop-down list, specify an optional parameter for slicing the specified length of the protocol.
 - In the **Offset** field, specify the length of the packet that must be sliced.
 - In the **Enhanced Name** field, enter the Enhanced Slicing profile name.
4. Click **Save**.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. For detailed information on masking, refer to [GigaSMART Masking](#)"GigaSMART Masking" topic in the *GigaVUE Fabric Management Guide*.

To add a masking application:

1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.
2. Click the Masking application and select **Details**. The Application quick view appears.



Application	Masking
Alias	masking
Protocol	none
Offset	
Pattern	
Length	

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the masking.
 - From the **Protocol** drop-down list, specify an optional parameter for masking the specified length of the protocol.
 - In the **Offset** field, specify the length of the packet that must be masked.
 - In the **Pattern** field, enter the pattern for masking the packet.
 - In the **Length** field, enter the length of the packet that must be masked.
4. Click **Save**.

Dedup

De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment. For detailed information on de-duplication, refer to [GigaSMART De-Duplication](#) "GigaSMART De-Duplication" topic in the *GigaVUE Fabric Management Guide*.

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.

The screenshot shows a modal window titled 'Application' with a close button (X) and a 'Save' button. The window displays configuration details for the 'Dedup' application. On the left, there is a sidebar with a 'dedup' icon. The main area contains the following fields:

Field	Value
Application	Dedup ⓘ
Alias	dedup
Action	<input type="radio"/> Count <input checked="" type="radio"/> Drop
IP Tclass	<input checked="" type="radio"/> Include <input type="radio"/> Ignore
IP TOS	<input checked="" type="radio"/> Include <input type="radio"/> Ignore
TCP Sequence	<input checked="" type="radio"/> Include <input type="radio"/> Ignore
VLAN	<input type="radio"/> Include <input checked="" type="radio"/> Ignore
Timer	50000

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the de-duplication.
 - In the Action field, select **Count** or **Drop** the detected duplicate packets.
 - For **IP Tclass**, **IP TOS**, **TCP Sequence**, and **VLAN** fields, select **Include** or **Exclude** the packets for de-duplication.
 - In the **Timer** field, enter the time interval (in seconds) for de-duplicating the packet.
4. Click **Save**.

Load Balancing

Load balancing app performs stateless distribution of the packets between different endpoints. For detailed information on load balancing, refer to [GigaSMART Load Balancing](#)"GigaSMART Load Balancing" topic in the *GigaVUE Fabric Management Guide*.

To add a load balancing application:

1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
2. Click the load balancing application and select **Details**. The Application quick view appears.

The screenshot shows the 'Application' quick view for a 'Load Balancing' application. The interface includes a grid on the left with a 'lb' application icon. The main panel is titled 'Application' and contains the following fields:

- Application:** Load Balancing
- Alias:** lb
- Hash Fields:** ipOnly (dropdown)
- Field Location:** outer (dropdown)
- Load balancing groups:** A section with a '+' and '-' button, and a table with columns for Application Endpoint ID (2) and Weight (1-100).

A 'Save' button is located in the top right corner.

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the load balancing app.
 - For **Hash Fields** field, select a hash field from the list.
 - **ipOnly**—includes Source IP, and Destination IP.
 - **ipAndPort**—includes Source IP, Destination IP, Source Port , and Destination Ports.
 - **fiveTuple**—includes Source IP, Destination IP, Source Port, Destination Port, and Protocol fields.
 - **gtpuTeid**—includes GTP-U.
 - For **Field location** field, select **Inner** or **Outer** location.

NOTE: Field location is not supported for **gtpuTeid**.

- In the **load balancing groups**, add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

4. Click **Save**.

PCAPng

The PCAPng application is a GigaSMART parser application that reads the various blocks in the received PCAPng files and validates the blocks to be sent to the destination application or to the tools.

NOTE: The PCAPng application is only applicable for the Ericsson 5G Core vTAP architecture. Refer to "PCAPng Application" topic in the *GigaVUE Fabric Management Guide* for detailed information.

Create Link Between UDP-in-GRE Tunnel and PCAPng Application

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. 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 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> NOTE: Do not enter spaces in the alias name. </div>
Description	The description of the tunnel endpoint
Type	Select UDPGRE as the tunnel type
Traffic Direction	The direction of the traffic flowing through the V Series node <ul style="list-style-type: none"> • Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6
Remote Tunnel IP	The IP address of the tunnel source
Key	GRE key value
Source L4 Port	Layer 4 source port number
Destination L4 Port	Layer 4 destination port number. You can configure only 4754 or 4755 as the destination UDP ports

3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

Create a link with source as PCAPng application and destination as one of the following:

- Other GigaSMART applications such as Slicing, Masking, etc.
- Other encapsulation TEPs.
- REP/MAP

Refer to the following image for a sample configuration.

Observability Gateway Application

Observability Gateway (OGW) application is used to convert Application Metadata Intelligence (AMI) output (CEF) into JSON format that can be exported to other tools. Refer Application Intelligence—Observability Gateway Application topic in *GigaVUE Fabric Management Guide* for more conceptual information and the entire workflow.

Rules and Pre-requisites:

Prerequisites to follow when creating a monitoring domain and deploying V Series node:

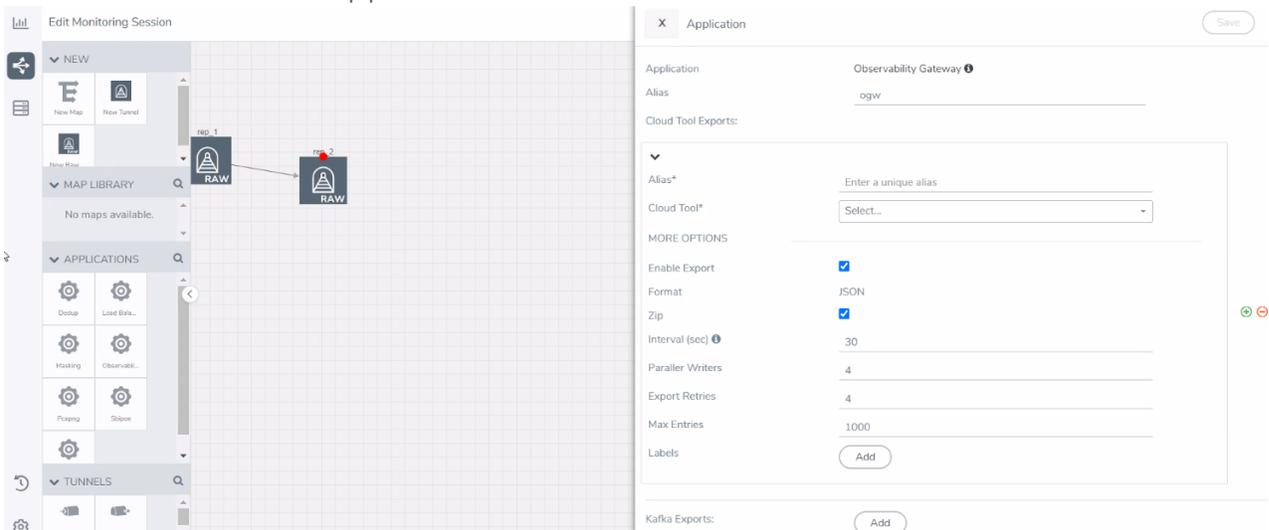
- Select **Traffic Acquisition Method** as None. Refer [Step 2: Deploy V Series nodes on VMware ESXi](#) for more detailed information on how to create a monitoring domain and deploy V Series nodes.
- After deploying the V Series node in the monitoring domain, click on the V Series Node's Name, and the V Series node quick view opens. Choose a data IP to which you wish to send CEF packets, then use the IP address of this data IP as the **Tool IP Address** when creating the Application Metadata Intelligence solution. Refer to Create Metadata Intelligence by Editing Monitoring Session from Dashboard topic in the *GigaVUE Fabric Management Guide* on how to configure AMI for OGW application.
- The V Series node deployed must be entirely dedicated to the OGW application, it cannot have other applications with it.
- When deploying this application in VMware NSX-T, create a monitoring domain with the **Setup NSX-T** toggle button disabled. Even if your V Series node is a part of VMware NSX-T host, you can still deploy it in VMware ESXi monitoring domain. Refer to [Sharing the Same Host across Different Monitoring Domains](#) for more detailed information on how to share a host between nodes in VMware ESXi and VMware NSX-T monitoring domain.

Rules to follow when using the OGW application:

- The monitoring session can only have Raw End Point (REP), it cannot have other applications, maps, or tunnels when using the OGW application. Refer [Create Raw Endpoint](#) for more detailed information on how to add a REP to the monitoring session and how to configure it.

To add OGW application:

1. Drag and drop **Observability Gateway** from **APPLICATIONS** to the graphical workspace. The Application quick view appears.
2. Enter the Alias for the application.



3. Enter the following details for the Cloud tool export in the Application quick view:

Fields	Description
Alias	Enter the alias name for the cloud tool.
Cloud Tool	Select the Cloud tool from the drop-down menu.
Account ID	Enter the account ID number of the selected Cloud Tool.
API Key	Enter the API key of the Cloud Tool.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file. NOTE: Enable this field when using New Relic as the cloud tool.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 30 minutes.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Cloud Tool. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 5000 and the minimum is 10, however 1000 is the default value.
Labels	Click Add . Enter the following details: <ul style="list-style-type: none"> o Enter the Key . o Enter the Value. NOTE: When New Relic is selected as the cloud tool, ensure that the key is eventType and the Value can only have alphanumeric characters, colons (:), periods (.), and underscores (_).

4. Click **Deploy** to deploy the monitoring session. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the V Series Node for which you wish to deploy the monitoring session.
5. After selecting the V Series Node, select the interfaces for the REPs deployed in the monitoring session from the drop-down menu. Then, click **Deploy**.

The monitoring session configuration health can be viewed on the Monitoring Session page. Refer [Cloud Health Monitoring](#) for more detailed information on how to view cloud configuration health.

To view the application statistics on the Monitoring Session Statistics page, click **View Monitoring Session Diagram** and click on the OGW application. The Statistics appears as a quick view page. To view the exporter related statistics, select **Exporter** from the top navigation button on the quick view page.

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 Tunnel 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.

