GigaVUE Cloud Suite for VMware–GigaVUE V Series Guide

GigaVUE Cloud Suite

Product Version: 5.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright 2021 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.

Document Version	Date Updated	Change Notes
1.0	12/22/2021	Original release of this document with 5.14.00 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 5
- Overview of GigaVUE V Series Node 6
  - Volume Based License (VBL) 6
- Configure V Series Node on ESXi 7
  - VMware ESXi System Requirements 8
  - Prerequisites for Integrating V Series Nodes with ESXi 10
  - Integrate V Series nodes with ESXi 10
- Configure V Series Node on NSX-T 31
  - Prerequisites for Integrating V Series Nodes with NSX-T 31
  - Recommended Form Factor (Instance Types) 33
  - Integrate V Series nodes with NSX-T 33
  - Remove Gigamon Service from NSX-T and GigaVUE-FM 57
- GigaVUE V Series Deployment Clean up 59
  - Remove Service Profiles 59
  - Remove Service Deployments 60
  - Remove Service Reference 61
  - Remove Service Manager 62
  - Remove Vendor Template and Service Definition 62
- Additional Sources of Information 64
  - Documentation 64
  - Documentation Feedback 67
  - Contact Technical Support 68
  - Contact Sales 68
  - The Gigamon Community 68

Glossary 70

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 (VBL)

All the V Series 2 nodes connected to GigaVUE-FM periodically reports the stats. GigaVUE-FM adds the required licensing tags into the Elasticsearch. All licensed applications, when running on the node, generate usage statistics. In the Volume-Based Licensing 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. You will have grace period for each license that are conveyed in the license file.

For purchasing licenses with the VBL option, contact our Gigamon Sales. Refer to Contact Sales.

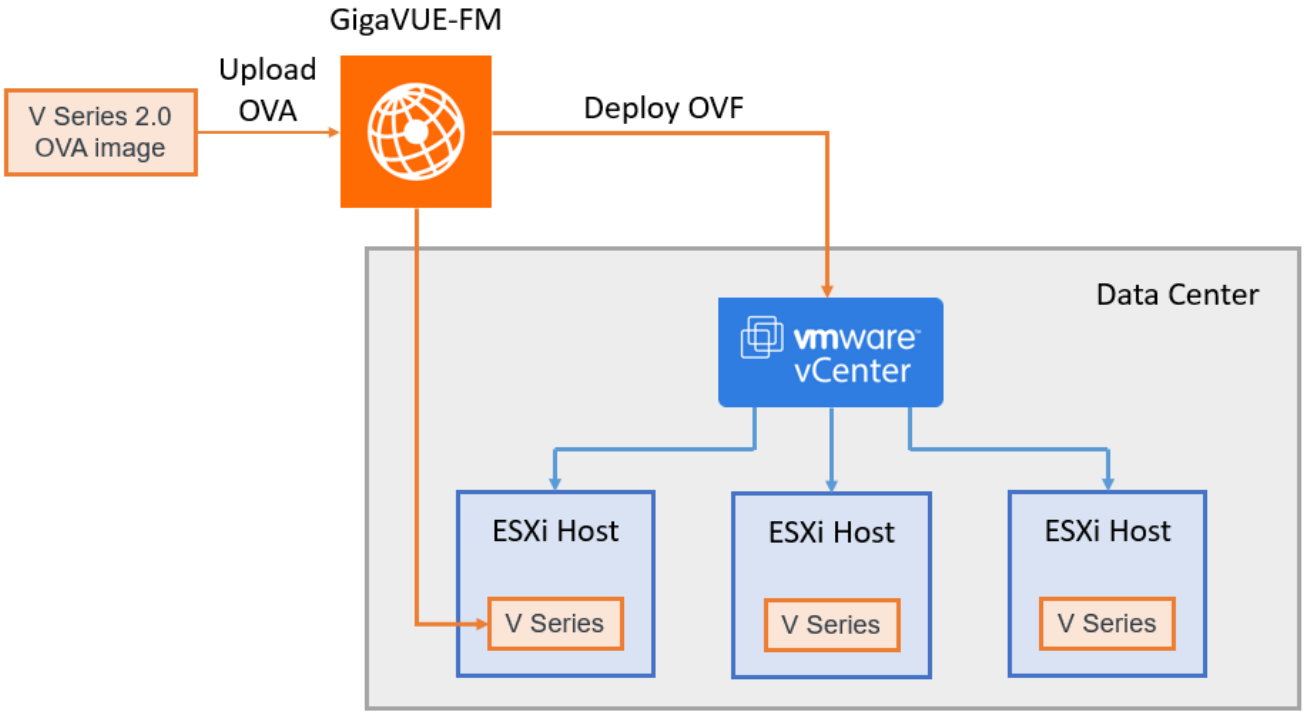
Configure V Series Node on ESXi

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.

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.

VMware ESXi System Requirements

Refer to the Release Notes for the hardware requirements on which VMware ESXi runs V Series Node.

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.

Direction	Type	Protocol	Port	Source/Destination	Purpose
GigaVUE-FM					
Inbound	• HTTPS • SSH	TCP	• 443 • 22	Administrator Subnet	Management connection to GigaVUE-FM
Outbound	HTTPS	TCP	443	All ESXi hosts IP and vCenter IP	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts and NSX-T managers to import the V Series OVA files
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with V Series node
V Series 2 node					
Inbound	Custom TCP Rule	TCP	8889	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series node
Inbound	• UDP • IP	• UDP (VXLAN) • GRE • UDPGRE	• 4789 • Protocol 47 • 4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom UDP Rule	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	• echo request • echo reply	Tool IP	Allows V Series node to health check tunnel destination traffic

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 **Roles > Administration > Role,** and then use the **Edit Role** dialog box in vCenter. 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
Host	Configuration ■ Network Configuration	VSS Tapping
	Inventory ■ Modify Cluster	Pin V Series Node to the host in cluster configurations. This prevents automatic migration.
Datastore	■ Allocate space	V Series Node Deployment
Distributed Switch	■ VSPAN Operation	VDS Tapping
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** ■ Add new disk ■ Add or remove device ■ Modify device settings	V Series Node Deployment V Series Node Deployment/VSS Tapping
	Interaction ■ Connect devices ■ Power on ■ Power Off	V Series Node Deployment V Series Node Deployment V Series Node Deployment
	Inventory ■ Create from existing ■ Remove	V Series Node Deployment V Series Node Deployment
	Provisioning ■ Clone virtual machine	V Series Node Deployment

Prerequisites for Integrating V Series Nodes with ESXi

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

- VMware vCenter ESXi Standard Version must be 6.7 u3, and 7.0.
- ESXi hosts must have the minimum vCPU and memory resources. 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.
- 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. Instances 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

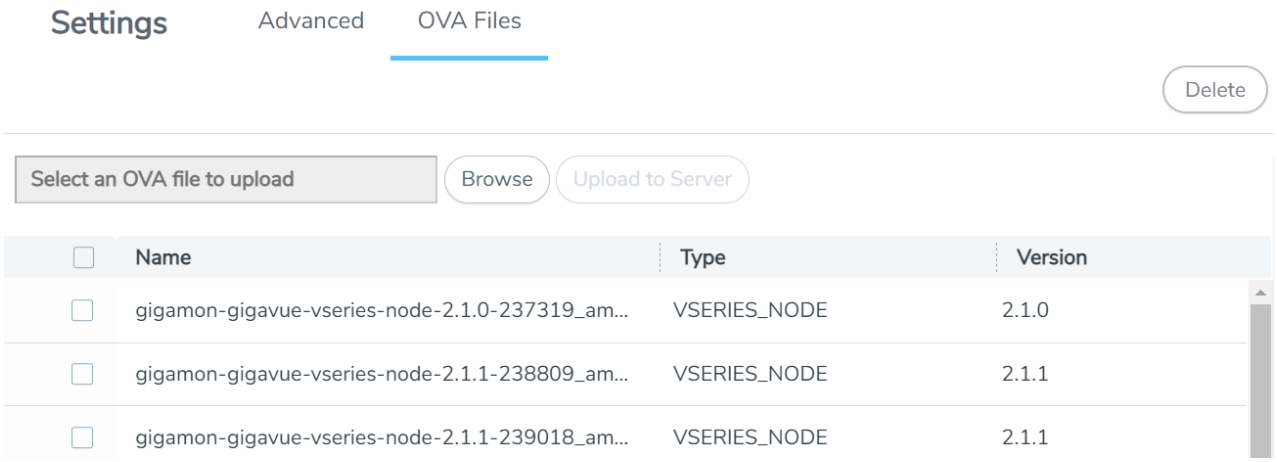
To integrate V Series nodes with ESXi, perform the following steps:

- Step 1: Upload V Series node Image into GigaVUE-FM
- Step 2: Deploy V Series nodes on VMware ESXi
- Step 3: 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.



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: Deploy V Series nodes on VMware ESXi

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

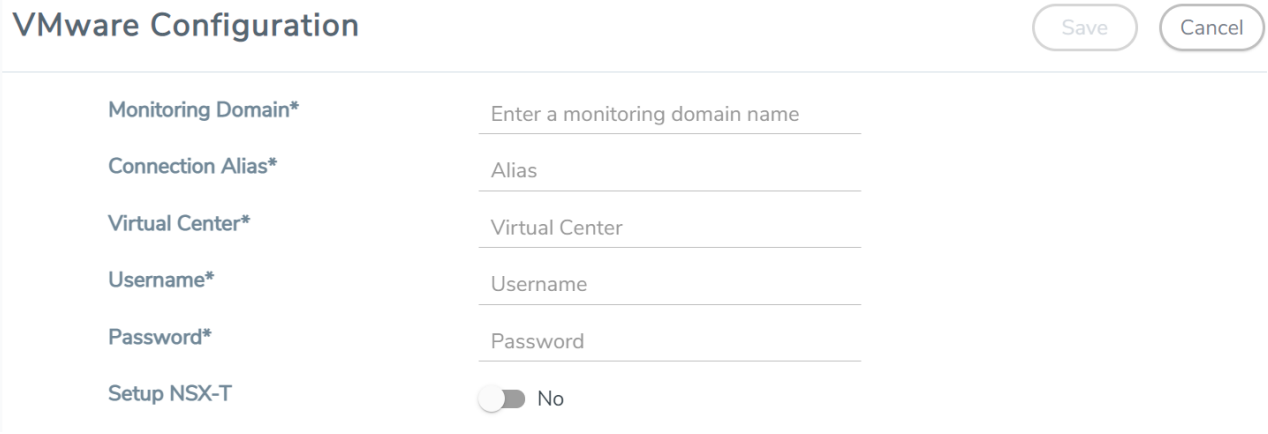
Refer to the following sections for details:

- Connect to VMware vCenter
- VMware Fabric Launch Configuration
- Upgrade V Series Node in GigaVUE-FM

Connect to VMware vCenter

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.



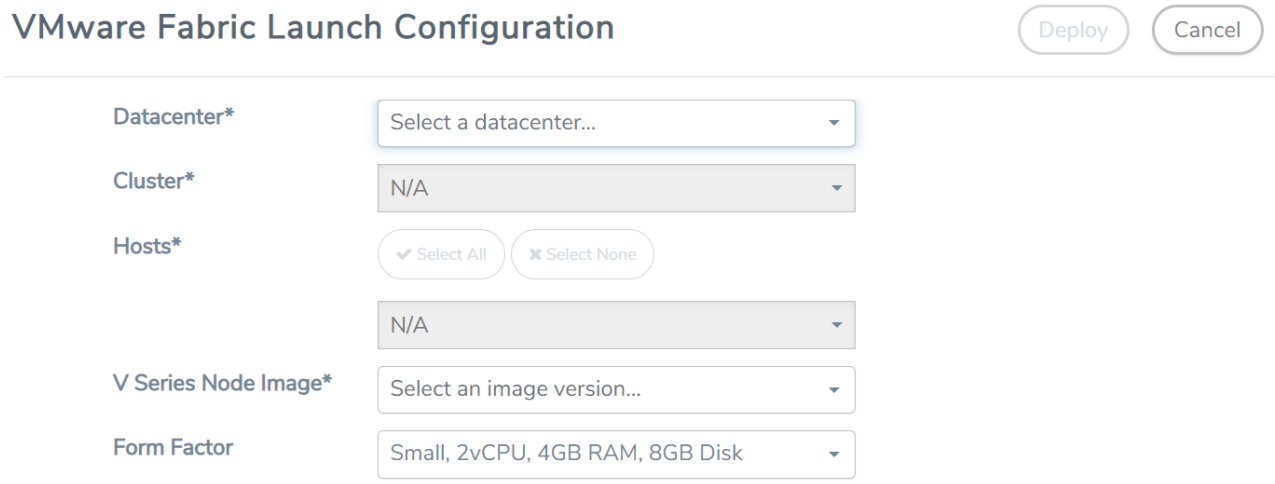
3. In the **VMware Configuration** page, enter or select the following details:

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
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.

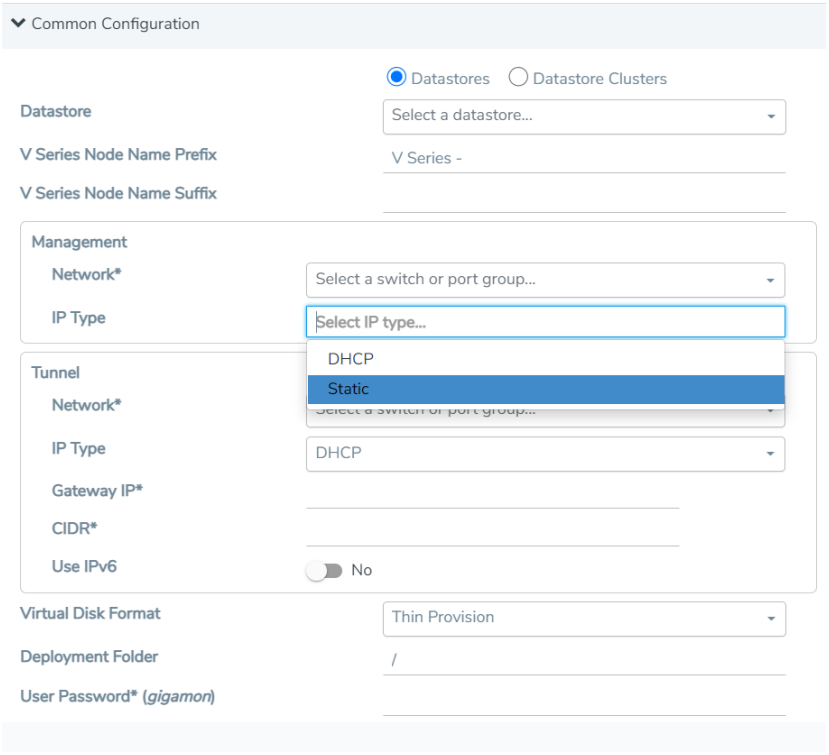
4. Click **Save**.