The Monitoring Session page also has the following buttons:

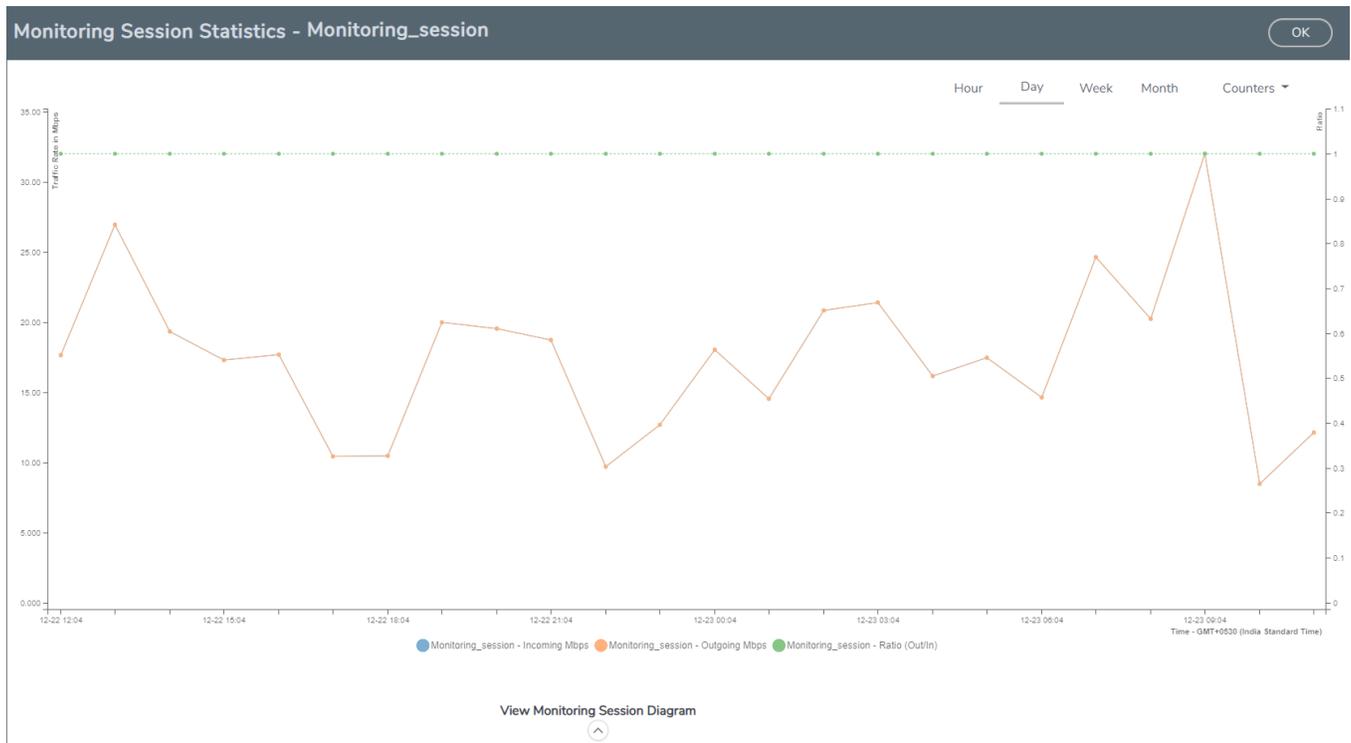
Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	<p>Opens the Edit page for the selected monitoring session.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.</p> </div>
Delete	Deletes the selected monitoring session.

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.



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.



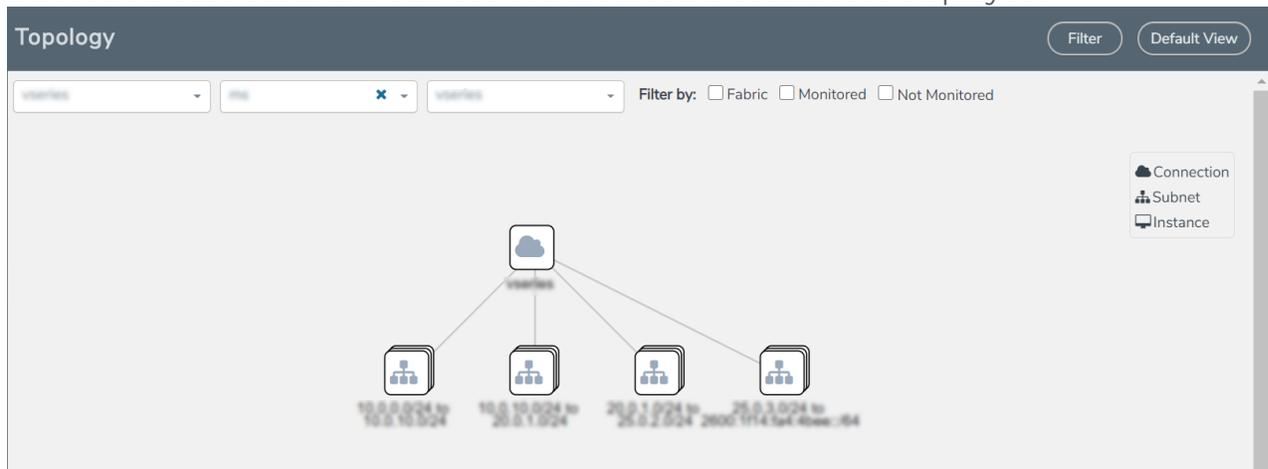
Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of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

Visualize the Network Topology

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.

Configure VMware Settings

To configure the VMware Settings:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > Settings**. The **Settings** page appears.
2. In the **Advanced** tab of the Settings page, click **Edit** to edit the Settings fields.

Advanced Settings

Save

Cancel

Maximum number of vCenter connections allowed	<input type="text" value="20"/>
Refresh interval for VM target selection inventory (secs)	<input type="text" value="120"/>
Refresh interval for fabric deployment inventory (secs)	<input type="text" value="900"/>

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

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](#)
- [Configure Application Intelligence Session](#)



Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **V Series Node API Proxy Server** (VPS) to scale and manage multiple 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

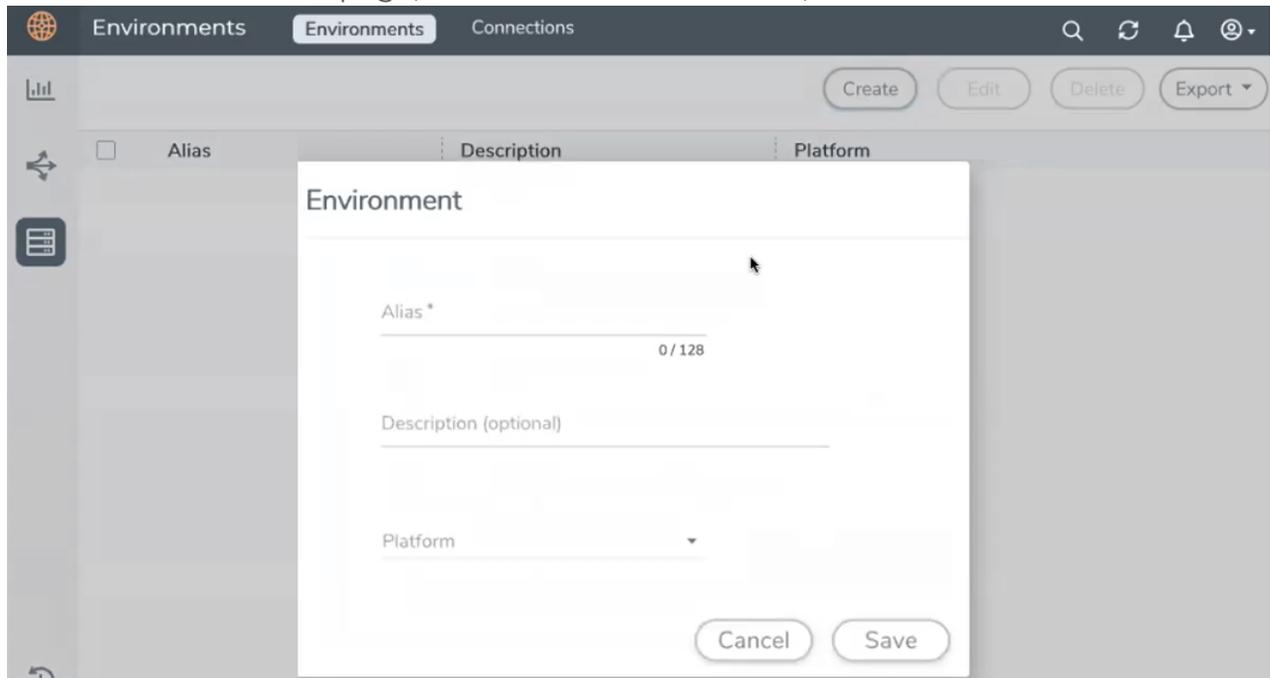
The Environments page allows you to create the following:

- **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.

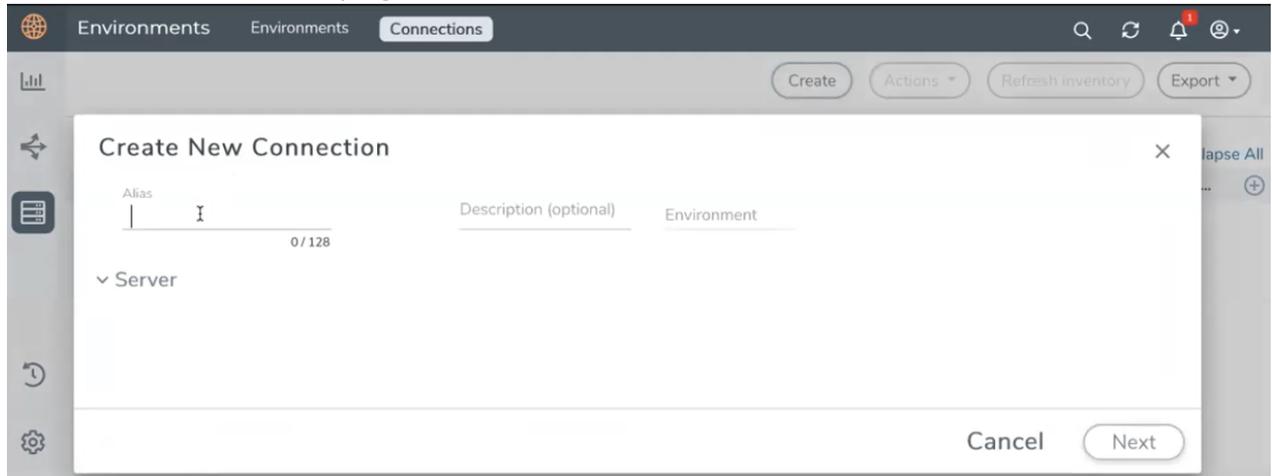
Connect to VMware ESXi

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 .

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
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
Tunnel CIDR	CIDR value of the Tunnel

Configure V Series Node on ESXi

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

Field	Description
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: <ul style="list-style-type: none"> • Edit Connection - Use to edit a connection. • Deploy Node - Use to deploy a node. <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>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.</p> </div> <ul style="list-style-type: none"> • 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.

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

+ -

+ New Criteria

Cancel
Save

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. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;">NOTE: You can create multiple criteria.</div>
Filter	The criteria based on which the traffic is filtered. Select from the list of available filters.
Operator	Select the required operator based on the filter selected. Options are: <ul style="list-style-type: none"> 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.

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 Description

Alias * Description (optional) Tunnel type

Cancel

Save

3. Enter or select the following information:

Field	Description
Alias	<p>The name of the tunnel endpoint.</p> <p>NOTE: Do not enter spaces in the alias name.</p>
Description	The description of the tunnel endpoint.
Tunnel Type	<p>The type of the tunnel.</p> <p>Select ERSPAN, or L2GRE, or VXLAN to create a tunnel.</p> <p>Do not select UDPGRE tunnel type.</p> <p>NOTE: VXLAN is the only supported tunnel type for Azure.</p>
Traffic Direction	<p>The direction of the traffic flowing through the V Series node.</p> <ul style="list-style-type: none"> 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. <p> ERSPAN, L2GRE, and VXLAN are the supported Ingress tunnel types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session.</p> <ul style="list-style-type: none"> 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	<p>For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.</p> <p>For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.</p>

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

Configure Application Intelligence Session

Application Visualization (earlier known as Application Monitoring) gathers the application statistics, and sends this information to GigaVUE-FM, which acts as an application monitor. The monitoring reports are sent to GigaVUE-FM through the destination port 2056. The application statistics appear as an array of monitoring reports that provide application-usage data in an easy-to-read graphical interface. This provides you with greater insight and control over how your network is being used and what applications are utilizing the most resources. To perform Application Monitoring, you must create the required application intelligence sessions on the nodes managed by GigaVUE-FM.

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

Complete the following prerequisites before creating an Application Intelligence solution in the 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.

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](#).
 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.

NOTE: Scale Unit is not applicable for the OpenStack platform.

Cloud Platform	Instance Size	Maximum Scale Unit
VMware	Large (8 vCPU and 16 GB RAM)	3
	Medium (4 vCPU and 8 GB RAM)	1
AWS	Large (c5n.2xlarge)	4
	Medium (t3a.xlarge)	3
Azure	Large (Standard_D8s_V4)	9
	Medium (Standard_D4s_v4)	3

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](#).
 - **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](#).



- 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.

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](#).

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.

You can also filter the traffic based on the applications. For more information, see [Create Application Filtering Intelligence](#).

Fabric Health Analytics for Virtual Resources (BETA)

Fabric Health Analytics is delivered as BETA in software version 5.16.00 and is subject to change in the upcoming release(s).

Fabric Health Analytics (FHA) in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using FHA¹ 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 BETA](#) 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.

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](#)

¹FHA 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.

[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)	<p>Statistical details of the virtual inventory based on the platform and the health status.</p> <p>You can view the following metric details at the top of the dashboard:</p> <ul style="list-style-type: none"> ● Number of Monitoring Sessions ● Number of V Series Nodes ● Number of Connections ● Number of GCB Nodes <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Health Status 	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	<p>Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node.</p> <p>You can filter the visualizations based on the following control filters:</p>	<i>V Series Node Maximum CPU Usage Trend</i>	<p>Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">NOTE: The maximum</div>

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> Platform Connection V Series Node 		<p>CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0.</p>
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	<p>Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.</p> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p>
		<i>V Series Node Rx Trend</i>	<p>Receiving trend of the V Series node in 5 minutes interval, for the past one hour.</p>
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	<p>Total packets received by each of the V Series network interface for the past 5 minutes.</p> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p>
		<i>V Series Node Tunnel Rx Packets/Errors</i>	<p>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.</p>
		<i>V Series Node</i>	<p>TX is for output tunnels</p>

Dashboard	Displays	Visualizations	Displays
		<i>Tunnel Tx Packets/Errors</i>	from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	<p>Displays visualizations related to Dedup application.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> Platform Connection VSeries Node 	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the dedup packets received against the dedup application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	<p>Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V-series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. V series node: Management IP of the V Series node. Choose the required V-series node from the drop-down. Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. <p>The following statistics are displayed for the tunnel:</p>	<i>Tunnel Bytes</i>	<p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> For input tunnel, transmitted traffic is displayed as zero. For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> Received Bytes Transmitted Bytes Received Packets Transmitted Packets Received Errored Packets Received Dropped Packets Transmitted Errored Packets Transmitted Dropped Packets 		
		<i>Tunnel Packets</i>	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	<p>Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V series node.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> Monitoring session V series node Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> Received Bytes Transmitted Bytes Received Packets Transmitted Packets Errored Packets Dropped Packets 	<i>App Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

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

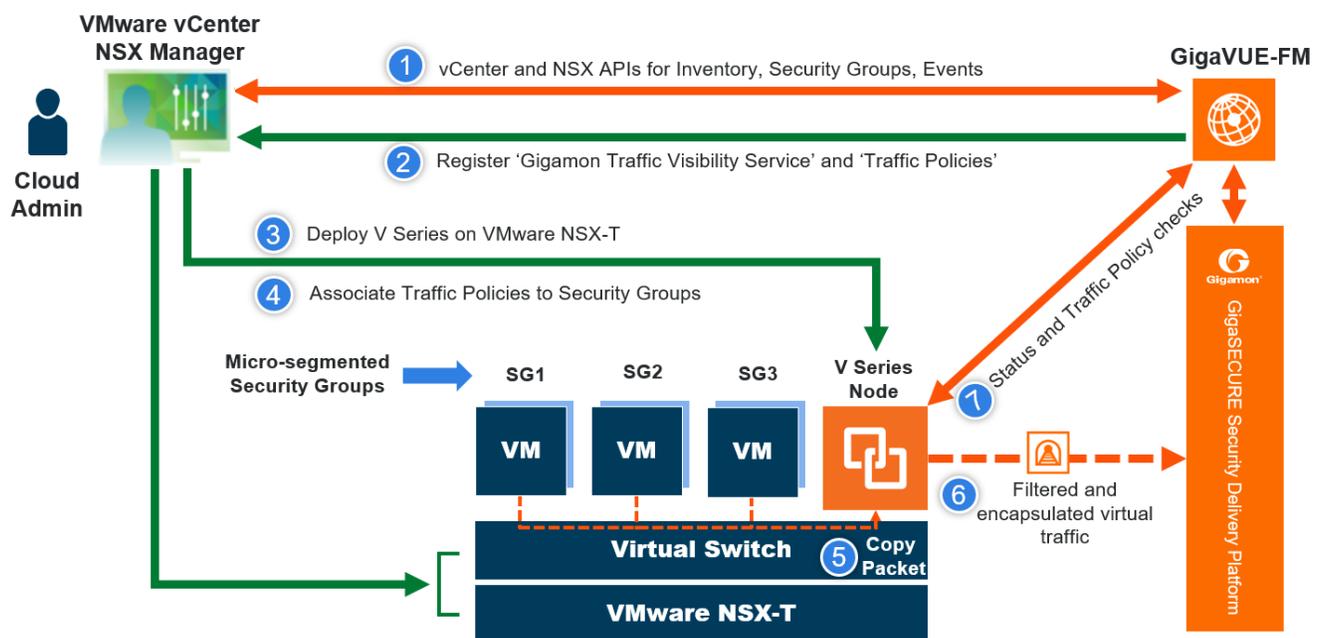
NOTE: The Tunnel (Virtual), App (Virtual) and Endpoint (Virtual) dashboards do not show data from the previous releases if the *Monitoring Session [Platform : Domain : Connection]* dashboard filter is applied. This is because, this filter relies on the new attributes in the Elasticsearch database, which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

Configure V Series Node on NSX-T

This section provides an overview of the V Series fabric 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:



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 V Series nodes with NSX-T

NOTE: These steps assume that VMware NSX-T is installed and configured.

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 V Series nodes with NSX-T:

- VMware vCenter Standard Version must be 7.0 with the required privileges. Refer to [Required VMware Virtual Center Privileges](#) for more information on vCenter privileges.
- Before deploying V Series nodes through GigaVUE-FM, Service segment must be created in the NSX-T manager.
- NSX-T version must be 3.1.3, 3.2.0 or 4.0.0.
- ESXi hosts must have the minimum vCPU and memory resources.
- GigaVUE-FM version must be 5.10.01 or later.
- V Series 2 device OVA image file.
- Port number 8889 must be available for GigaVUE-FM to access V Series nodes.

NOTE: GigaVUE-FM supports service insertion only for overlay transport zone associated with the E-W traffic. Service insertion is not supported for vlan transport zone associated with the N-S traffic or when the VMware NSX-T manager in federation mode.

NOTE: You cannot have both GigaVUE-VM and V Series node visibility solutions deployed on the same vCenter.

The V Series 2 Node OVA image files can be downloaded from [Gigamon Customer Portal](#).

Network Firewall Requirements

Following are the Network Firewall Requirements for V Series 2 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	V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with V Series node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
Remote Source	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 V Series nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
V Series Nodes	Tool/ HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows V Series node to communicate and tunnel traffic to the Tool
			N/A	IP 47	GRE	
V Series Nodes	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-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						

Configure V Series Node on NSX-T

Prerequisites for Integrating V Series Nodes with NSX-T

Recommended Form Factor (Instance Types)

The form factor (instance type) size of the V Series 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. Instance sizes can be different for V Series nodes in different ESXi hosts and the default size is Small.

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

Required VMware Virtual Center Privileges

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

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
Virtual machine	Interaction <ul style="list-style-type: none"> ▪ Power on ▪ Power Off 	V Series Node Deployment V Series Node Deployment

Integrate V Series nodes with NSX-T

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

- [Step 1: Create Users in VMware vCenter and GigaVUE-FM](#)
- [Step 2: Upload V Series node Image into GigaVUE-FM](#)
- [Step 3: Connect to VMware vCenter in GigaVUE-FM](#)
- [Step 4: Create a Service Segment in NSX-T](#)
- [Step 5: Deploy GigaVUE V Series Nodes on VMware NSX-T](#)
- [Step 6: Configure Monitoring Sessions](#)
- [Step 7: Create NSX-T Group and Service Chain](#)

Step 1: Create Users in VMware vCenter and GigaVUE-FM

For NSX-T and GigaVUE-FM to communicate, a Gigamon-FM user must be created in NSX-T, and an NSX-T user must be created in Gigamon-FM. Also, a GigaVUE-FM user must be created in NSX-T for GigaVUE-FM to perform NSX-T inventory functions. 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 Virtual Center Privileges](#) 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.

Create GigaVUE-FM 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. This user will be a GigaVUE-FM user that the GigaVUE-FM uses to communicate with NSX-T Manager.

To create a user in NSX-T:

1. In NSX-T, navigate to **System > Settings > Users and Roles** and click **USERS** tab.
2. On the **USERS** 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.

- for **NSX-T version 2.x**, select Principal Identity with Role and select the Role as Enterprise Admin.
3. Click **Save** and then a GigaVUE-FM user is created in NSX-T.

Create VMware NSX-T user in GigaVUE-FM

For NSX-T to be able to communicate with GigaVUE-FM, you need to create a user in GigaVUE-FM who has the admin role. To create an NSX-T user in GigaVUE-FM, do the following:

1. From the left navigation pane, select **Settings > Authentication > User Management**. The **User Management** page appears.

- In the **Users** tab, click **Add**. The Create User page appears.

Create User
✕

Name	Name	
Username	Username	
Email	Email	
Password	Password	?
Confirm Password	Confirm Password	

Cancel
Save

- On the **Create User** page, specify the following for the new user:
 - In the **Name** field, enter the name of the call back user. For example, you can use NSX-T Manger Callback as the user name to help you associate this user with the NSX-T Manger.
 - 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.
 - In the Email field, enter the email ID of the user.
 - In the **Password** field, enter the password for the user specified in the **Name** and **Username** fields.
 - In the **Confirm Password** field, reenter the password.

The FM Users NSX-T page should look like the example shown in the following figure when you are done.

- Click **Save**.

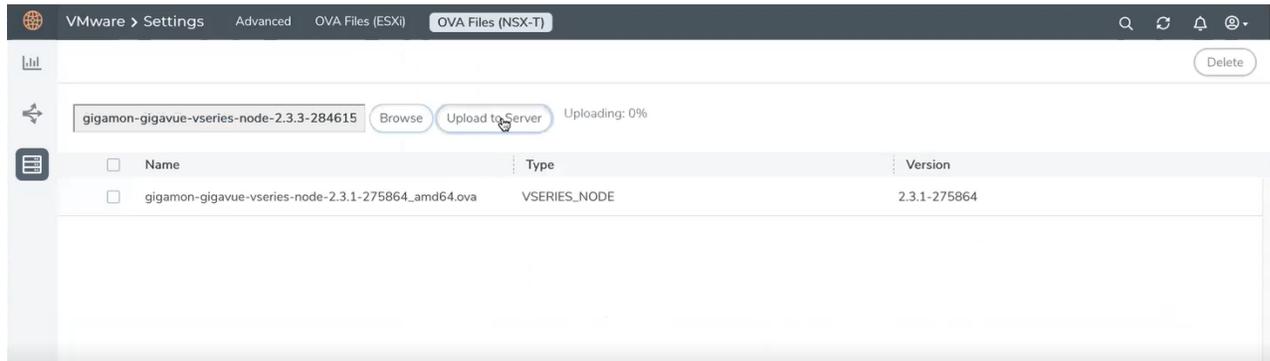
Refer [Deploying GigaVUE Cloud Suite for VMware vCenter using V Series](#) for more detailed information.