VMware Fabric Launch Configuration

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.



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	Select the ESXi hosts for V Series deployment. 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. Select the IP type as **Static** if you wish to deploy a node using Static IP address. 
V Series Node Image	Web server URL of the directory where V Series node OVA files to deploy V Series nodes are available.
Form Factor	Instance size of the V Series node. Refer Prerequisites for Integrating V Series Nodes with ESXi for more information.

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

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

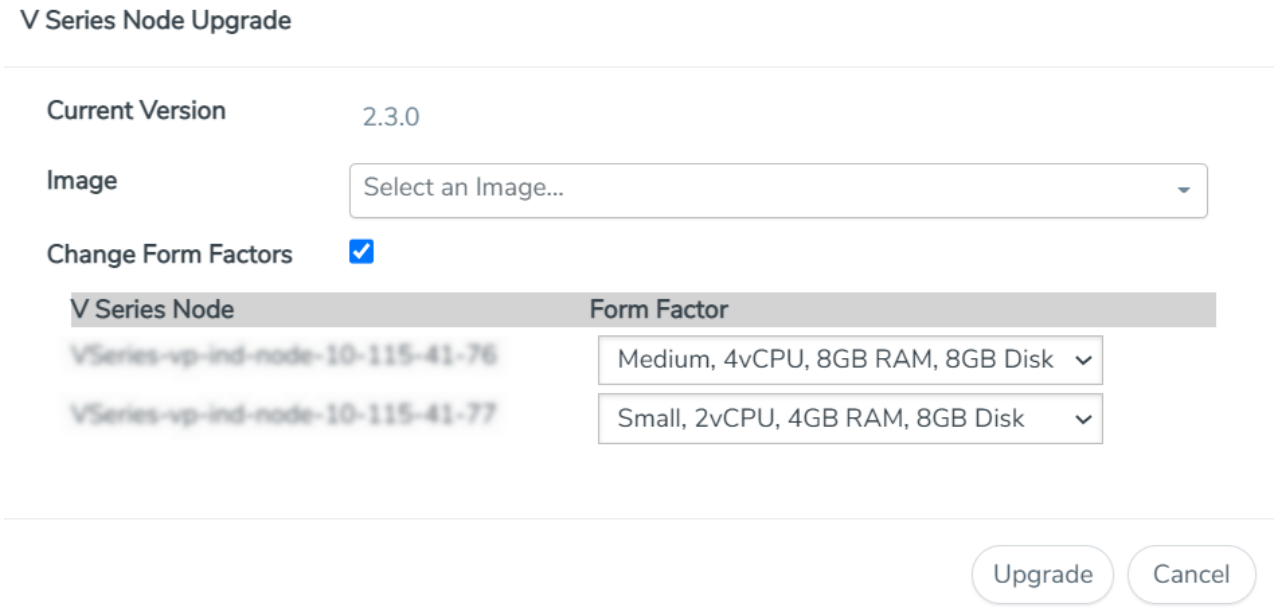
Upgrade V Series Node in GigaVUE-FM

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.

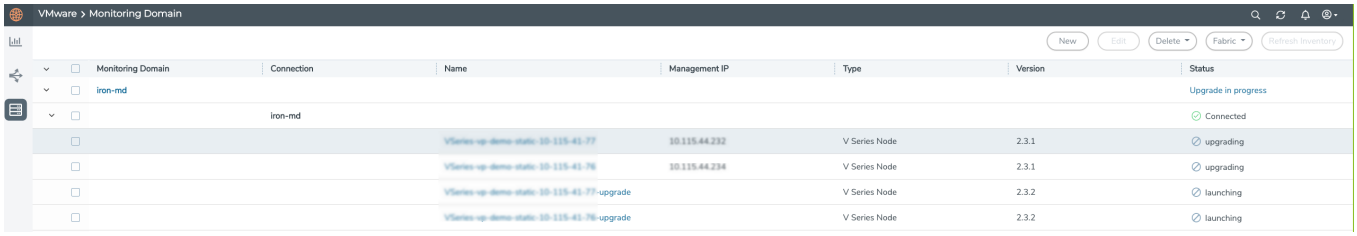


NOTE: All the V Series node with Static IP address retain their old IP address even after the upgrade.

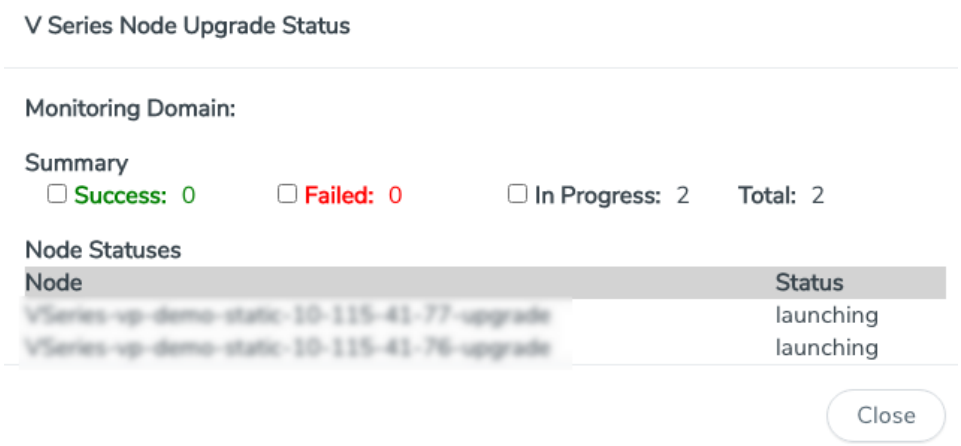
3. Enter the required information for all the available V Series nodes and click **Upgrade** to launch the V Series Node upgrade.

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.



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



- 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 3: 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
- Deploy Monitoring Session
- View Monitoring Session Statistics
- Visualize the Network Topology
- Configure VMware Settings

Create a Monitoring Session

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

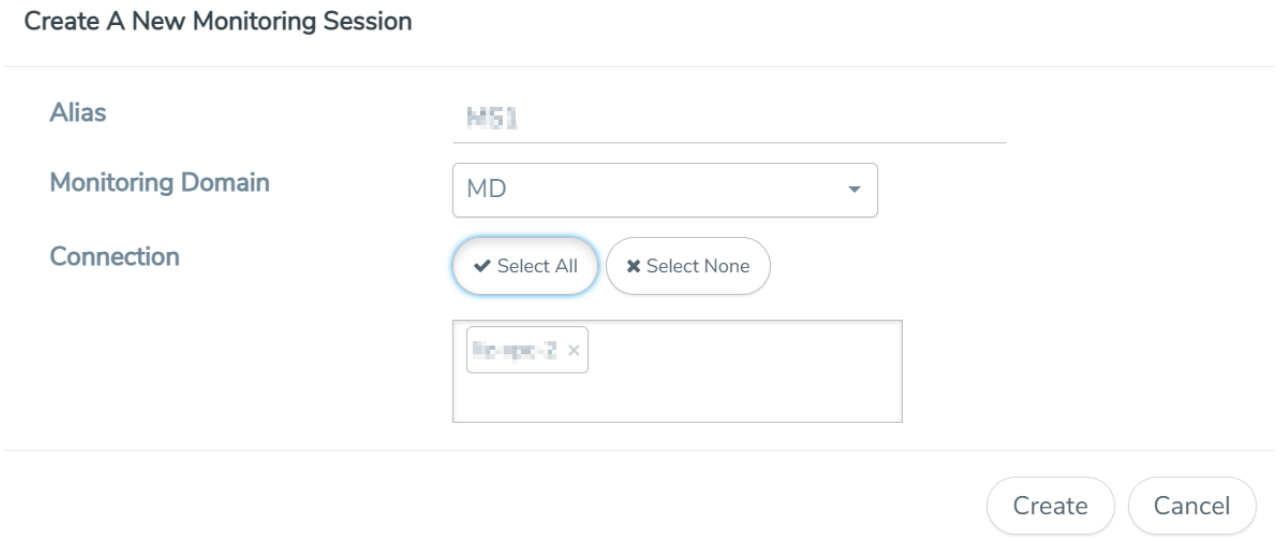
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

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

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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



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 a New 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. • 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. • 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.
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**.

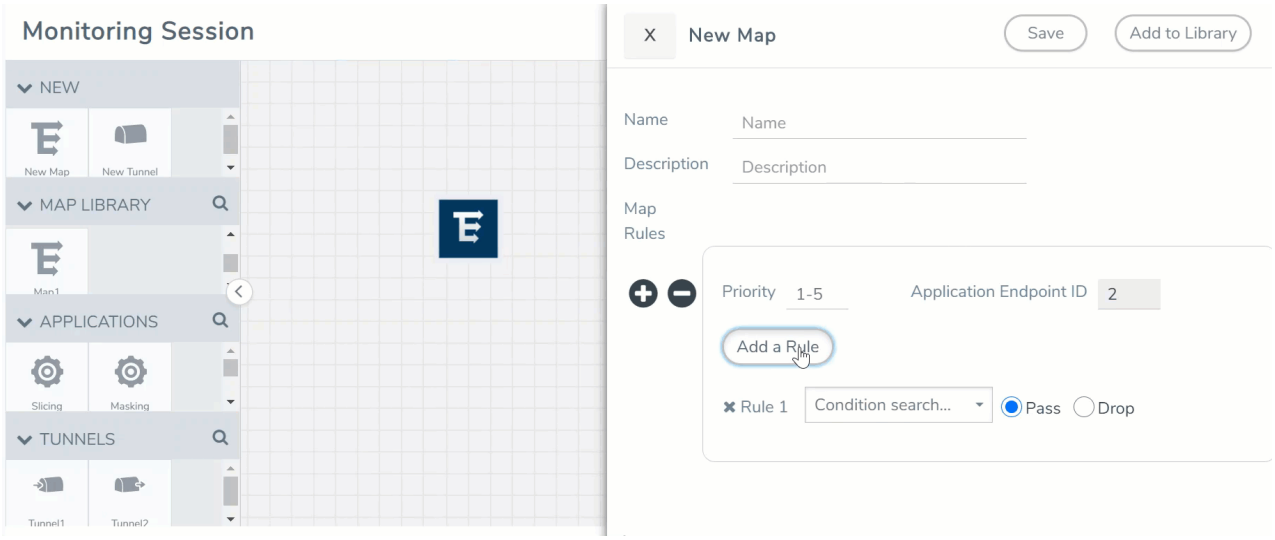
Create a New Map

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	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 maximum of 25 rules. To add ATS rules for a non Inclusion/Exclusion map, you must select atleaset one rule condition. To add a map rule: a. Enter a **Priority** value from 1 to 5 for the rule with 5 being the highest and 1 is the lowest priority. b. Click **Add a Rule**. The new rule field appear for the Application Endpoint. c. Select a required condition from the drop-down list. d. Select the rule to **Pass** or **Drop** through the map. If two rules with same condition are configured as pass and drop, • 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. For detailed information on filtering fragmented and unfragmented packets, refer to "GigaSMART Adaptive Packet Filtering (APF)" section on the *GigaVUE Fabric Management Guide*.

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

- Slicing
- Masking
- Dedup
- Load Balancing

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:

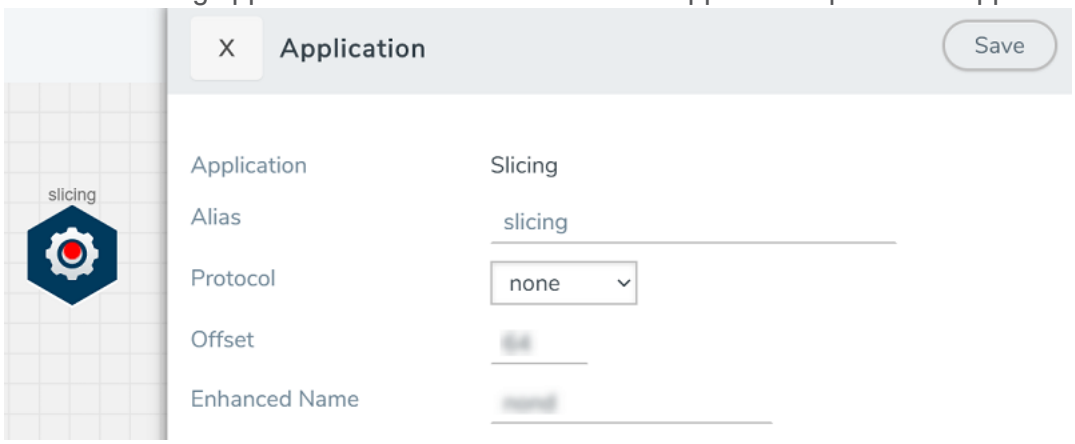
1. Drag and drop an application from **APPLICATIONS** to the canvas.
2. In the canvas, click the application and select **Details**.
3. Enter or select the required values for the selected application and click **Save**.

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.



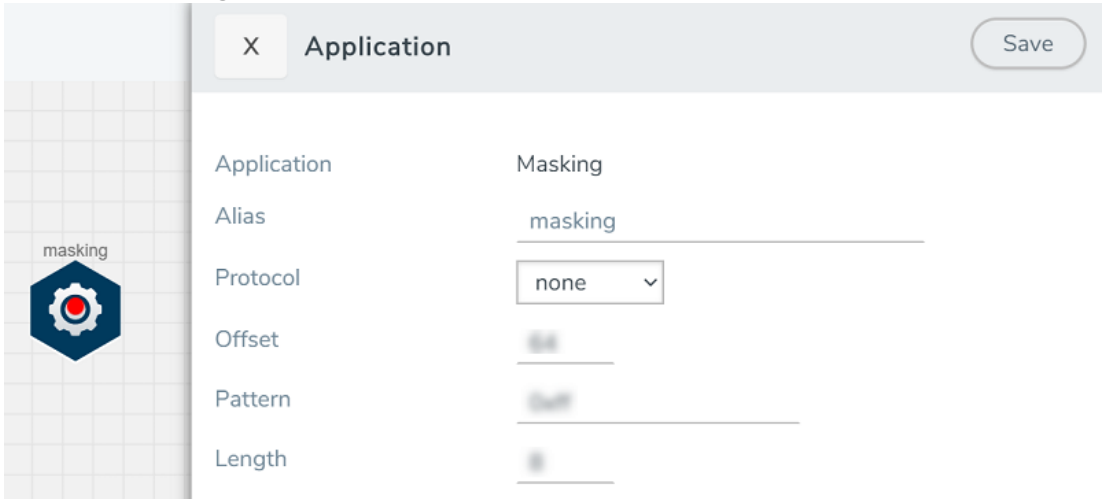
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the slicing.
   - From the **Protocol** drop-down list, specify an optional parameter for slicing the specified length of the protocol.
   - In the **Offset** field, specify the length of 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.