Step 2: Upload 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. From the left navigation pane, select **Inventory > VIRTUAL > VMware > Settings**. The **Settings** page appears.
2. In the Settings page, click **OVA Files (NSX-T)** tab.



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

Step 3: Connect to VMware vCenter in GigaVUE-FM

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. In GigaVUE-FM, from the left navigation pane, select **Inventory > VIRTUAL > VMware > Monitoring Domain**. The Monitoring Domain page appears.
2. On the **Monitoring Domain** page, click **New**. The **VMware Configuration** page appears.

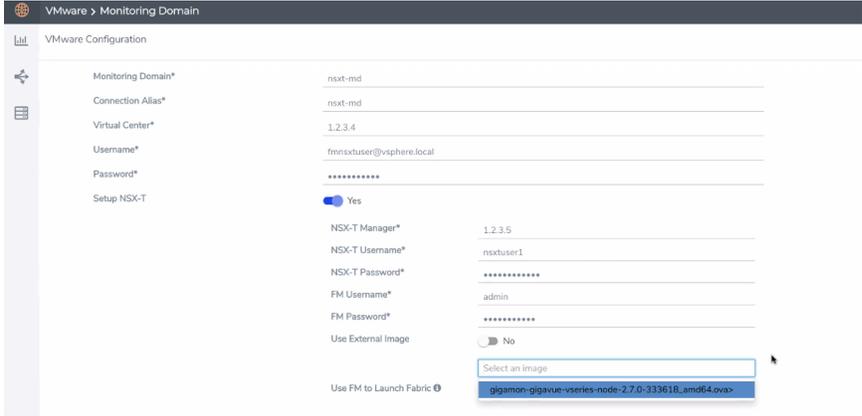
VMware Configuration Save Cancel

Monitoring Domain*	Enter a monitoring domain name
Connection Alias*	Alias
Virtual Center*	Virtual Center
Username*	Username
Password*	Password
Setup NSX-T	<input checked="" type="checkbox"/> Yes
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	<input checked="" type="checkbox"/> Yes
	Image URL
Use FM to Launch Fabric	<input checked="" type="checkbox"/> Yes

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

Field	Description
Username	Username of the vCenter user with admin role privilege
Password	vCenter password used to connect to the vCenter
Setup NSX-T	<p>Enable to setup NSX-T and the fields of NSX-T to appear.</p> <p>Enter or select the following details for NSX-T:</p> <ul style="list-style-type: none"> • 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. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <ul style="list-style-type: none"> • The NSX-T user account must have admin privileges. • Each NSX-T manager can support a maximum of one monitoring domain. </div> <ul style="list-style-type: none"> • FM Username: Username of your GigaVUE-FM account. • FM Password: Password of your GigaVUE-FM account.

Field	Description
	<ul style="list-style-type: none"> • Use External Image: The 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. <ol style="list-style-type: none"> 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: <i>http://<server-IP:port>/<path to where the OVF files are saved></i> and the port can be any valid number. The default port number is 80. <div data-bbox="609 562 1471 674" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>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.</p> </div> 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. <div data-bbox="609 783 1471 1199" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">  </div> <div data-bbox="609 1220 1471 1306" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>NOTE: When using an internal image, before VMware Configuration save the OVA files to the dedicated directory.</p> </div>

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

To edit a monitoring domain, click on the **Edit** button in the VMware Monitoring Domain page, 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.

Step 4: Create a Service Segment in 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 OVF's are allowed for deployment
 - 1: only VMware-signed and well-known CA-signed OVF's are allowed for deployment
 - 2: no validation
4. Save and Exit the file.

Step 5: Deploy GigaVUE V Series Nodes on 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](#)
- [Upgrade GigaVUE V Series Node in 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.

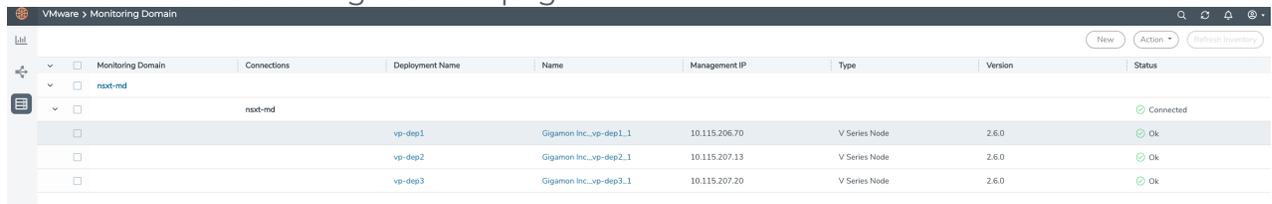
The screenshot displays the 'VMware NSX-T Fabric Deployment' configuration page. The interface includes a left-hand navigation menu with icons for home, back, and settings. The main configuration area is divided into several sections:

- Deployment Name:** A text input field.
- Datacenter:** A dropdown menu with the placeholder text 'Select a datacenter...'.
- Cluster:** A dropdown menu with the value 'N/A'.
- Datastore:** A dropdown menu with the value 'N/A'.
- Management:** A section containing two sub-sections:
 - Network:** A dropdown menu with the value 'N/A'.
 - IP Type:** A dropdown menu with the placeholder text 'Select IP type...'.
- Tunnel:** A section containing three sub-sections:
 - Network:** A dropdown menu with the value 'N/A'.
 - IP Type:** A dropdown menu with the placeholder text 'Select IP type...'.
 - Gateway IP:** A text input field.
 - Netmask Length:** A text input field with the value '1-32' and a help icon.
- User Password:** A text input field with the placeholder text '(gigamon)'.
- Confirm User Password:** A text input field.
- Form Factor:** A dropdown menu with the value 'Small, 2vCPU, 4GB RAM, 8GB Disk'.
- Service Attachment:** A dropdown menu with the placeholder text 'Select service attachment...'.
- Deployment Type:** A dropdown menu with the placeholder text 'Select deployment type...'.
- Deployment Count:** A text input field with the value '1-10'.

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 V Series nodes
Datastore	Network datastore shared among all NSX-T hosts.
Management	
Network	Management network for V Series nodes
IP Type	Select the management network IP type as Static or DHCP
Tunnel Network	
Network	Tunnel Network for the V Series nodes
IP Type	Select the tunnel network IP address type as Static or DHCP
Gateway IP	Gateway IP address of the Tunnel Network
Netmask Length	Tunnel network's subnet mask value in CIDR format. Eg. 21 for /21
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. <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> <p>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.</p> </div>
Deployment Count (for Clustered deployment type)	Number of 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.



The screenshot shows the VMware Monitoring Domain interface. A table lists the following V Series nodes:

Deployment Name	Name	Management IP	Type	Version	Status
vp-dep1	Gigamon Inc...vp-dep1.1	10.115.206.70	V Series Node	2.6.0	Ok
vp-dep2	Gigamon Inc...vp-dep2.1	10.115.207.13	V Series Node	2.6.0	Ok
vp-dep3	Gigamon Inc...vp-dep3.1	10.115.207.20	V Series Node	2.6.0	Ok

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.

Upgrade GigaVUE V Series Node in 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. In GigaVUE-FM, on the left navigation pane, select **Inventory > VIRTUAL > VMware > Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select a monitoring domain and click **Fabric**. From the drop-down list, select **Upgrade Fabric**, the **V Series Node Upgrade** dialog box appears.

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- XXXXXXXXXX -node1-10-210-27-202	OK

Clear Close

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.

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 V Series Nodes and Monitoring Domain](#)
- [Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager](#)
- [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 [Step 3: Connect to VMware vCenter in GigaVUE-FM](#) 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.

The screenshot shows the 'VMware Configuration' page in GigaVUE-FM. The page is titled 'VMware Configuration' and has a 'Save' and 'Cancel' button in the top right corner. The page is divided into two main sections: a left sidebar with a menu and a main content area. The main content area contains several configuration fields:

- Monitoring Domain***: Enter a monitoring domain name
- Connection Alias***: Alias
- Virtual Center***: Virtual Center
- Username***: Username
- Password***: Password
- Setup NSX-T**: Yes
- 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**: Yes
- Image URL**: Image URL
- Use FM to Launch Fabric**: Yes

NOTE: When creating the Monitoring Domain for deploying V Series Nodes, you can use the VMware NSX-T username and password that has at least "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.
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 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...	10.10.10.10	V Series Node	3.4.0	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 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.

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 **Edit** in the Monitoring Domain page. The VMware **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.

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.

Step 6: Configure Monitoring Sessions

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](#)
- [Create Ingress and Egress Tunnel](#)
- [Create a New Map](#)
- [Add Applications to Monitoring Session](#)
- [Deploy Monitoring Session](#)
- [View Monitoring Session Statistics](#)
- [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

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.

Create Ingress and Egress Tunnel

Traffic from the V Series 2 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 **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table.

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 to create a tunnel.
Traffic Direction	The direction of the traffic flowing through the V Series node. <ul style="list-style-type: none"> • Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node. 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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <ul style="list-style-type: none"> • 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. </div>
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 delete a tunnel, select the required tunnel and click **Delete**.

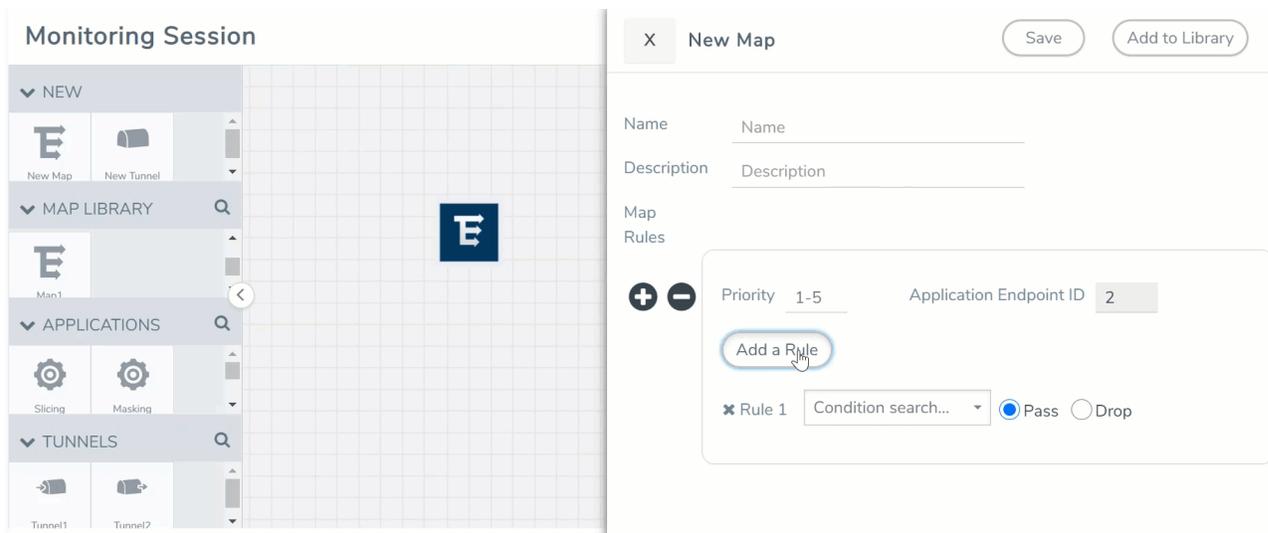
Create a New Map

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 detailed information on GigaVUE-FM licenses, refer to "Licenses" section in the *GigaVUE Administration Guide*.

To create a new map:

1. After creating a new monitoring session, or click **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.



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
Comments	Description of the map
Map Rules	<p>The rules for filtering the traffic in the map. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add multiple rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. A rule set can have only 5 rules per map and 25 conditions per map. To add ATS rules for an Inclusion/Exclusion map, you must select atleast one rule condition.</p> <p>To add a map rule:</p> <ol style="list-style-type: none"> Enter a Priority value from 1 to 5 for the rule with 5 being the highest and 1 is the lowest priority. Click Add a Rule. The new rule field appear for the Application Endpoint. Select a required condition from the drop-down list. Select the rule to Pass or Drop through the map. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> If two rules with same condition are configured as pass and drop,</p> <ul style="list-style-type: none"> on a same tunnel endpoint, the traffic filtering precedence will be based on the priority value. on two different tunnel endpoints, the traffic will be passed or dropped to the respective tunnel endpoints. <p>For detailed information on filtering fragmented and unfragmented packets, refer to "GigaSMART Adaptive Packet Filtering (APF)" section on the <i>GigaVUE Fabric Management Guide</i>.</p> </div>



- 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. 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**.
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.

Add Applications to Monitoring Session

GigaVUE Cloud Suite with GigaVUE V Series 2 node supports the following GigaSMART applications in the GigaVUE-FM canvas:

- [Slicing](#)
- [Masking](#)
- [Dedup](#)
- [Load Balancing](#)
- [PCAPng](#)

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*.

For the detailed list of GigaSMART Operation supported for V Series 2 nodes, refer to "Supported GigaSMART Operation" topic in the *GigaVUE Fabric Management Guide*.

You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools. Refer to the [Volume Based License \(VBL\)](#) section for more information on Licenses for using V Series 2 Nodes.

To add a GigaSMART application:

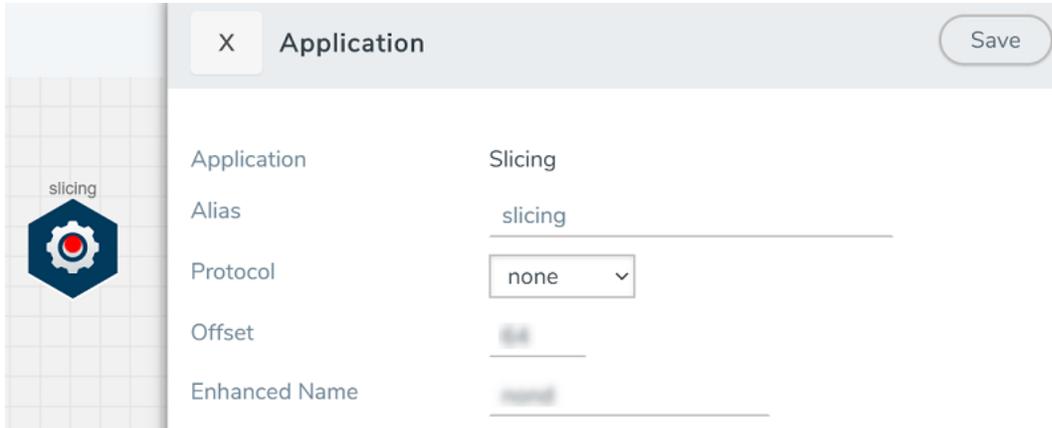
1. Drag and drop an application from **APPLICATIONS** to the canvas.
2. In the canvas, click the application and select **Details**.
3. Enter or select the required values for the selected application and click **Save**.

Slicing

Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. For detailed information on Slicing, refer to [GigaSMART Packet Slicing](#) "GigaSMART Packet Slicing" topic in the *GigaVUE Fabric Management Guide*.

To add a slicing application:

1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.
2. Click the Slicing application and select **Details**. The Application quick view appears.



Field	Value
Application	Slicing
Alias	slicing
Protocol	none
Offset	64
Enhanced Name	none

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the slicing.
 - From the **Protocol** drop-down list, specify an optional parameter for slicing the specified length of the protocol.
 - In the **Offset** field, specify the length of the packet that must be sliced.
 - In the **Enhanced Name** field, enter the Enhanced Slicing profile name.
4. Click **Save**.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. For detailed information on masking, refer to [GigaSMART Masking](#) "GigaSMART Masking" topic in the *GigaVUE Fabric Management Guide*.

To add a masking application:

1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.
2. Click the Masking application and select **Details**. The Application quick view appears.

Application	Masking
Alias	masking
Protocol	none
Offset	0
Pattern	0000
Length	8

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the masking.
 - From the **Protocol** drop-down list, specify an optional parameter for masking the specified length of the protocol.
 - In the **Offset** field, specify the length of the packet that must be masked.
 - In the **Pattern** field, enter the pattern for masking the packet.
 - In the **Length** field, enter the length of the packet that must be masked.
4. Click **Save**.

Dedup

De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment. For detailed information on de-duplication, refer to [GigaSMART De-Duplication](#) "GigaSMART De-Duplication" topic in the *GigaVUE Fabric Management Guide*.

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.

Application	Dedup ⓘ	
Alias	dedup	
Action	<input type="radio"/> Count	<input checked="" type="radio"/> Drop
IP Tclass	<input checked="" type="radio"/> Include	<input type="radio"/> Ignore
IP TOS	<input checked="" type="radio"/> Include	<input type="radio"/> Ignore
TCP Sequence	<input checked="" type="radio"/> Include	<input type="radio"/> Ignore
VLAN	<input type="radio"/> Include	<input checked="" type="radio"/> Ignore
Timer	50000	

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the de-duplication.
 - In the Action field, select **Count** or **Drop** the detected duplicate packets.
 - For **IP Tclass**, **IP TOS**, **TCP Sequence**, and **VLAN** fields, select **Include** or **Exclude** the packets for de-duplication.
 - In the **Timer** field, enter the time interval (in seconds) for de-duplicating the packet.
4. Click **Save**.

Load Balancing

Load balancing app performs stateless distribution of the packets between different endpoints. For detailed information on load balancing, refer to [GigaSMART Load Balancing](#) "GigaSMART Load Balancing" topic in the *GigaVUE Fabric Management Guide*.

To add a load balancing application:

1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
2. Click the load balancing application and select **Details**. The Application quick view appears.

Application	Load Balancing
Alias	lb
Hash Fields	ipOnly
Field Location	outer
Load balancing groups	
Application Endpoint ID	2
Weight	1-100

3. In the Application quick view, enter the information as follows:
 - In the **Alias** field, enter a name for the load balancing app.
 - For **Hash Fields** field, select a hash field from the list.
 - **ipOnly**—includes Source IP, and Destination IP.
 - **ipAndPort**—includes Source IP, Destination IP, Source Port , and Destination Ports.
 - **fiveTuple**—includes Source IP, Destination IP, Source Port, Destination Port, and Protocol fields.
 - **gtpuTeid**—includes GTP-U.

- For **Field location** field, select **Inner** or **Outer** location.

NOTE: Field location is not supported for **gtpuTeid**.

- In the **load balancing groups**, add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

4. Click **Save**.

PCAPng

The PCAPng application is a GigaSMART parser application that reads the various blocks in the received PCAPng files and validates the blocks to be sent to the destination application or to the tools.

NOTE: The PCAPng application is only applicable for the Ericsson 5G Core vTAP architecture. Refer to "PCAPng Application" topic in the *GigaVUE Fabric Management Guide* for detailed information.

Create Link Between UDP-in-GRE Tunnel and PCAPng Application

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. 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 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> NOTE: Do not enter spaces in the alias name. </div>
Description	The description of the tunnel endpoint
Type	Select UDPGRE as the tunnel type
Traffic Direction	The direction of the traffic flowing through the V Series node <ul style="list-style-type: none"> • Choose In (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6
Remote Tunnel IP	The IP address of the tunnel source
Key	GRE key value
Source L4 Port	Layer 4 source port number
Destination L4 Port	Layer 4 destination port number. You can configure only 4754 or 4755 as the destination UDP ports

3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

Create a link with source as PCAPng application and destination as one of the following:

- Other GigaSMART applications such as Slicing, Masking, etc.
- Other encapsulation TEPs.
- REP/MAP

Refer to the following image for a sample configuration.

Refer [Deploying Application Intelligence solutions for VMware NSX-T 3.1.3](#) for more detailed information.

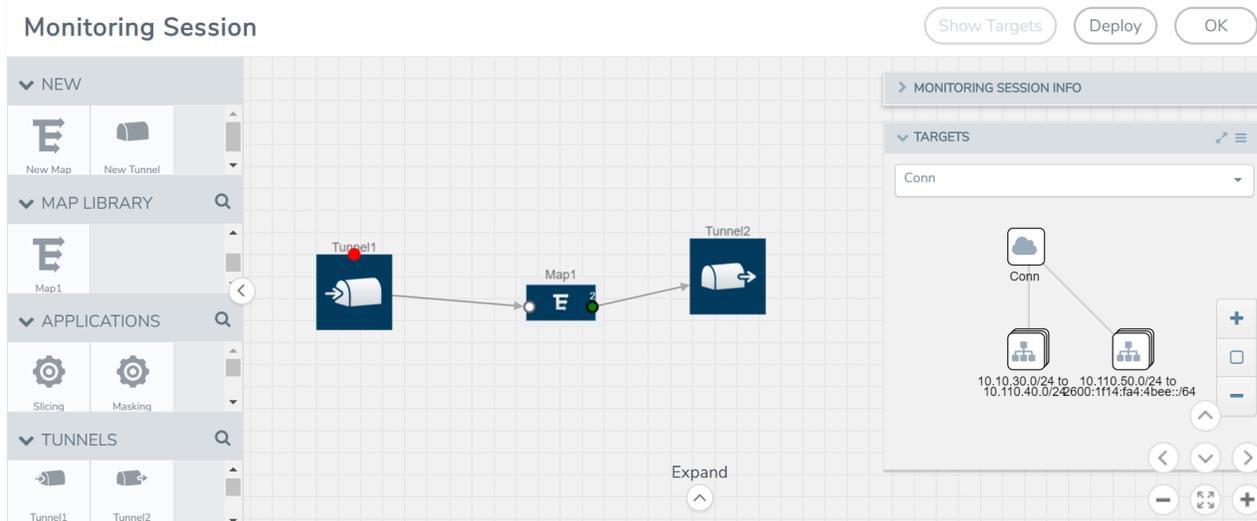
Deploy Monitoring Session

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

- 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.



- (Not applicable for NSX-T solution and Tunnel 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.
- 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.