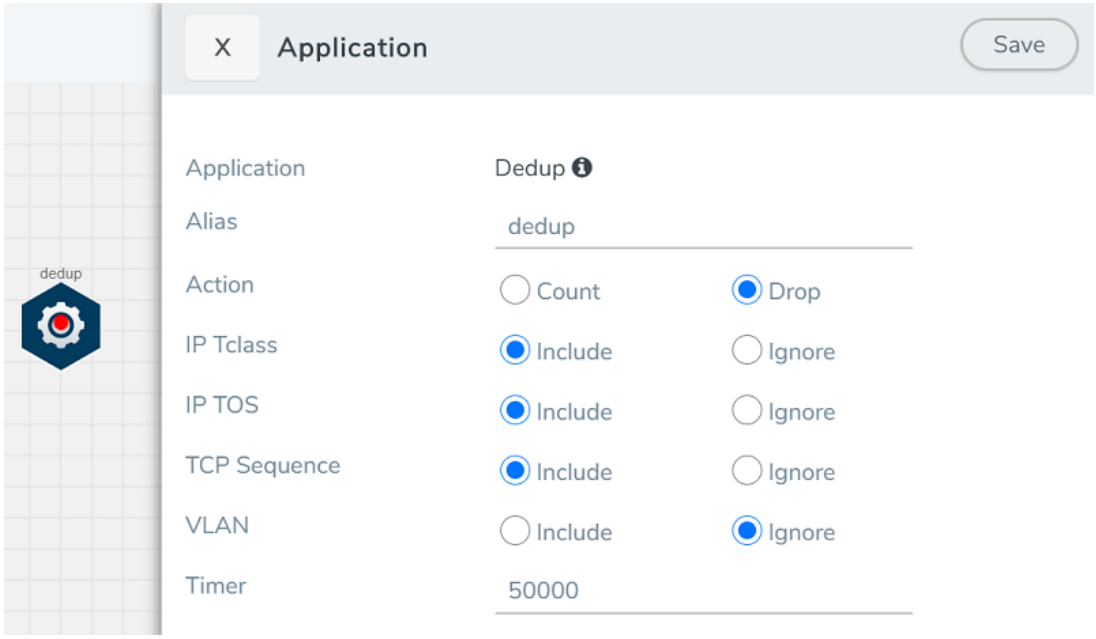
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the masking.
   - From the **Protocol** drop-down list, specify an optional parameter for masking the specified length of the protocol.
   - In the **Offset** field, specify the length of 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.



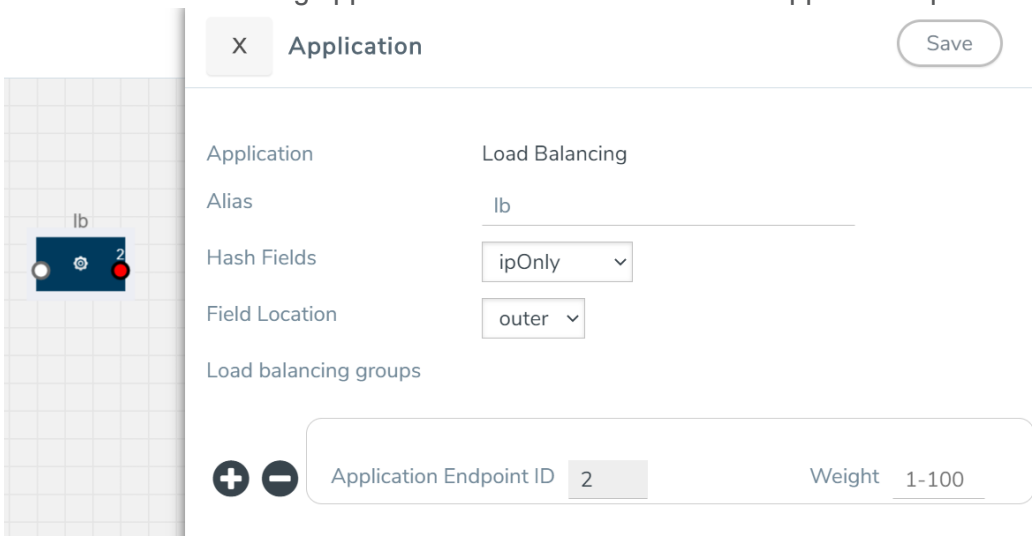
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the de-duplication.
   - In the Action field, select **Count** or **Drop** the detected duplicate packets.
   - For **IP Tclass**, **IP TOS**, **TCP Sequence**, and **VLAN** fields, select **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.



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**.

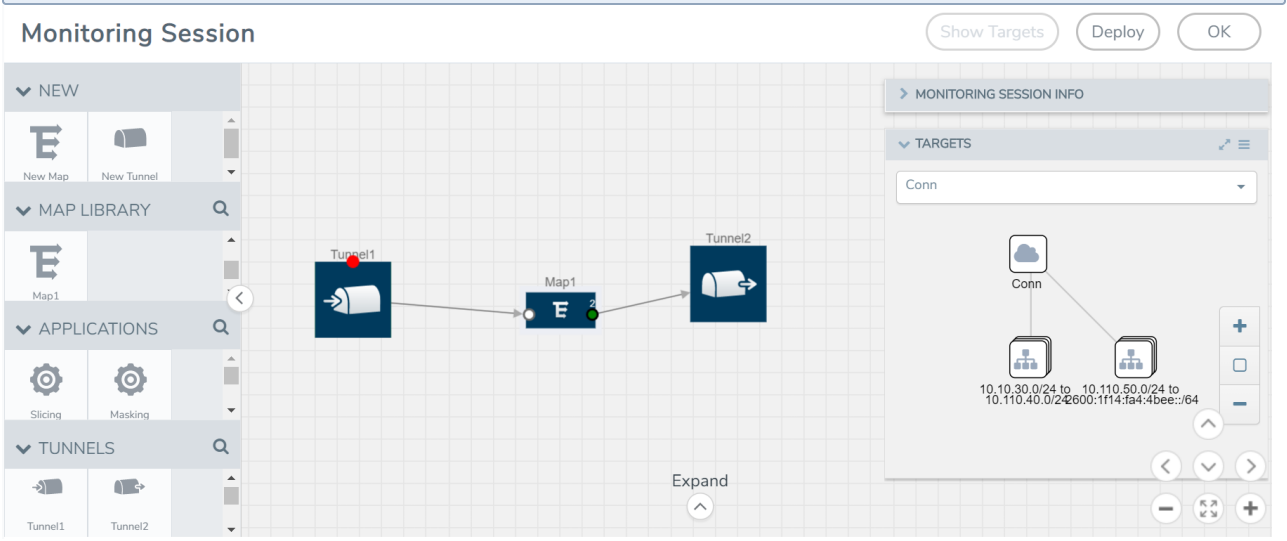
Deploy Monitoring Session

To deploy the monitoring session:

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

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

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



3. (Not applicable for NSX-T solution and 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:

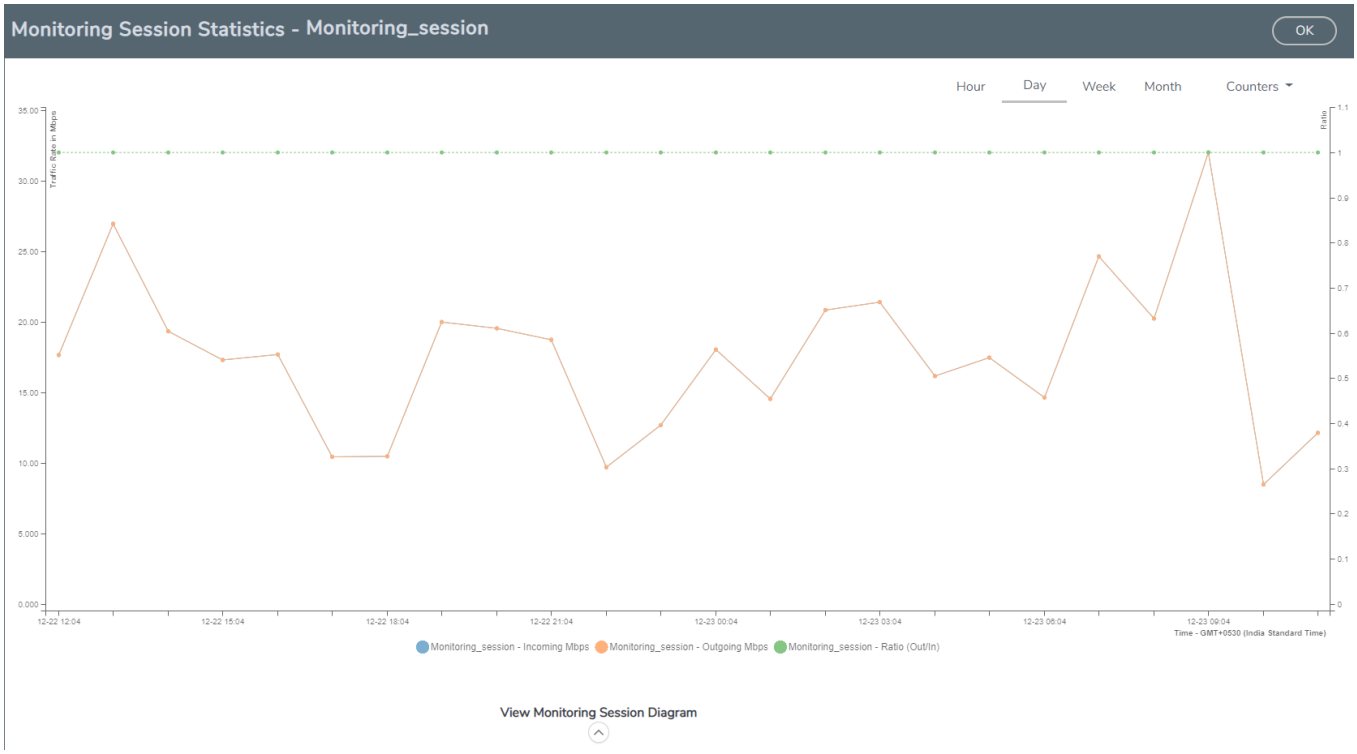
- **Undeploy**–Undeploys the selected monitoring session.
- **Clone**–Duplicates the selected monitoring session.
- **Edit**–Opens the Edit page for the selected monitoring session.
- **Delete**–Deletes the selected monitoring session.

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.

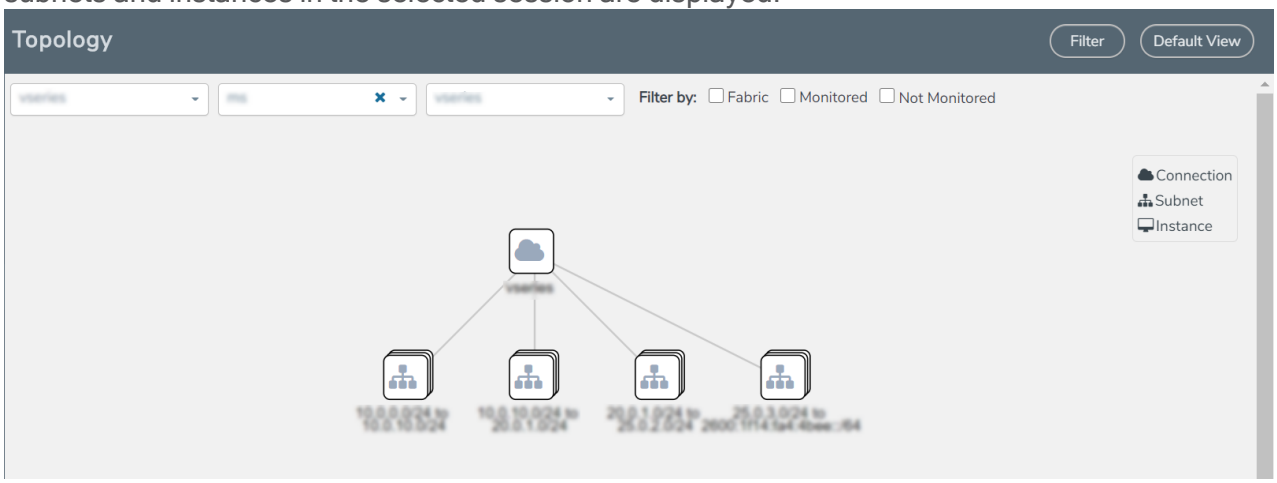
Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of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

Refer to the following table for details:

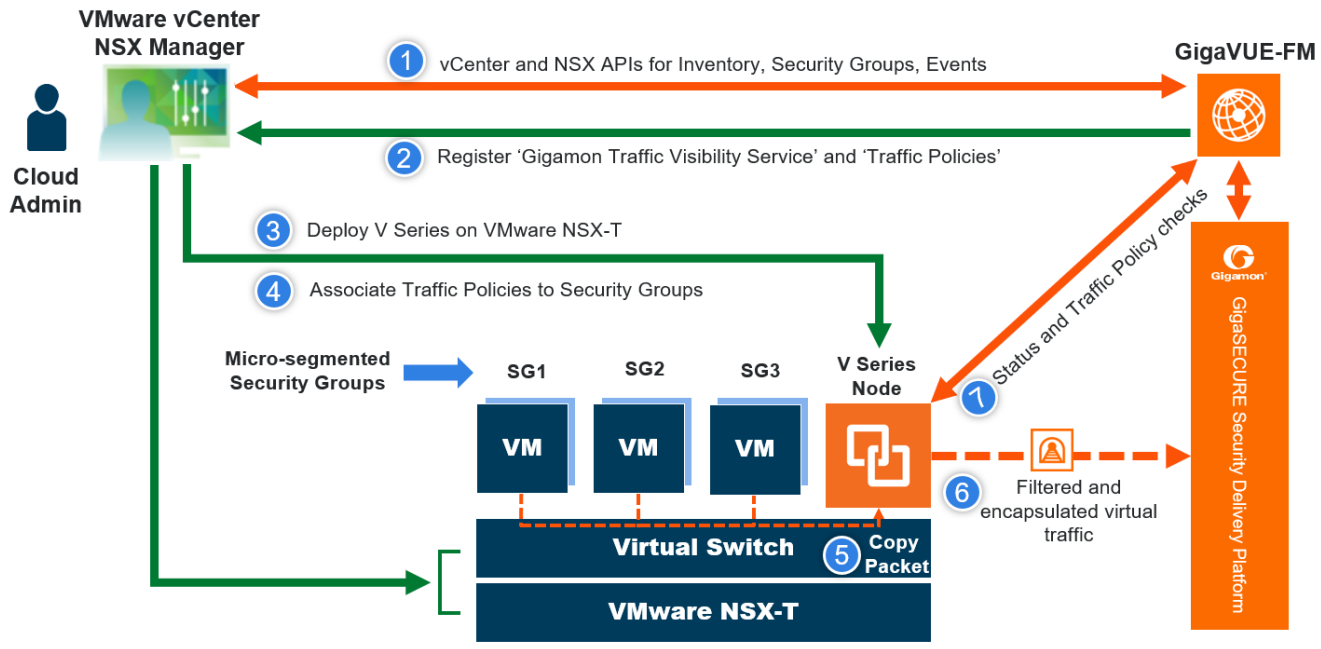
Settings	Description
Maximum number of vCenter connections allowed	Specifies the maximum number of vCenter connections you can establish in GigaVUE-FM
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the state of target VMs in VMware vCenter
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the state of GigaVUE-FM fabrics deployed in VMware vCenter

Configure 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:



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.