The Monitoring Session page also has the following buttons:

Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected monitoring session. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session</p> </div>

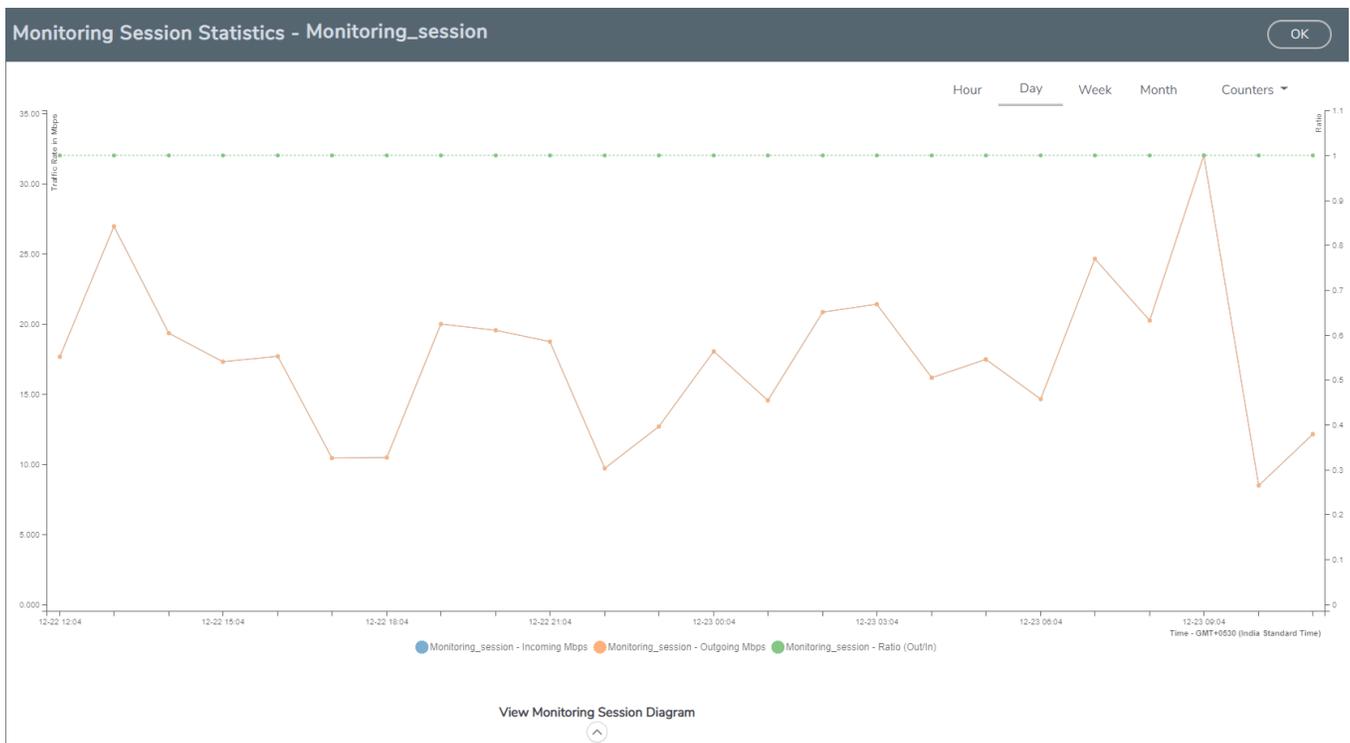
Button	Description
	again.
Delete	Deletes the selected monitoring session.

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.



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

- Directly below the graph, you can click on **Incoming Mbps**, **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.



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.

Configure VMware Settings

To configure the VMware Settings:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > Settings**. The **Settings** page appears.
2. In the **Advanced** tab of the Settings page, click **Edit** to edit the Settings fields.

Advanced Settings

Maximum number of vCenter connections allowed	<input type="text" value="20"/>
Refresh interval for VM target selection inventory (secs)	<input type="text" value="120"/>
Refresh interval for fabric deployment inventory (secs)	<input type="text" value="900"/>

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

Step 7: 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.

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](#)
- [Configure Application Intelligence Session](#)



Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **V Series Node API Proxy Server** (VPS) to scale and manage multiple 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

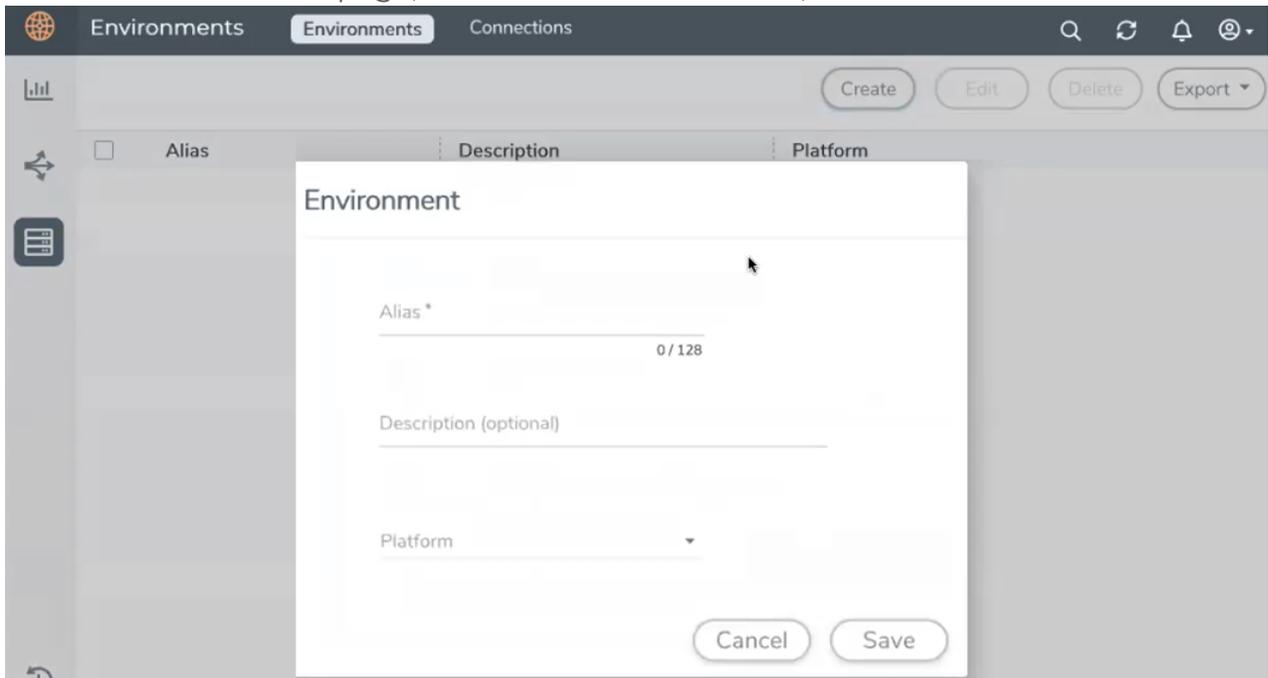
The Environments page allows you to create the following:

- **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 following format: <i>http://<server-IP;port>/<path to where the OVF files are saved></i> and the port can be any valid number.
GigaVUE-FM User Name	GigaVUE-FM username.
GigaVUE-FM Password	GigaVUE-FM password

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
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.
CIDR	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

Field	Description
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)	<p>Deployment type is clustered.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>NOTE: Host-based deployment option is disabled, as there can be one V series node per ESXi host.</p> </div> <p>Deployment count is restricted to one V Series nodes (Service Instances).</p>

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

Button	Description
Create	Use to create new connection.
Actions	<p>Provides the following options:</p> <ul style="list-style-type: none"> • Edit Connection - Use to edit a connection. You can only edit the following fields in the Edit Connection page: <ul style="list-style-type: none"> ▪ 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 option to 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 [Step 7: 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	Description	
Alias *	Description (optional)	Tunnel type

Cancel

Save

3. Enter or select the following information:

Field	Description
Alias	<p>The name of the tunnel endpoint.</p> <p>NOTE: Do not enter spaces in the alias name.</p>
Description	The description of the tunnel endpoint.
Tunnel Type	<p>The type of the tunnel.</p> <p>Select ERSPAN, or L2GRE, or VXLAN to create a tunnel.</p> <p>Do not select UDPGRE tunnel type.</p> <p>NOTE: VXLAN is the only supported tunnel type for Azure.</p>
Traffic Direction	<p>The direction of the traffic flowing through the V Series node.</p> <ul style="list-style-type: none"> 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. <p> ERSPAN, L2GRE, and VXLAN are the supported Ingress tunnel types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session.</p> <ul style="list-style-type: none"> 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	<p>For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.</p> <p>For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.</p>

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

Configure Application Intelligence Session

Application Visualization (earlier known as Application Monitoring) gathers the application statistics, and sends this information to GigaVUE-FM, which acts as an application monitor. The monitoring reports are sent to GigaVUE-FM through the destination port 2056. The application statistics appear as an array of monitoring reports that provide application-usage data in an easy-to-read graphical interface. This provides you with greater insight and control over how your network is being used and what applications are utilizing the most resources. To perform Application Monitoring, you must create the required application intelligence sessions on the nodes managed by GigaVUE-FM.

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

Complete the following prerequisites before creating an Application Intelligence solution in the 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.

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](#).
 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.

NOTE: Scale Unit is not applicable for the OpenStack platform.

Cloud Platform	Instance Size	Maximum Scale Unit
VMware	Large (8 vCPU and 16 GB RAM)	3
	Medium (4 vCPU and 8 GB RAM)	1
AWS	Large (c5n.2xlarge)	4
	Medium (t3a.xlarge)	3
Azure	Large (Standard_D8s_V4)	9
	Medium (Standard_D4s_v4)	3

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](#).
 - **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](#).



- 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.

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](#).

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.

You can also filter the traffic based on the applications. For more information, see [Create Application Filtering Intelligence](#).

Fabric Health Analytics for Virtual Resources (BETA)

Fabric Health Analytics is delivered as BETA in software version 5.16.00 and is subject to change in the upcoming release(s).

Fabric Health Analytics (FHA) in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using FHA¹ 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 BETA](#) 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.

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](#)

¹FHA 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.

[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)	<p>Statistical details of the virtual inventory based on the platform and the health status.</p> <p>You can view the following metric details at the top of the dashboard:</p> <ul style="list-style-type: none"> ● Number of Monitoring Sessions ● Number of V Series Nodes ● Number of Connections ● Number of GCB Nodes <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> • Platform • Health Status 	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	<p>Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node.</p> <p>You can filter the visualizations based on the following control filters:</p>	<i>V Series Node Maximum CPU Usage Trend</i>	<p>Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">NOTE: The maximum</div>

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> Platform Connection V Series Node 		<p>CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0.</p>
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	<p>Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.</p> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p>
		<i>V Series Node Rx Trend</i>	<p>Receiving trend of the V Series node in 5 minutes interval, for the past one hour.</p>
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	<p>Total packets received by each of the V Series network interface for the past 5 minutes.</p> <p>NOTE: You cannot use the time based filter options to filter and visualize the data.</p>
		<i>V Series Node Tunnel Rx Packets/Errors</i>	<p>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.</p>
		<i>V Series Node</i>	<p>TX is for output tunnels</p>

Dashboard	Displays	Visualizations	Displays
		<i>Tunnel Tx Packets/Errors</i>	from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	<p>Displays visualizations related to Dedup application.</p> <p>You can filter the visualizations based on the following control filters:</p> <ul style="list-style-type: none"> Platform Connection VSeries Node 	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the dedup packets received against the dedup application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	<p>Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V-series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. V series node: Management IP of the V Series node. Choose the required V-series node from the drop-down. Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. <p>The following statistics are displayed for the tunnel:</p>	<i>Tunnel Bytes</i>	<p>Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.</p> <ul style="list-style-type: none"> For input tunnel, transmitted traffic is displayed as zero. For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	Visualizations	Displays
	<ul style="list-style-type: none"> Received Bytes Transmitted Bytes Received Packets Transmitted Packets Received Errored Packets Received Dropped Packets Transmitted Errored Packets Transmitted Dropped Packets 		
		<i>Tunnel Packets</i>	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	<p>Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V series node.</p> <p>You can select the following control filters, based on which the visualizations will get updated:</p> <ul style="list-style-type: none"> Monitoring session V series node Application: Select the required application. By default, the visualizations displayed includes all the applications. <p>By default, the following statistics are displayed:</p> <ul style="list-style-type: none"> Received Bytes Transmitted Bytes Received Packets Transmitted Packets Errored Packets Dropped Packets 	<i>App Bytes</i>	Displays received traffic vs transmitted traffic, in Bytes.

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

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

Remove Gigamon Service from NSX-T and GigaVUE-FM

To clean up the Gigamon 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.

Cloud Health Monitoring

GigaVUE-FM allows you to monitor the configuration health status of the entire monitoring session and also the individual fabric components for which monitoring session is configured. This feature provides 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

For G-vTAP Agents:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

View Monitoring Session Configuration Health

You can view the configuration status of the monitoring session and the components deployed, in the monitoring session page. This section provides information about the configuration health status of the various fabric components deployed in the monitoring session.

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

Health

This column displays the configuration health status of the entire monitoring session.

The error message associated with monitoring session configuration appears when you hover over the health column. You can use the error message to help you troubleshoot and identify the components that are in conflict or mis-configured.

V Series Node Health

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

You can view the health status of the individual V Series Nodes and also the error message associated with them, by clicking on the V Series Node Health column.

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

The screenshot shows the AWS Monitoring Session interface. The top navigation bar includes 'AWS', 'Monitoring Session', and 'Topology'. Below the navigation bar, there are several tabs: 'Monitoring Domain', 'Monitoring Session', 'Statistics', 'Health', 'V Series Nodes Health', 'VPCs', 'Deployment Status', 'Number of Targets', and 'Targets Source...'. The 'V Series Nodes Health' tab is active, displaying a table with columns for 'V Series Node', 'Management IP', 'Version', and 'Health'. The table shows one entry: 'Gigamon-VSeriesNode-1' with a Management IP of '10.0.1.115', Version '2.6.0', and Health 'Ok'. Below the table, there is a 'V Series Nodes Health' section with a close button (X) and a plus button (+). The interface also includes a search bar, a toolbar with buttons like 'Deploy', 'Undeploy', 'New', 'Clone', 'Edit', 'Delete', and 'Export', and a pagination control showing 'Go to page: 1 of 1' and 'Total Records: 3'.

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.

View Monitoring Session Statistics

You can now 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.

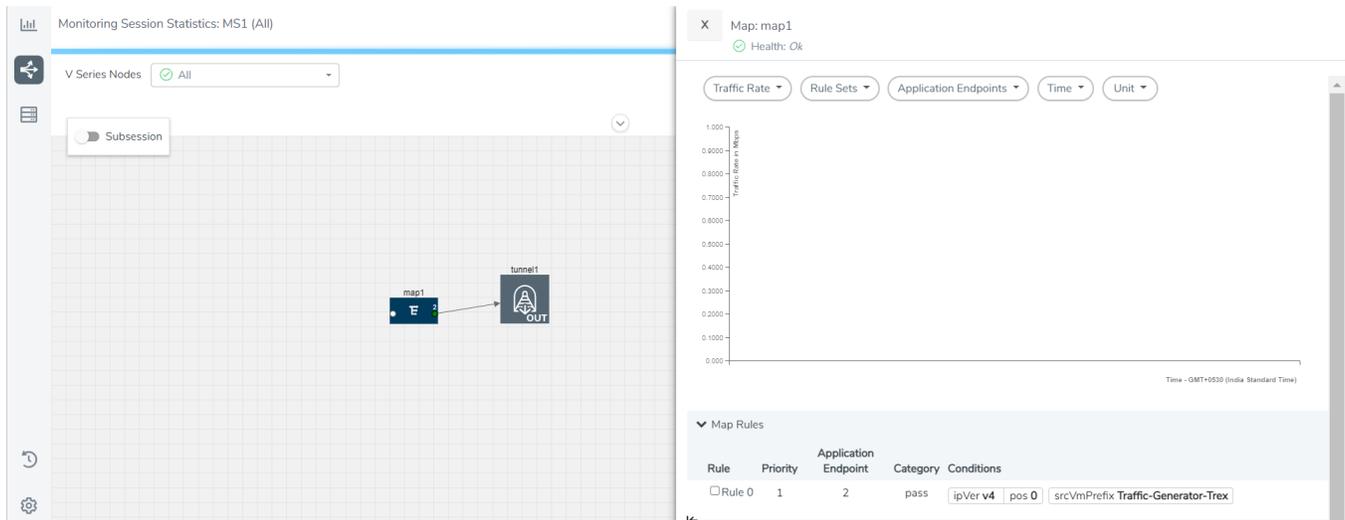
Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

View Monitoring Session Diagram

The Monitoring Session diagram page displays the applications and end points deployed in a particular monitoring session in pictorial form. To view the statistics of a particular application or an endpoint, click on the application icon for which you want to view the statistics. You can also view the statistics of a particular application for an individual V Series Node by selecting 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 page.

When you select a V Series Node from the V Series Node drop-down, the application icon displays the name of that particular application as configured in the V Series Node.

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.



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:

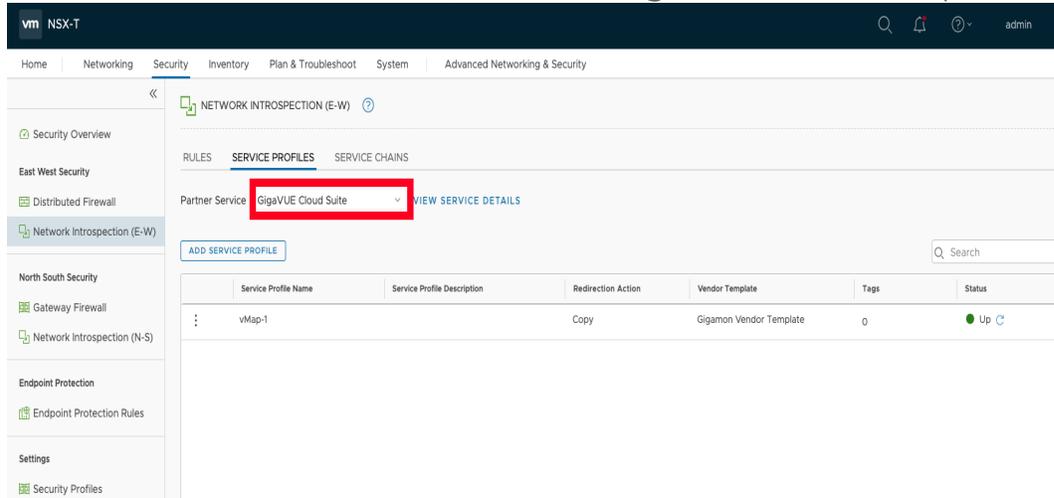
- [Remove Service Profiles](#)
- [Remove Service Deployments](#)

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

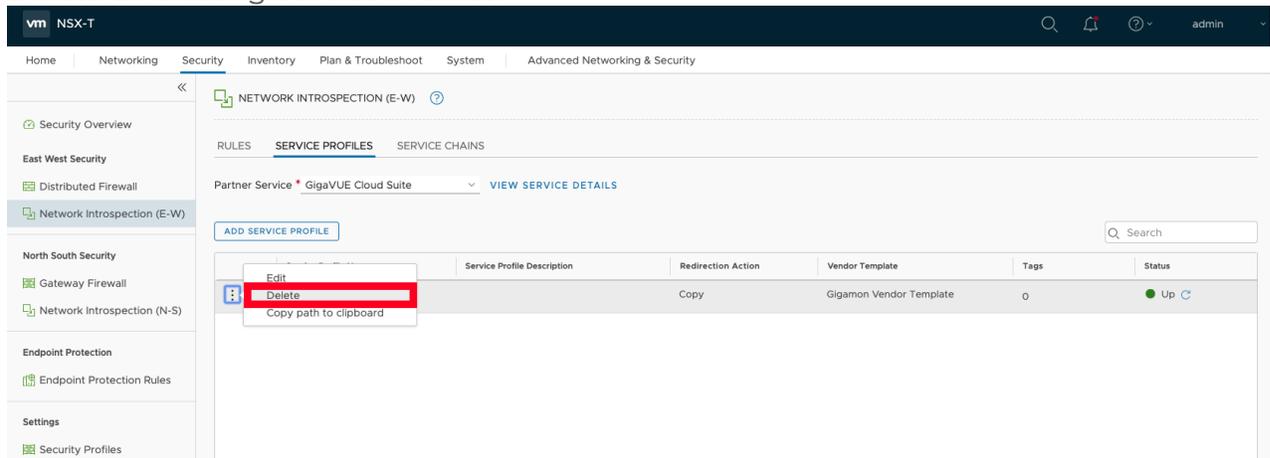
Remove Service Profiles

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.



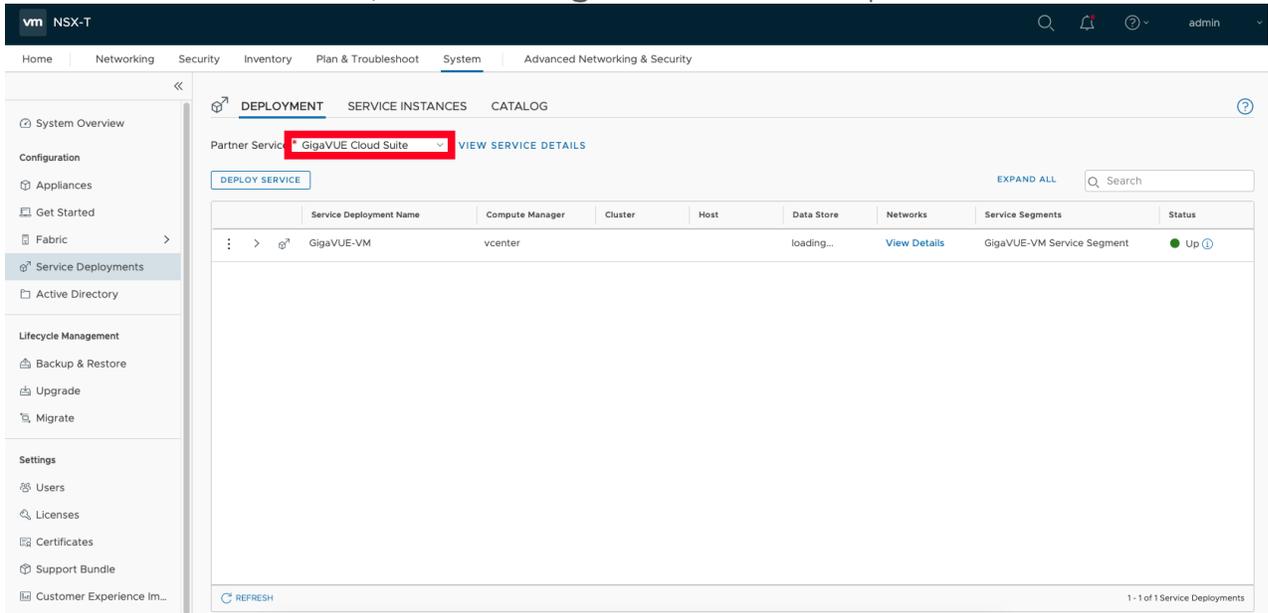
3. Delete all existing Service Profiles.