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 segments must be created in the NSX-T manager.
- NSX-T version must be 3.0.3 and 3.1.2.
- 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.
- All the target VMs must have VMware guest tools or Open VM tools.
- Port number 8889 must be available for GigaVUE-FM to access V Series nodes.

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.

Direction	Type	Protocol	Port	Source/Destination	Purpose
GigaVUE-FM					
Inbound	• HTTPS • SSH	TCP	• 443 • 22	Administrator Subnet	Management connection to GigaVUE-FM
Outbound	HTTPS	TCP	443	All ESXi hosts IP and vCenter IP	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts and NSX-T managers to import the V Series OVA files
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with V Series node
V Series 2 node					
Inbound	Custom TCP Rule	TCP	8889	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series node

Direction	Type	Protocol	Port	Source/Destination	Purpose
Inbound	• UDP • IP	• UDP (VXLAN) • GRE • UDPGRE	• 4789 • Protocol 47 • 4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom UDP Rule	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	• echo request • echo reply	Tool IP	Allows V Series node to health check tunnel destination traffic

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. Instances 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

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: Create a Service Segment in NSX-T
- Step 3: Deploy V Series nodes on VMware NSX-T
- Step 4: Configure Monitoring Sessions
- Step 5: 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-Tinventory 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 privilieges.

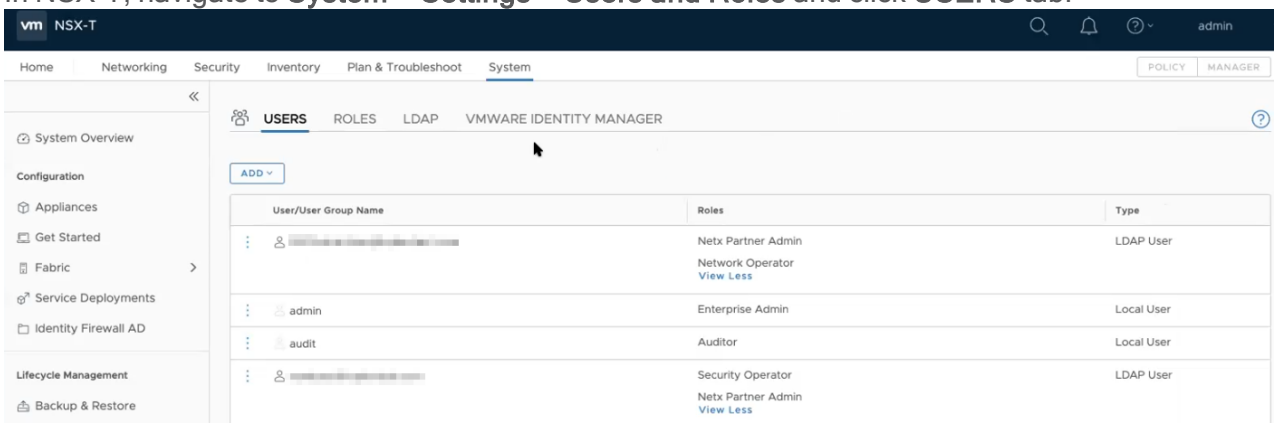
NOTE: GigaVUE-FM connects to NSX-T Manager that supports TLSv1.0, TLSv1.1, and TLSv1.2.

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.



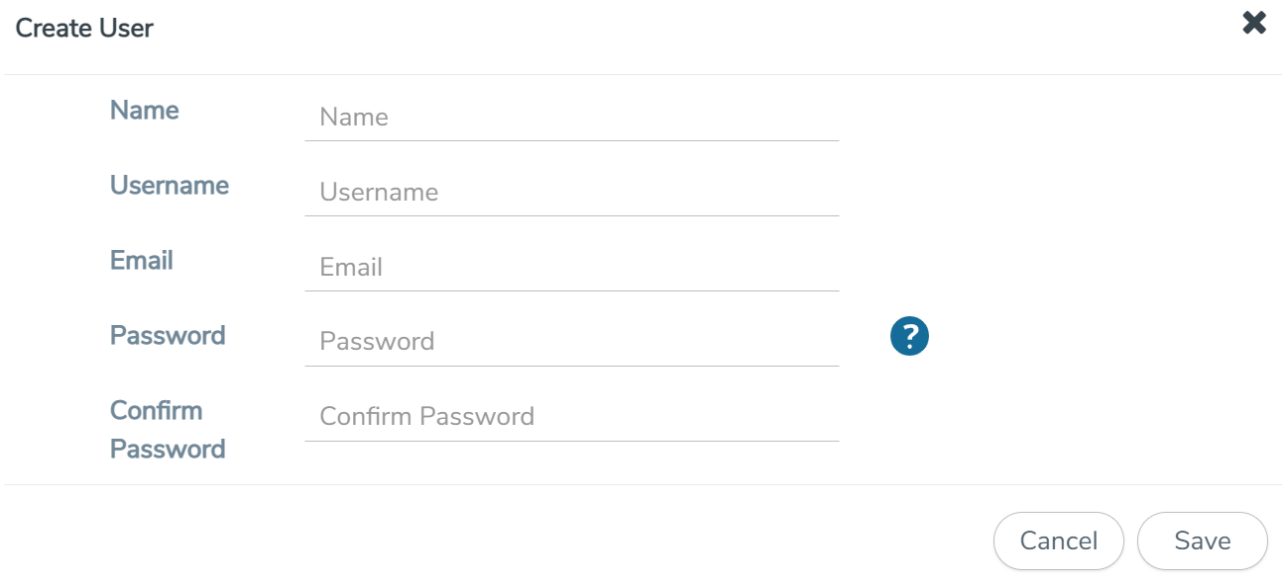
2. On the **USERS** tab, click **ADD** and then from the drop-down list,
   - for **NSX-T version 3.x**, select LDAP with one of the following Role combinations:
     - NETX Partner Administrator and Security Operator
     - NETX Partner Administrator and Network Operator
   - for **NSX-T version 2.x**, 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.

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



3. 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.
4. Click **Save**.

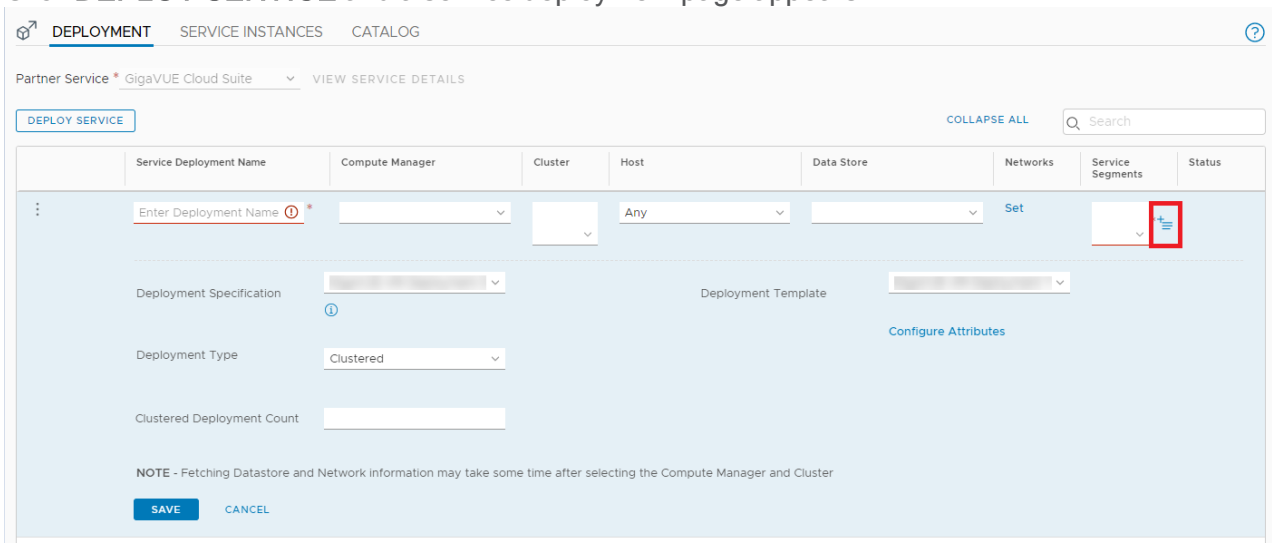
Step 2: Create a Service Segment in NSX-T

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

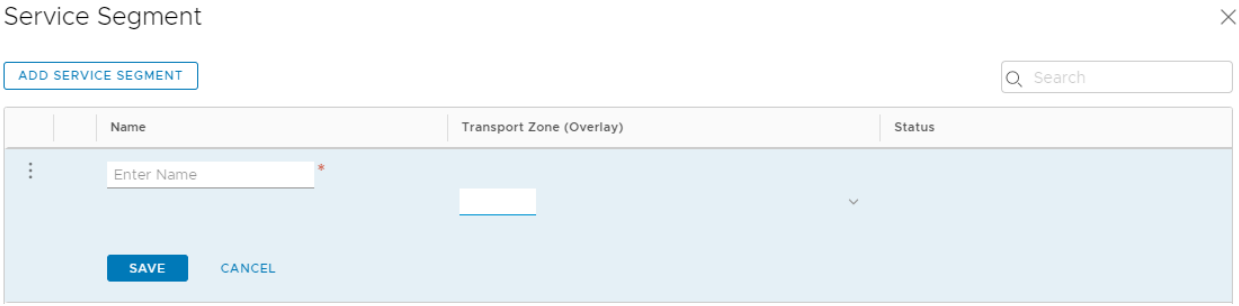
To create a service segment in VMware NSX-T:

1. On the NSX manager, go to **System > Service deployment > Deployment**. GigaVUE-FM and NSX-T must be synced to reflect the GigaVUE cloud suite as the partner service in NSX-T. On the same page, click the **View service details** link to check the version details.

2. Click **DEPLOY SERVICE** and a service deployment page appears.



3. On the Service Segments column, click **+** and the Service Segment page appears.
4. On the Service Segment page, click **ADD SERVICE SEGMENT** and a new row appears to create a service segment.



5. Enter the name and map it to the overlay transport zone created for the VMs.
6. 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
2. Open **/config/vmware/auth/ovf_validation.properties** file
3. Set a value for **THIRD_PARTY_OVFS_VALIDATION_FLAG** as **2**. The definition of the legends are as follows:
   - 0: only VMware-signed OVFs are allowed for deployment
   - 1: only VMware-signed and well-known CA-signed OVFs are allowed for deployment
   - 2: no validation
4. Save and Exit the file.

Step 3: Deploy V Series nodes on VMware NSX-T

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

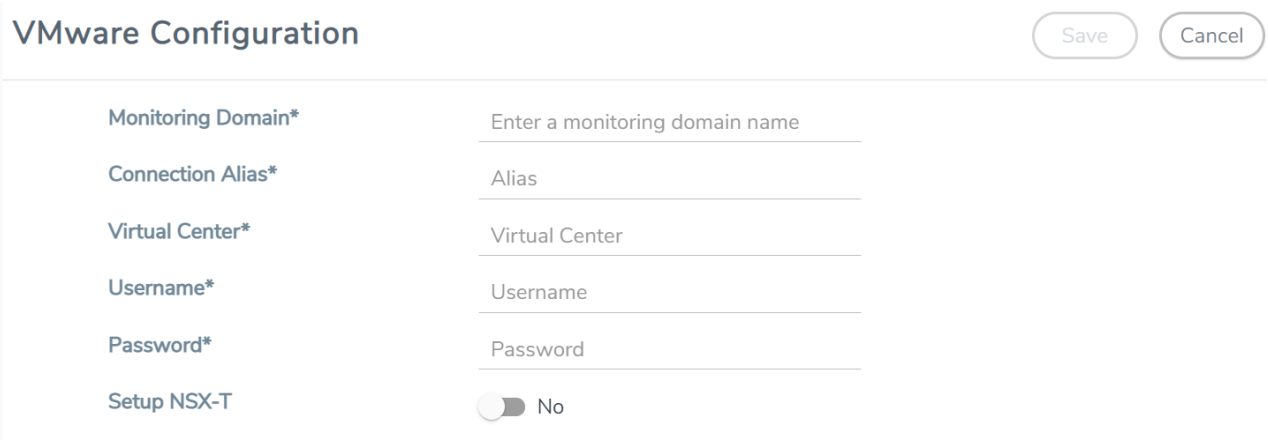
Refer to the following sections for details:

- Connect to VMware vCenter
- Deploy V Series fabric on VMware NSX-T
- Upgrade V Series Node in GigaVUE-FM

Connect to VMware vCenter

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.



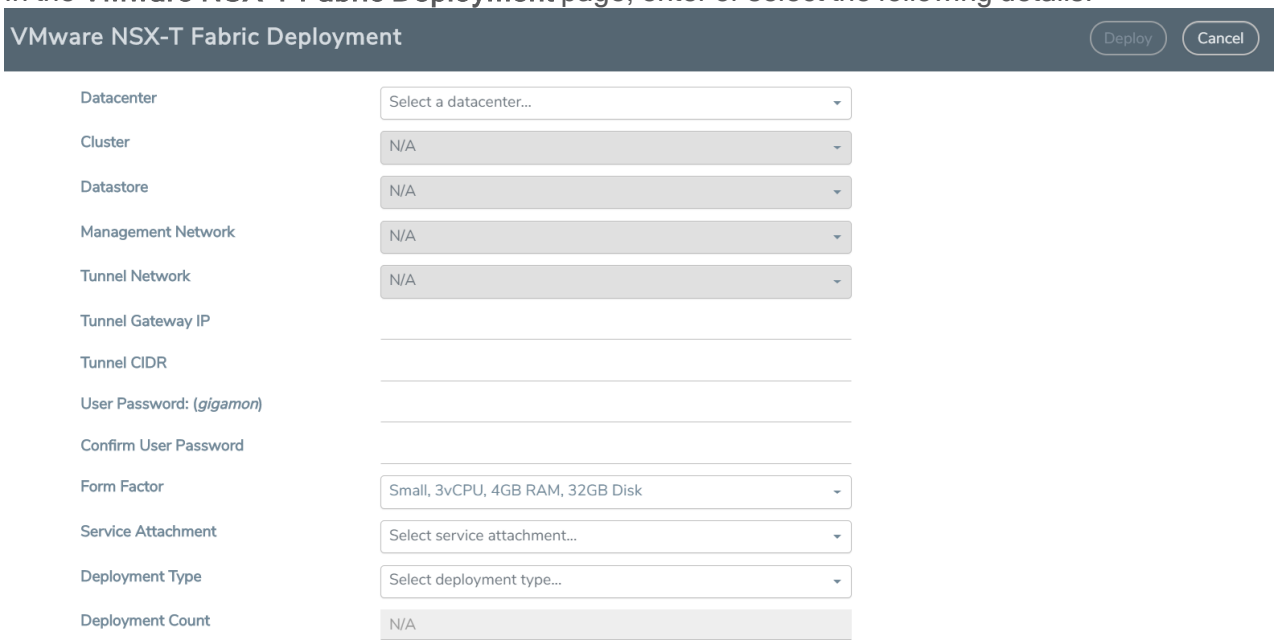
3. In the **VMware Configuration** page, enter or select the following details:

Field	Description
Monitoring Domain	Name of the monitoring domain
Connection Alias	Name of the connection
Virtual Center	IP address of the vCenter
Username	Username of the vCenter user with admin role privilege
Password	vCenter password used to connect to the vCenter
Setup NSX-T	**Enable** to setup NSX-T and the fields of NSX-T to appear. Enter or select the following details for NSX-T: • **NSX-T Manager:** IP address or Hostname of your VMware NSX-T. • **NSX-T Username:** Username of the your NSX-T account. • **NSX-T Password:** Password of the your NSX-T account. • The NSX-T user account must have admin privileges. • Each NSX-T manager can support a maximum of one monitoring domain. • **FM Username:** Username of the your GigaVUE-FM account. • **FM Password:** Password of the your GigaVUE-FM account. • **Image URL:** Web server URL of the directory where V Series node OVA, VMDK, and OVF files are available. The Web Server URL must be in the follwoing format: *http://<server-IP:port>/<path to where the OVF files are saved>* and the port can be any valid number. The default port number is 80. **NOTE:** Before VMware Configuration, all the contents of the OVA file must be extracted and placed in the directory which represents the Image URL.

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

Deploy V Series fabric on VMware NSX-T

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



Field	Description
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
Tunnel Network	Tunnel Network for the V Series nodes
Tunnel Gateway IP	IP address of the Tunnel Gateway
Tunnel CIDR	CIDR value of the Tunnel
User Password: (gigamon)	SSH Password of the V Series node
Form Factor	Instance size of the V Series node
Service Attachment	Service segment created on NSX-T
Deployment Type	Type of V series node deployment. You can select Clustered or Host Based deployment type
Deployment Count (for Clustered deployment type)	Number of V Series nodes (Service Instances) to deploy

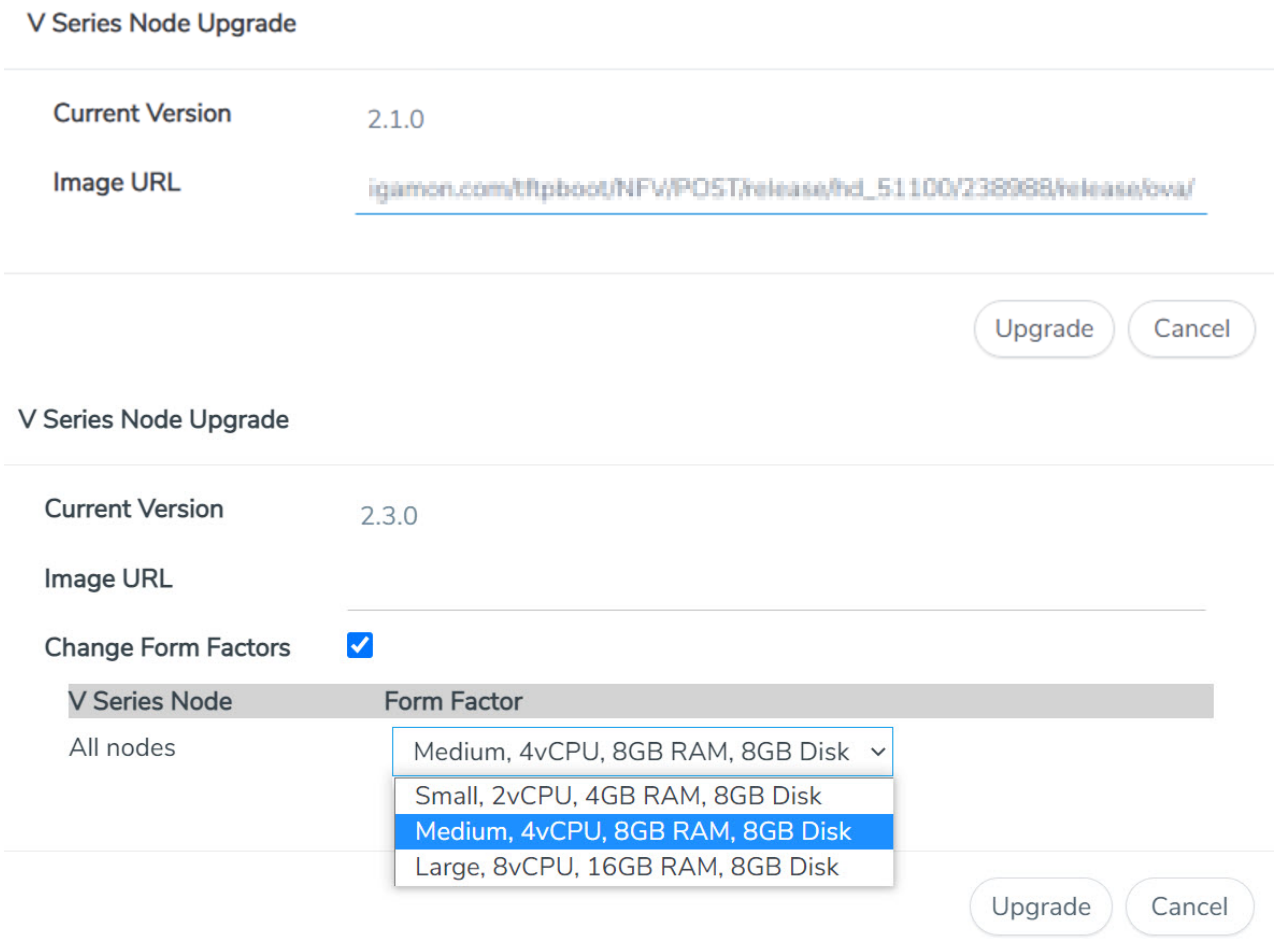
2. Click **Deploy**. After the V series node is deployed in vCenter, it appears on the Monitoring Domain page under Fabric tab of the selected Monitoring Domain.

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.

Upgrade 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.

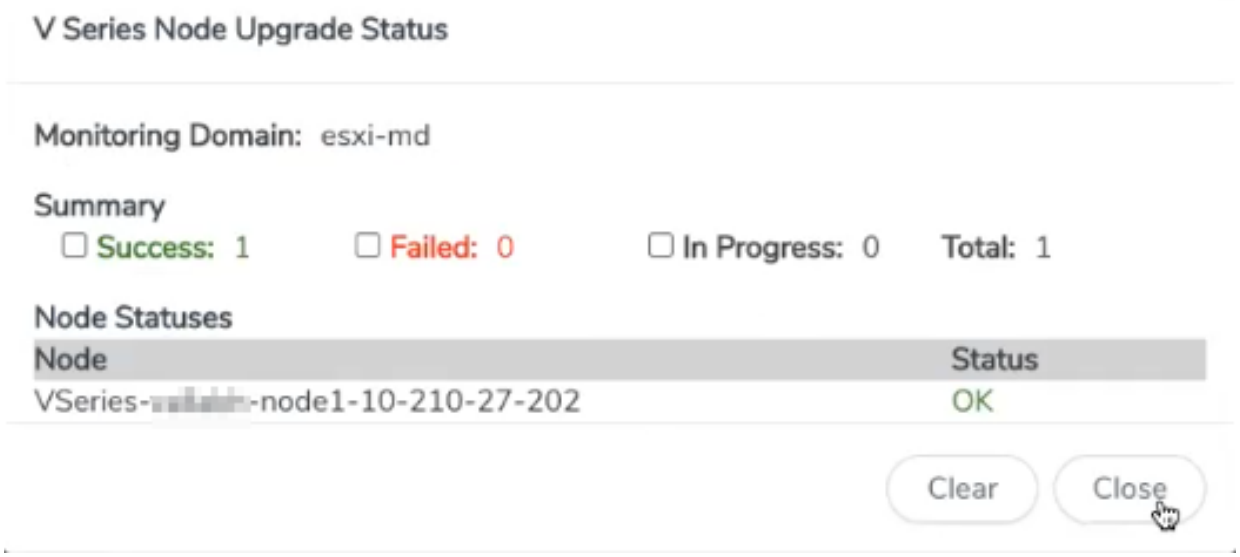


3. Enter the **Image URL** of the latest V Series Node OVA image. Click the **Change Form Factors** check box to modify the form factor (instance) size.

   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**.

4. 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.



Click **Clear** to delete the logs 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.

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 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.

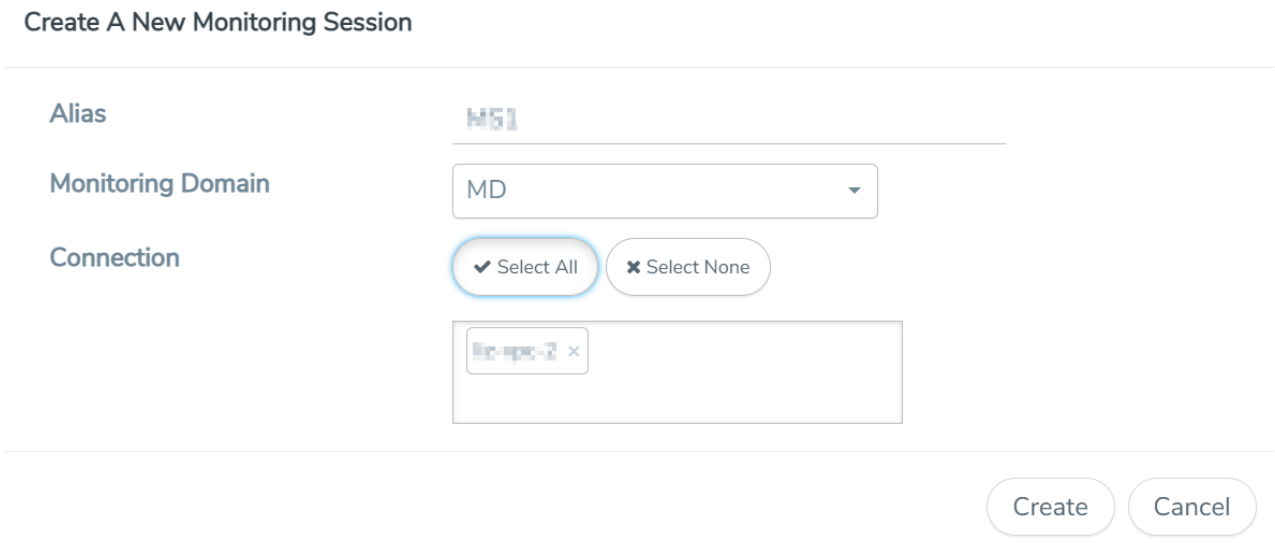
When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

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.



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 a New 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. • 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. • 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.
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**.

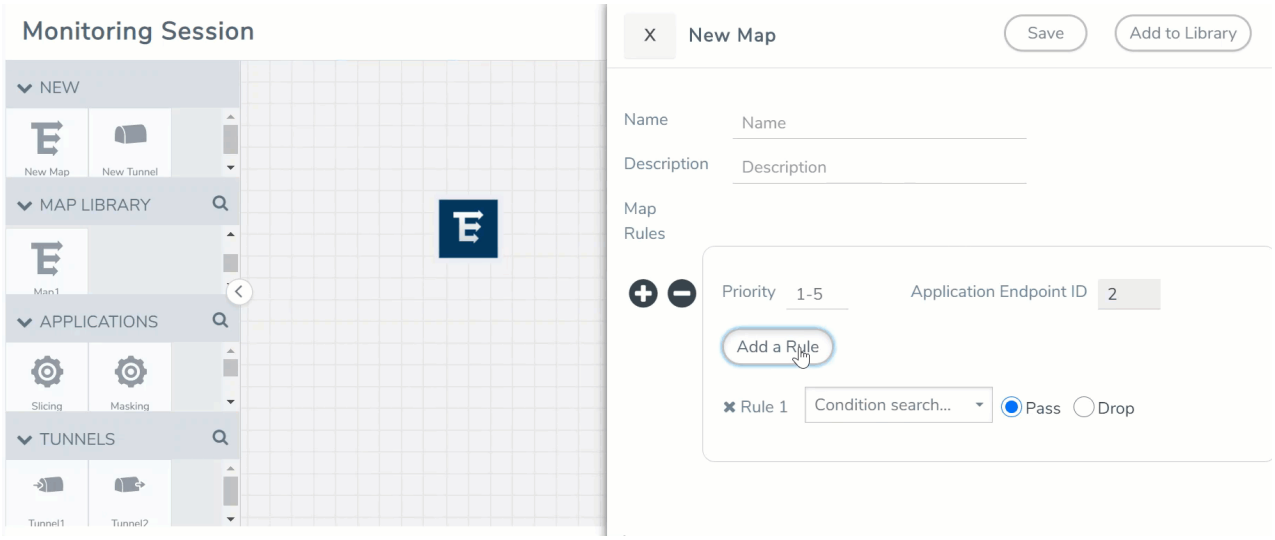
Create a New Map

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	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 maximum of 25 rules. To add ATS rules for a non Inclusion/Exclusion map, you must select atleaset one rule condition. To add a map rule: a. Enter a **Priority** value from 1 to 5 for the rule with 5 being the highest and 1 is the lowest priority. b. Click **Add a Rule**. The new rule field appear for the Application Endpoint. c. Select a required condition from the drop-down list. d. Select the rule to **Pass** or **Drop** through the map. If two rules with same condition are configured as pass and drop, • 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. For detailed information on filtering fragmented and unfragmented packets, refer to "GigaSMART Adaptive Packet Filtering (APF)" section on the *GigaVUE Fabric Management Guide*.