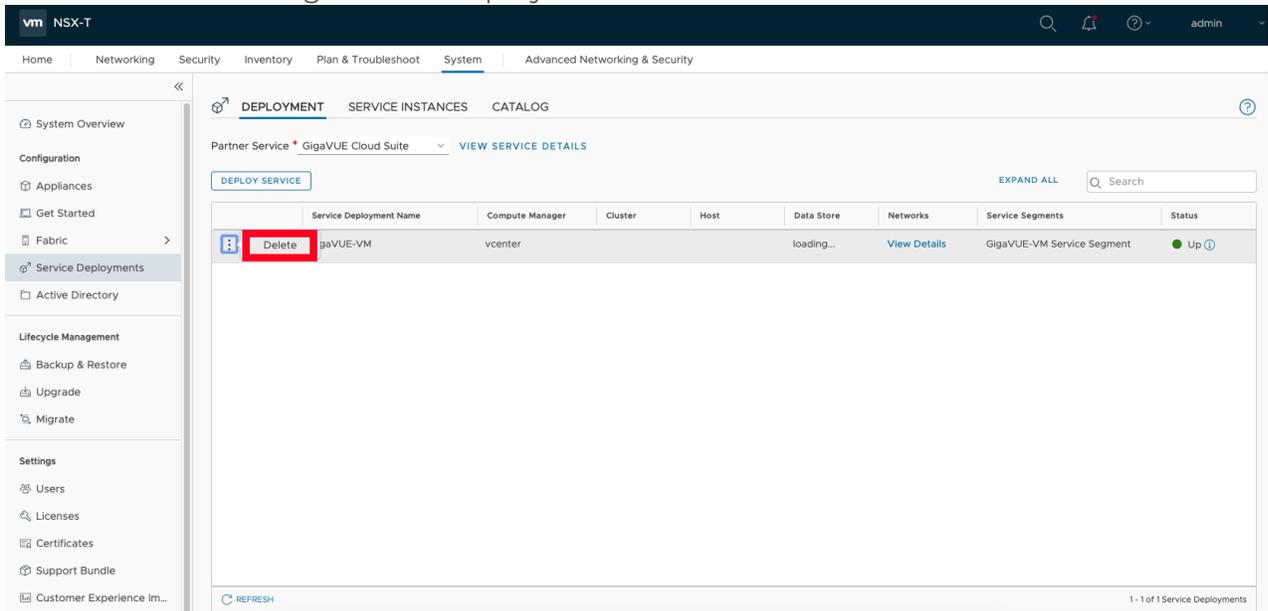
Remove Service Deployments

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.

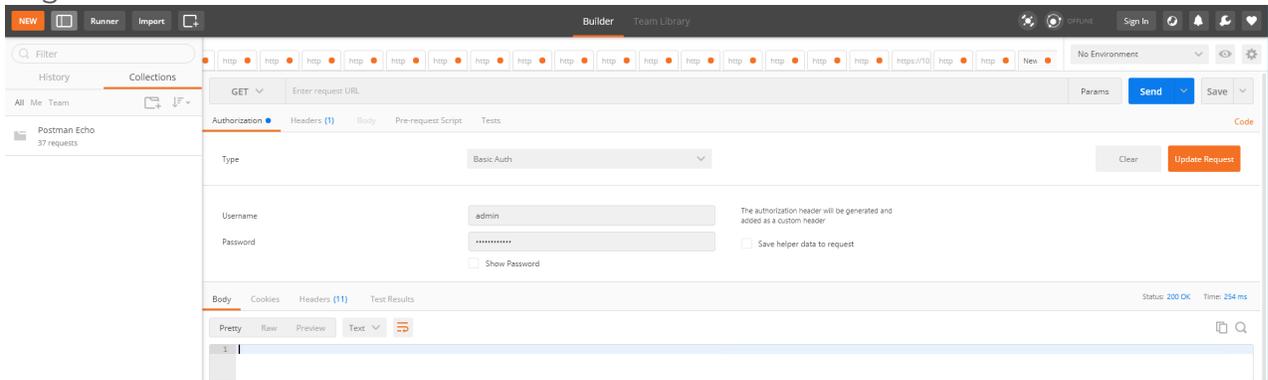


3. Delete all the existing Service Deployments.



To remove the Service Deployments through NSX-T API:

1. Login to Postman.

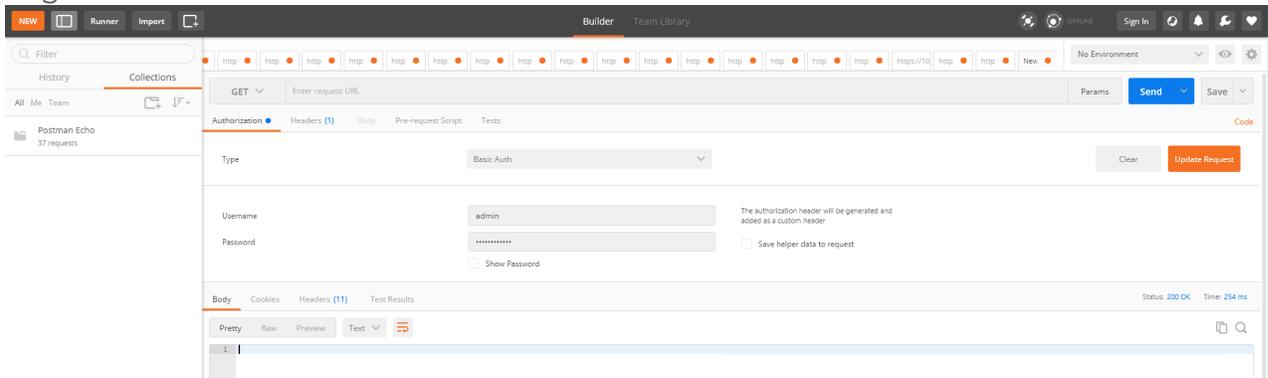


2. Get the Service ID.**GET** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/`
3. Get the ID of the Service Deployments.**GET** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/`
4. Delete all Service Deployments.**DELETE** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/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

Remove Service Reference

To remove Service References through NSX-T API:

1. Login to Postman.

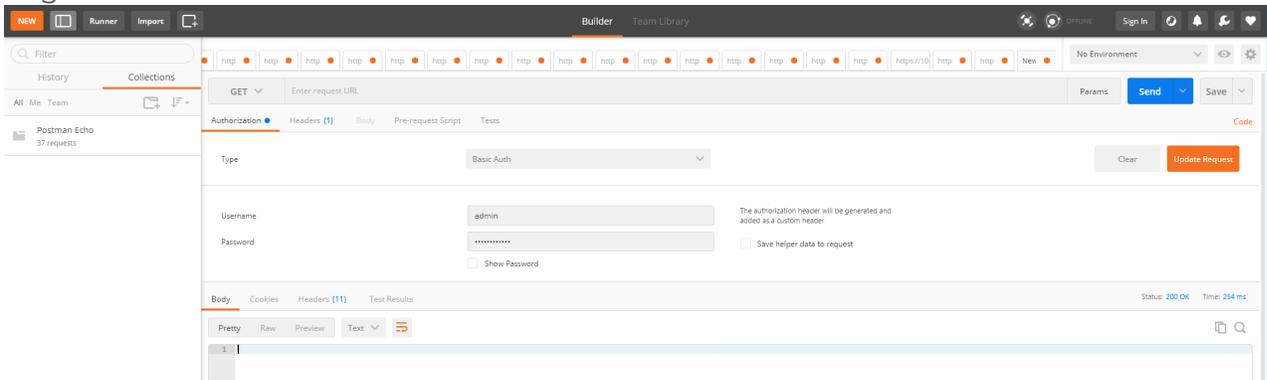


2. Get the Service Reference ID.**GET** `https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/`
3. Delete the Service Reference.**DELETE** `https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/<Service_Reference_ID>`

Remove Service Manager

To remove Service Manager through NSX-T API:

1. Login to Postman.

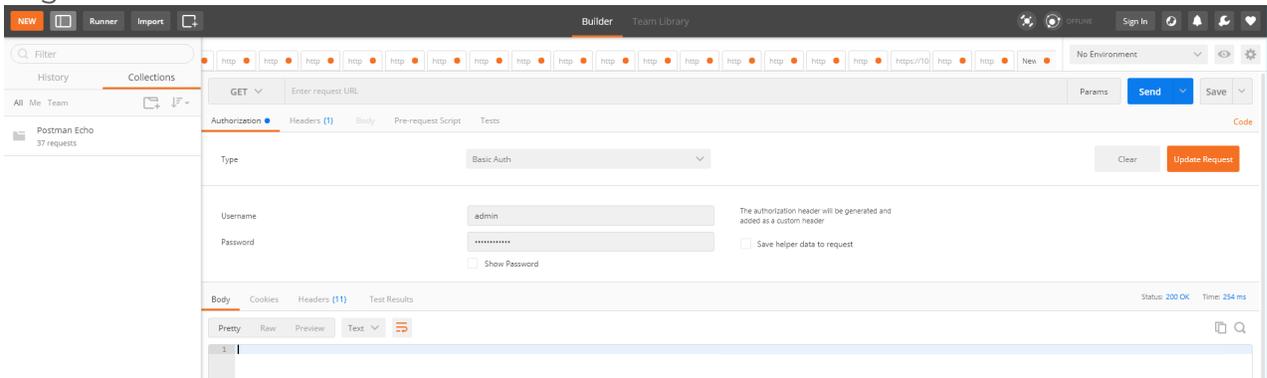


2. Get the Service Manager ID.**GET** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/service-managers/`
3. Delete the Service Manager.**DELETE** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/service-managers/<Service_Manager_ID>`

Remove Vendor Template and Service Definition

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

1. Login to Postman.



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 Gigamon 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 6.0 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
	*G-TAP A Series 2 Installation Guide
	GigaVUE-HC1 Hardware Installation Guide
	GigaVUE-HC2 Hardware Installation Guide
	GigaVUE-HC3 Hardware Installation Guide
	GigaVUE-HC1-PLUS Hardware Installation Guide
	GigaVUE M Series Hardware Installation Guide
	GigaVUE-TA25 Hardware Installation Guide

GigaVUE Cloud Suite 6.0 Hardware and Software Guides

GigaVUE-TA200 Hardware Installation Guide

GigaVUE-TA400 Hardware Installation Guide

GigaVUE-TA10 Hardware Installation Guide

GigaVUE-TA40 Hardware Installation Guide

GigaVUE-TA100 Hardware Installation Guide

GigaVUE-TA100-CXP Hardware Installation Guide

***GigaVUE-OS Installation Guide for DELL S4112F-ON**

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

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 Quick Start Guide

GigaVUE Cloud Suite for AWS—GigaVUE V Series 2 Guide

GigaVUE Cloud Suite for Azure—GigaVUE V Series 2 Guide

GigaVUE Cloud Suite for OpenStack—GigaVUE V Series 2 Guide

GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide

GigaVUE Cloud Suite for AnyCloud Guide

Universal Container Tap Guide

Gigamon Containerized Broker Guide

GigaVUE Cloud Suite for Kubernetes Guide

GigaVUE Cloud Suite for AWS—GigaVUE V Series 1 Guide

GigaVUE Cloud Suite 6.0 Hardware and Software Guides	
GigaVUE Cloud Suite for OpenStack—GigaVUE V Series 1 Guide	
GigaVUE Cloud Suite for Nutanix Guide	
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide	
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 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	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	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 Gigamon Community

The **Gigamon 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 Gigamon Community site to:

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

The Gigamon 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)