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

- Slicing
- Masking
- Dedup
- Load Balancing

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:

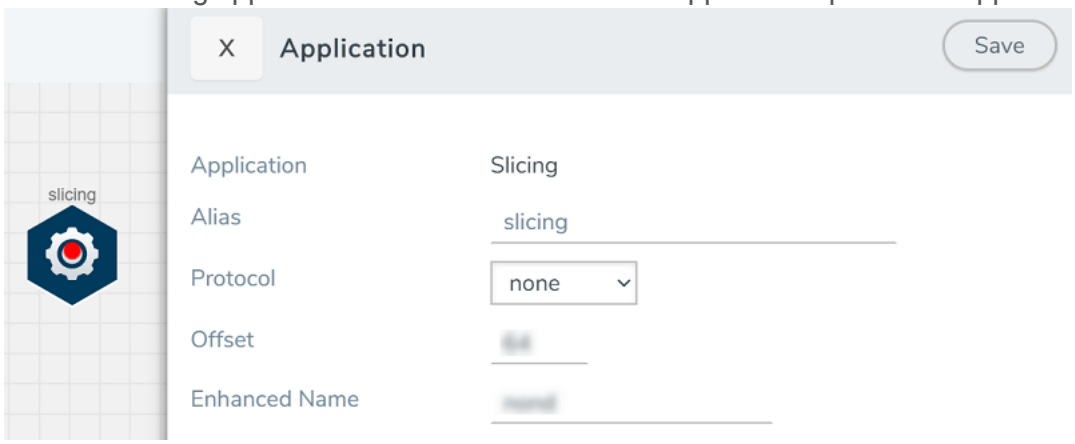
1. Drag and drop an application from **APPLICATIONS** to the canvas.
2. In the canvas, click the application and select **Details**.
3. Enter or select the required values for the selected application and click **Save**.

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.



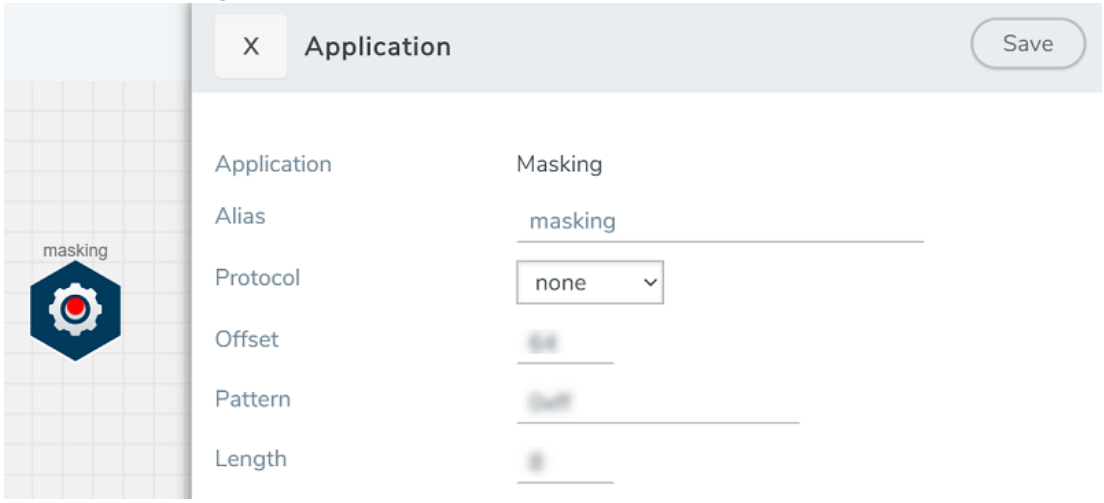
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the slicing.
   - From the **Protocol** drop-down list, specify an optional parameter for slicing the specified length of the protocol.
   - In the **Offset** field, specify the length of 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.



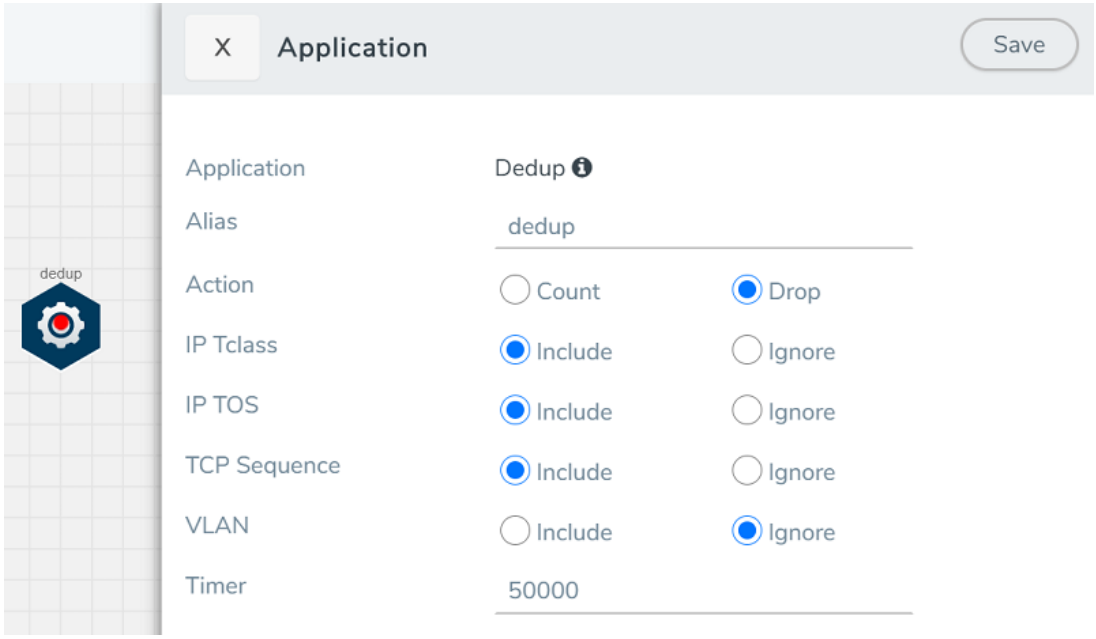
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the masking.
   - From the **Protocol** drop-down list, specify an optional parameter for masking the specified length of the protocol.
   - In the **Offset** field, specify the length of 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.



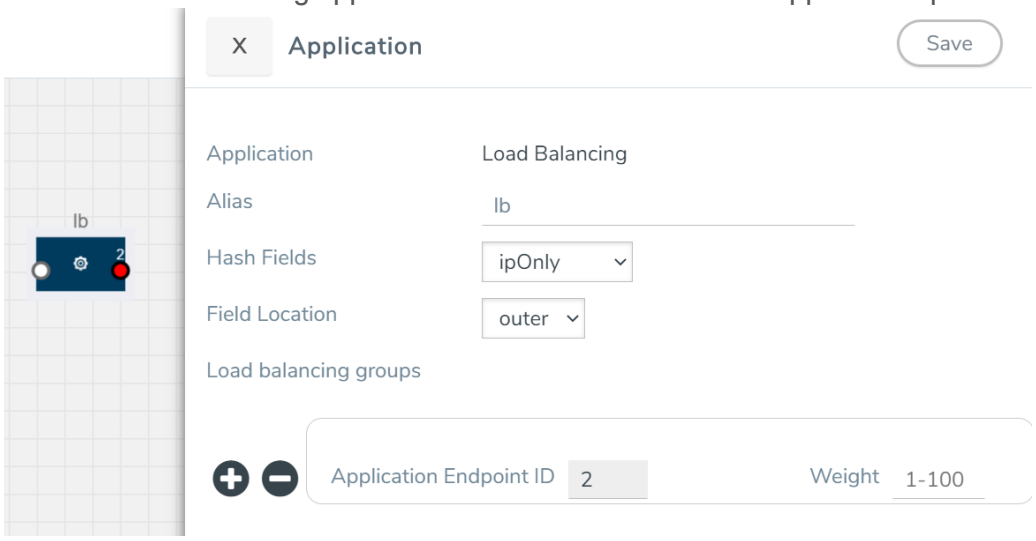
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the de-duplication.
   - In the Action field, select **Count** or **Drop** the detected duplicate packets.
   - For **IP Tclass**, **IP TOS**, **TCP Sequence**, and **VLAN** fields, select **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.



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**.

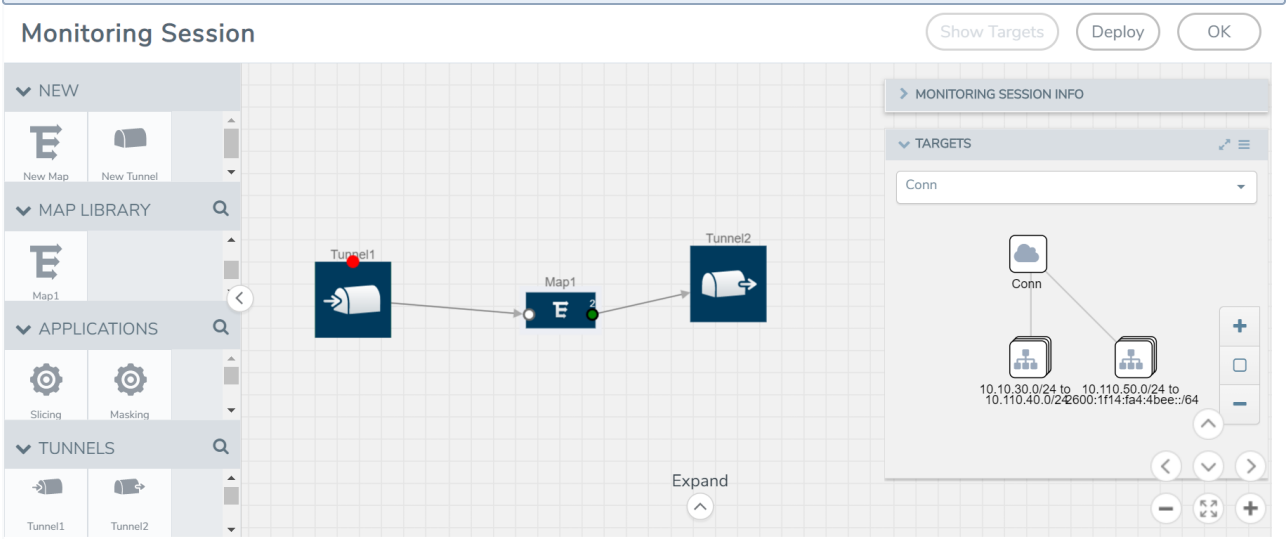
Deploy Monitoring Session

To deploy the monitoring session:

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

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

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



3. (Not applicable for NSX-T solution and 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:

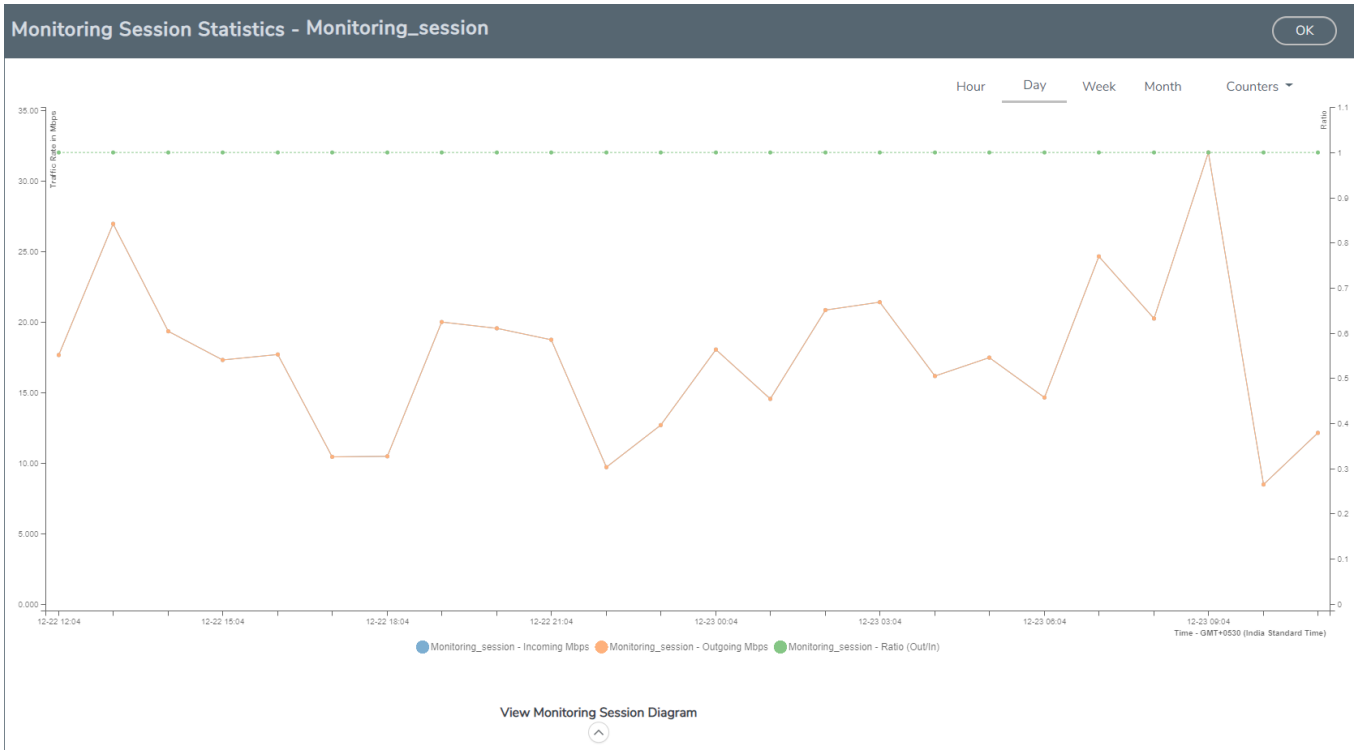
- **Undeploy**–Undeploys the selected monitoring session.
- **Clone**–Duplicates the selected monitoring session.
- **Edit**–Opens the Edit page for the selected monitoring session.
- **Delete**–Deletes the selected monitoring session.

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.

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.

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 5: Create NSX-T Group and Service Chain

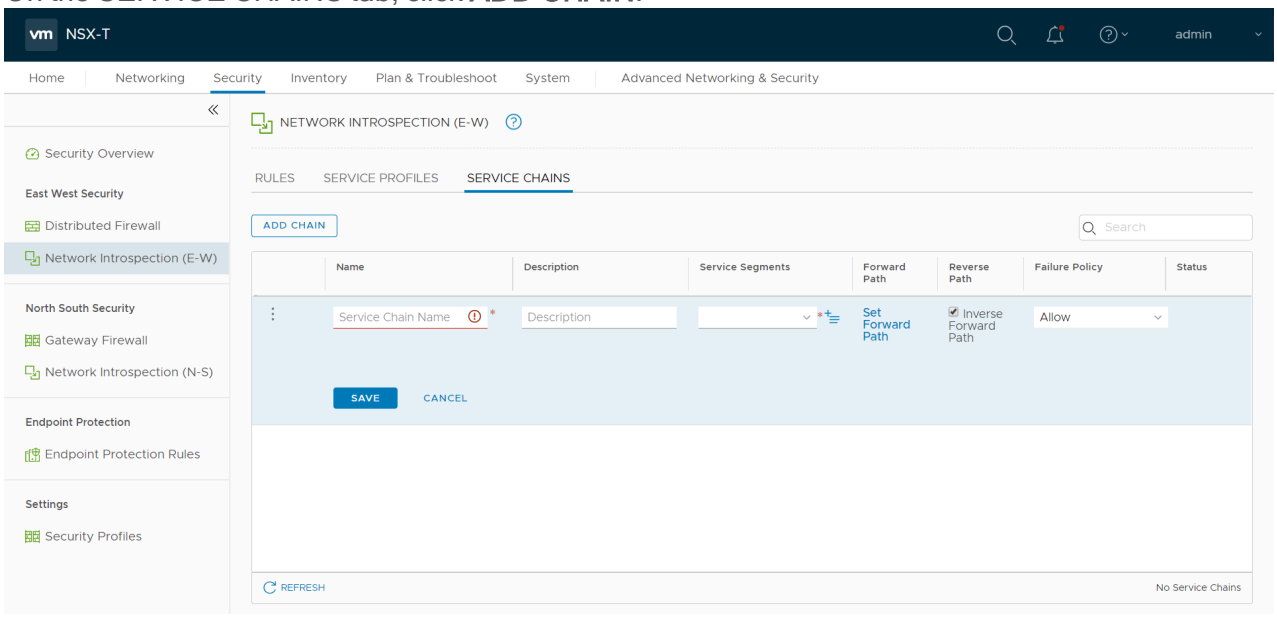
An NSX-T group and service chain must be created to redirect network traffic to the GigaVUE Cloud Suite. An NSX-T group defines which VMs are to be monitored. The service chain associates the GigaVUE Cloud Suite and map profile to the group.

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 > Network Introspection (E-W)** 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.

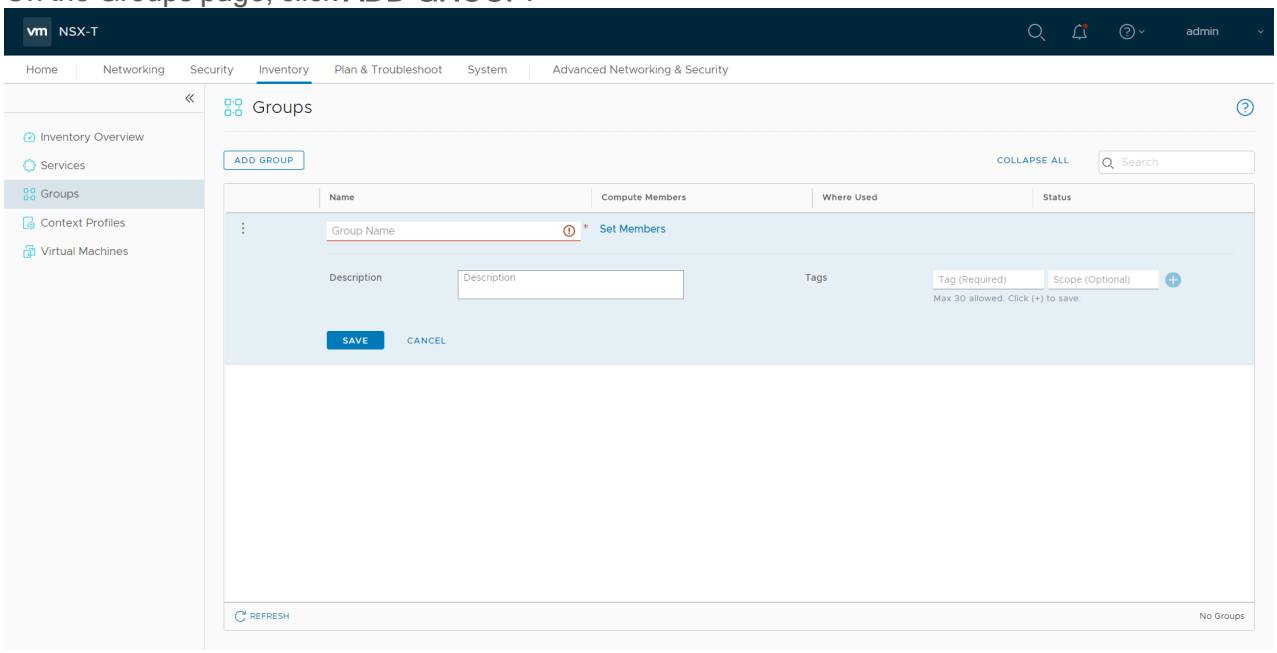
The new Service Chain is then updated in the **NSX-T Virtual Maps** page of GigaVUE-FM.

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**.



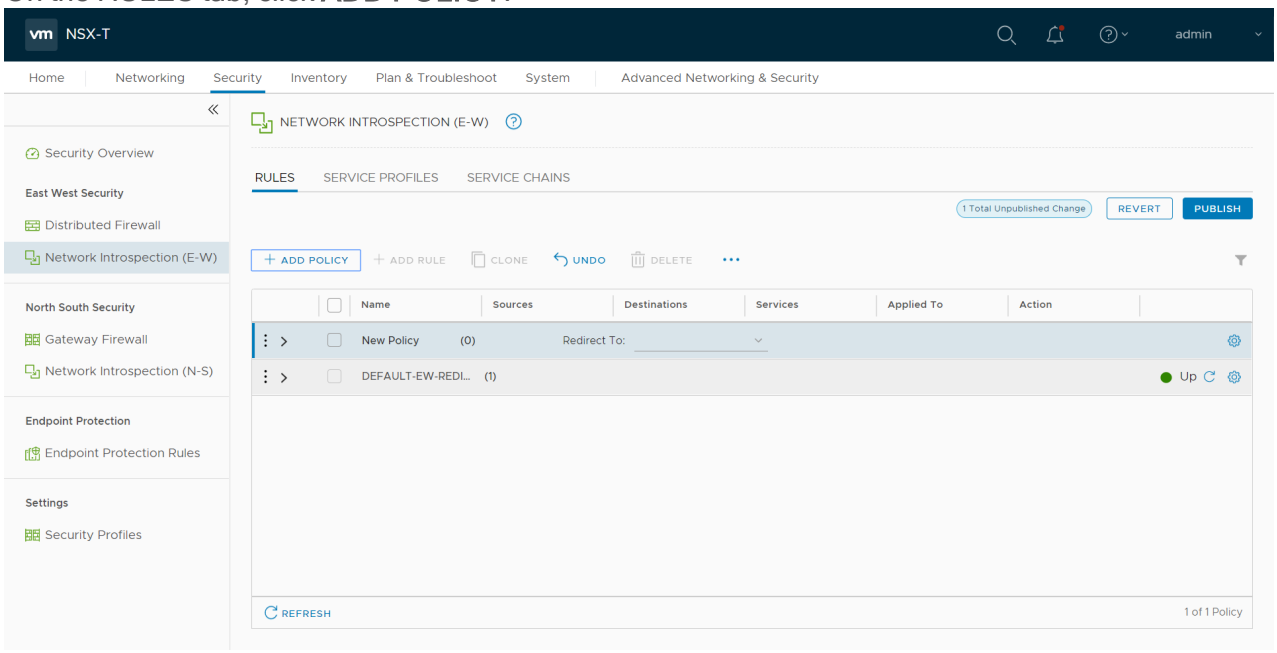
3. On the New Group, enter or select the values as follows.
   a. Enter a name for the new group.
   b. Click **Set Members** and the **Select Members** dialog box appears.
      - Add or select Membership Criteria, Members, IP/MAC Addresses, and AD Groups.
   c. Enter the description for the group.
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 > Network Introspection (E-W)** and then click **RULES** tab.
2. On the RULES tab, 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.

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:

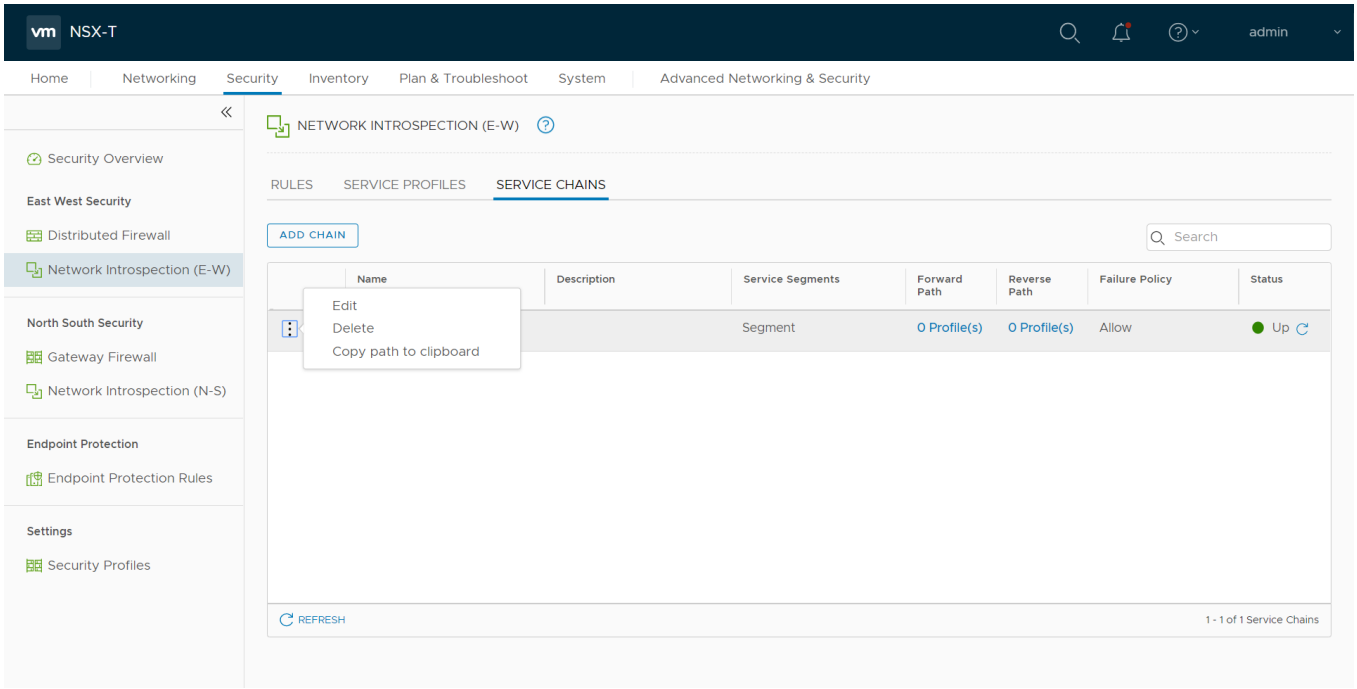
- Step 1: Remove the Service Chains
- Step 2: Delete the Monitoring Session
- Step 3: Undeploy GigaVUE Cloud Suite - V Series VMs
- Step 4: Delete the NSX-T Manager and vCenter Connections

Step 1: Remove the Service Chains

To delete the network monitoring services:

1. In NSX-T, select **Security > Network Introspection (E-W)**.

2. Select the **SERVICE CHAINS** tab.
3. 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.

GigaVUE V Series Deployment Clean up

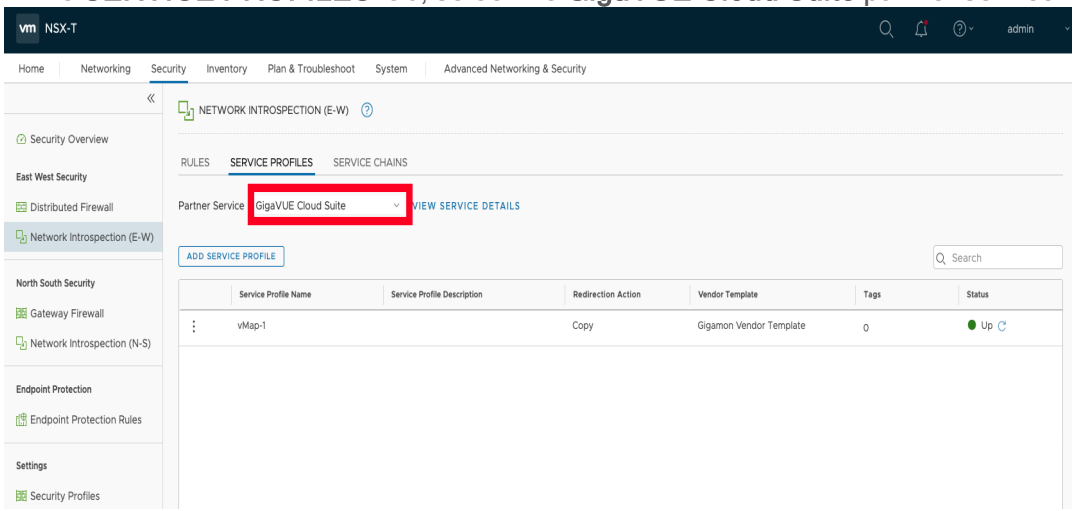
On installation failure or incomplete service removal, you must clean up V Series nodes before reattempting the installation. To clean up the V Series deployments from NSX-T and GigaVUE-FM, perform the following steps:

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

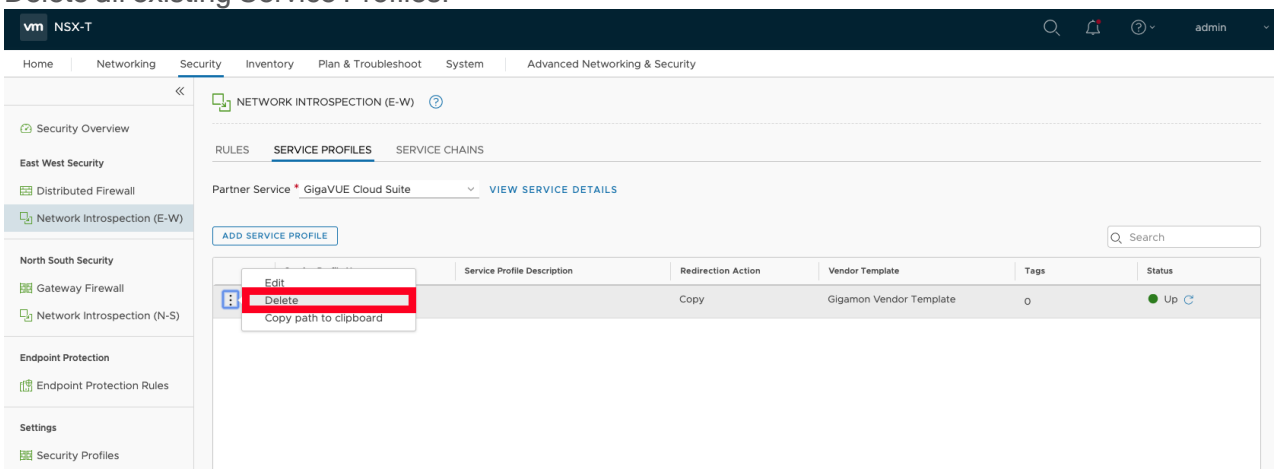
Remove Service Profiles

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.



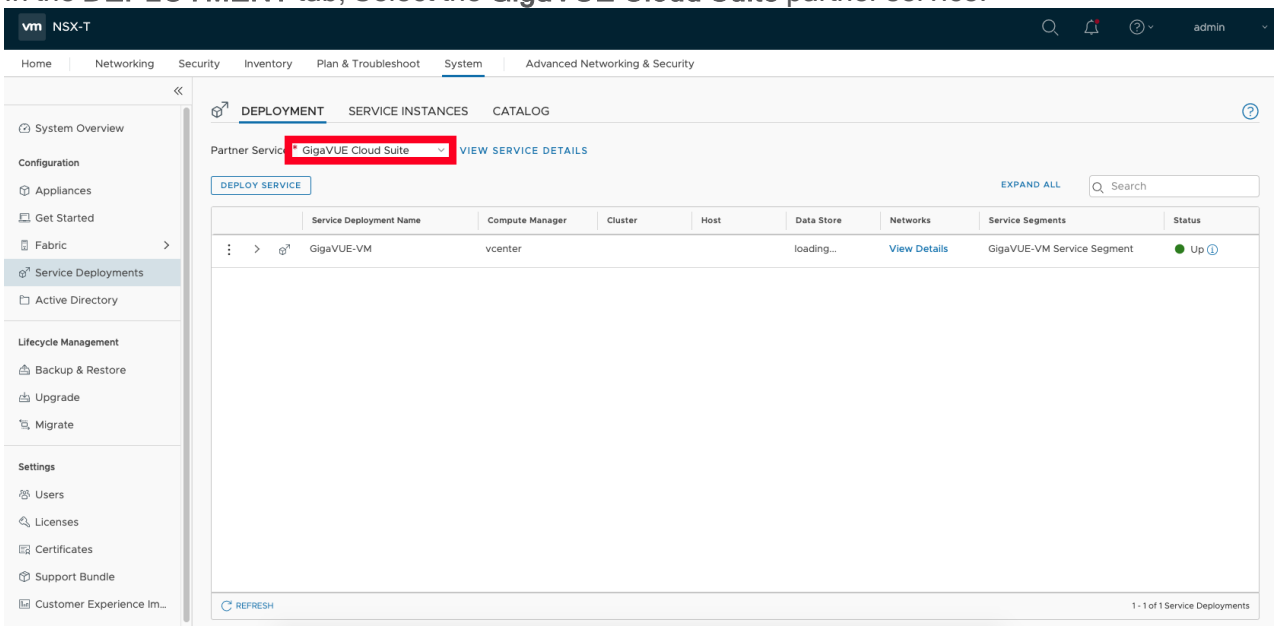
3. Delete all existing Service Profiles.



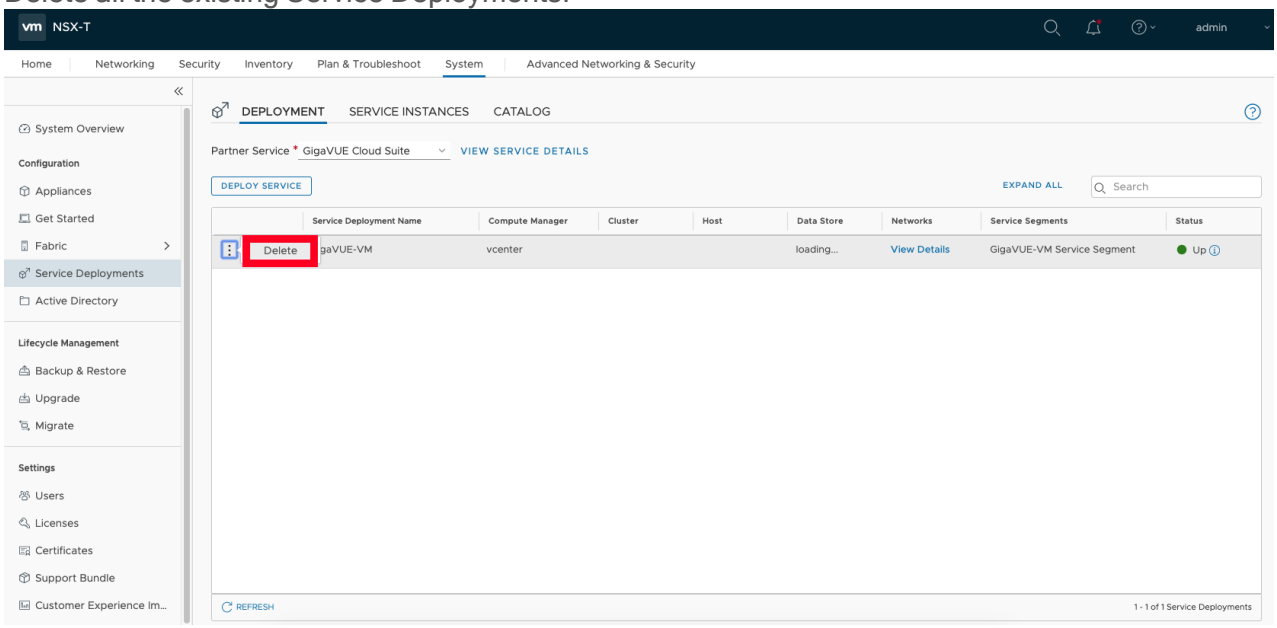
Remove Service Deployments

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.

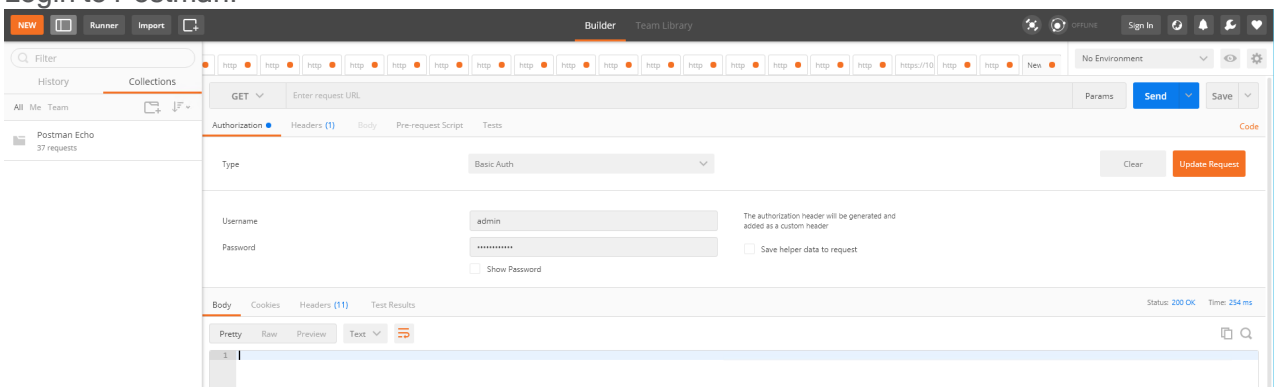


3. Delete all the existing Service Deployments.



To remove the Service Deployments through NSX-T API:

1. Login to Postman.

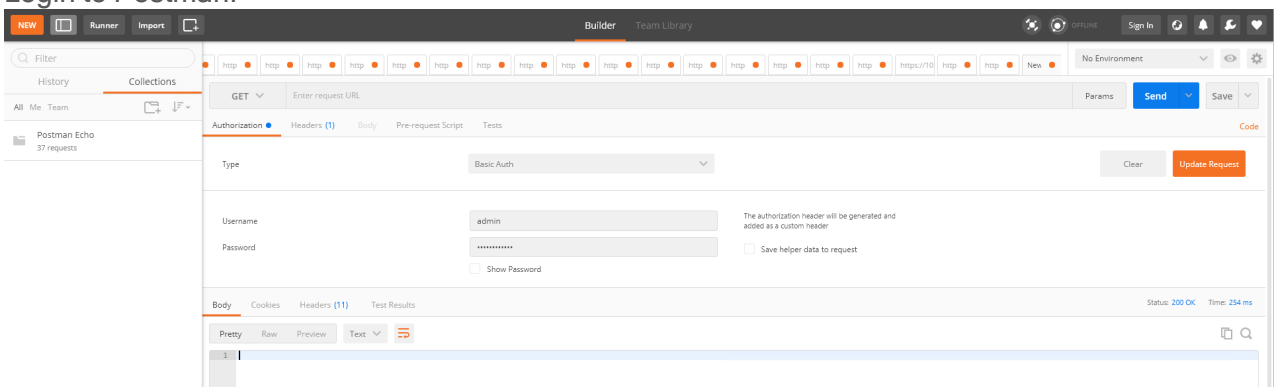


2. Get the Service ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/
3. Get the ID of the Service Deployments.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/
4. Delete all Service Deployments.**DELETE** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/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

Remove Service Reference

To remove Service References through NSX-T API:

1. Login to Postman.

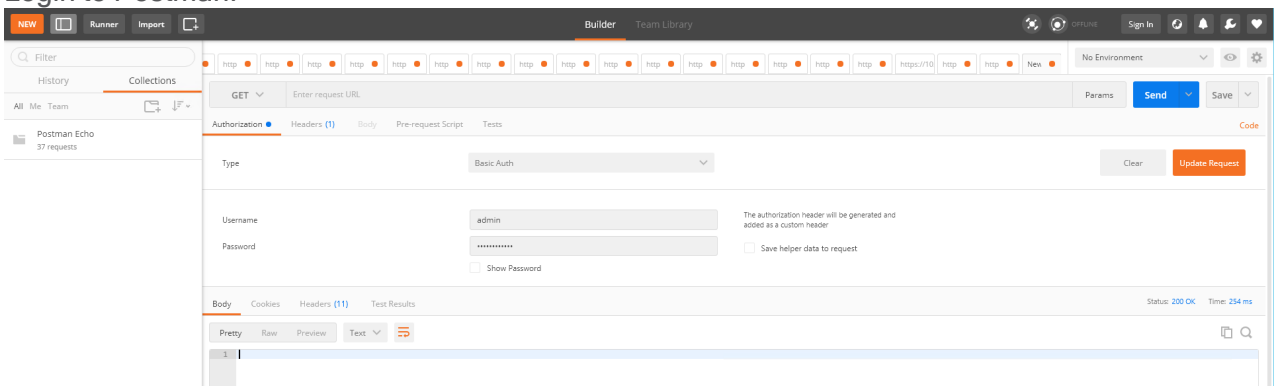


2. Get the Service Reference ID.**GET** https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/
3. Delete the Service Reference.**DELETE** https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/<Service_Reference_ID>

Remove Service Manager

To remove Service Manager through NSX-T API:

1. Login to Postman.

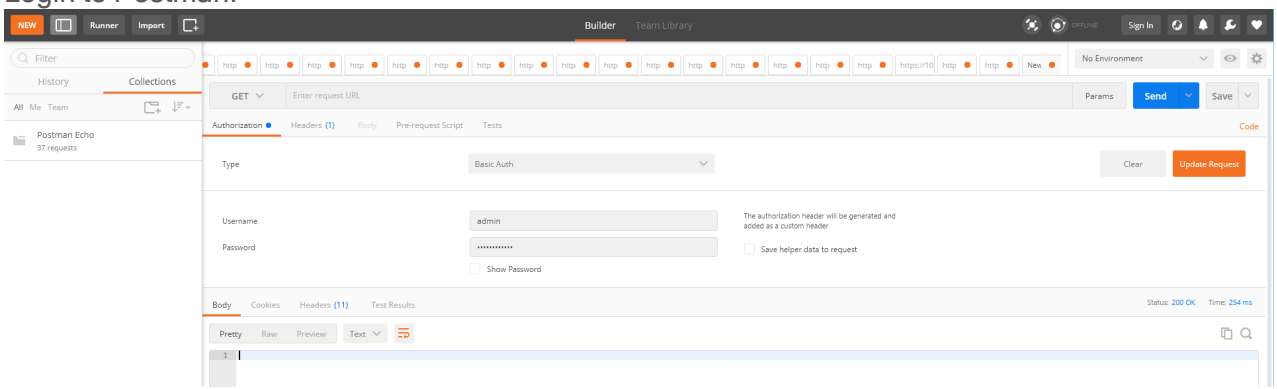


2. Get the Service Manager ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/service-managers/
3. Delete the Service Manager.**DELETE** https://<NSX_Manager_IP>/api/v1/serviceinsertion/serivce-managers/<Service_Manager_ID>

Remove Vendor Template and Service Definition

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

1. Login to Postman.



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 5.14 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, 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 2Installation Guide
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide

GigaVUE Cloud Suite 5.14 Hardware and Software Guides
Administration
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
Fabric Management
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 Configuration and Monitoring how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE Cloud Suite for AnyCloud Guide how to deploy the GigaVUE Cloud Suite solution in any cloud platform
GigaVUE Cloud Suite for AWS Guide
GigaVUE Cloud Suite for AWS Quick Start Guide quick view of AWS deployment
GigaVUE Cloud Suite for AWS SecretRegions Guide
GigaVUE Cloud Suite for Azure Guide
GigaVUE Cloud Suite for Kubernetes Guide
GigaVUE Cloud Suite for Nutanix Guide
GigaVUE Cloud Suite for OpenStack Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
Reference
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H 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)

GigaVUE Cloud Suite 5.14 Hardware and Software Guides
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.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	
For Online Topics	Online doc link	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	Document Title	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	Describe the issue	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings** > **Support** > **Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The 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)