



# GigaVUE Cloud Suite for VMware-GigaVUE- VM 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](http://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

<b>GigaVUE Cloud Suite for VMware-GigaVUE-VM Guide</b> .....	<b>1</b>
Change Notes .....	3
Contents .....	4
<b>GigaVUE Cloud Suite for VMware-GigaVUE-VM</b> .....	<b>7</b>
<b>GigaVUE-VM Overview</b> .....	<b>8</b>
Communication with GigaVUE-FM .....	8
GigaVUE-VM Features and Benefits .....	9
GigaVUE-VM Rules and Notes .....	10
GigaVUE-VM Licenses .....	10
GigaVUE-VM License Types .....	10
GigaVUE-VM License Packages .....	12
Obtain New License .....	14
Retrieve Lost License .....	14
Virtual Dashboard .....	14
Virtual Dashboard Profiles .....	14
Virtual Dashboard Widgets .....	15
<b>Configure GigaVUE-VM on ESXi</b> .....	<b>18</b>
Before You Install .....	18
VMware ESXi System Requirements .....	19
Privileges Required for VMware Virtual Center .....	19
How to Use GigaVUE-VM vCenter Management .....	20
Set up Connection between GigaVUE-FM and Virtual Center .....	21
Deploy GigaVUE-VM Nodes .....	22
Configure Port Groups/Port-Profiles .....	23
Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster .....	24
Configure Tunnel Endpoint .....	30
Tunnel Configuration Options .....	30
Create Tunnel Endpoint .....	32
Tunnel Validation .....	33
Configure H Series IP Interfaces for the GigaVUE-VM Tunnel Library .....	34
TCP Tunnel between GigaVUE-VM and GigaVUE Cloud Suite HC Series Nodes .....	36
Configure Virtual Maps for VMware vCenter .....	42
Configure vMap for VMware .....	44
vMaps and vMotion Migration .....	46

GigaVUE-VM: Monitor Intra-Host and Inter-Host Traffic .....	47
Changes in vDS Port ID Require vMap Redeployment .....	48
Bulk Upgrade GigaVUE-VM Nodes .....	48
Backup and Restore GigaVUE-FM for VMware .....	49
Events .....	49
Alarms .....	50
Audit Logs .....	50
<b>Configure GigaVUE-VM on NSX-V .....</b>	<b>52</b>
Prerequisites for Integrating GigaVUE-VM with NSX-V .....	52
Integrate GigaVUE-VM with NSX-V .....	53
Step 1: Create Users in VMware vCenter and GigaVUE-FM .....	53
Step 2: Register NSX-V vCenter in GigaVUE-FM .....	55
Step 3: Upload the GVM OVA Image .....	56
Step 4: Register NSX-V Manager in GigaVUE-FM .....	57
Step 5: Install Gigamon Traffic Visibility Service on vCenter Clusters ..	57
Step 6: Configure GigaVUE-FM Tunnels and Virtual Maps .....	58
Step 7: Create NSX-V Security Group and Security Policy .....	60
Upgrade GigaVUE-VM on NSX-V .....	62
Upload OVA file .....	62
Upgrade Gigamon Traffic Visibility in the VMware vCenter .....	63
View Upgraded GigaVUE-VM Nodes .....	64
Remove Gigamon Service from NSX-V and GigaVUE-FM .....	65
Step 1: Delete Network Monitoring Services .....	65
Step 2: Delete NSX-V Virtual Maps from GigaVUE-FM .....	66
Step 3: Delete Traffic Visibility Service from NSX-V .....	66
Step 4: Delete NSX-V Manager from GigaVUE-FM .....	66
Step 5: Delete Virtual Center from GigaVUE-FM .....	66
<b>Configure GigaVUE-VM on NSX-T .....</b>	<b>67</b>
Prerequisites for Integrating GigaVUE-VM with NSX-T .....	67
Integrate GigaVUE-VM with NSX-T .....	67
Step 1: Create Users in VMware vCenter and GigaVUE-FM .....	68
Step 2: Register NSX-T vCenter and NSX-T Manager in GigaVUE-FM69	
Step 3: Deploy GigaVUE-VM on vCenter Clusters .....	72
Step 4: Configure GigaVUE-FM Tunnels and Virtual Maps .....	74
Step 5: Create NSX-T Group and Service Chain .....	76
Remove Gigamon Service from NSX-T and GigaVUE-FM .....	78
Step 1: Remove the Service Chains .....	78
Step 2: Delete the vMaps .....	79
Step 3: Undeploy GigaVUE Cloud Suite-VMs .....	79
Step 4: Delete the NSX-T manager and vCenter connections .....	79
GigaVUE-VM Deployment Clean up .....	80
Remove Service Profiles .....	80

Remove Service Deployments .....	81
Remove Service Reference .....	82
Remove Service Manager .....	83
Remove Vendor Template and Service Definition .....	83
<b>GigaVUE-VM Reference .....</b>	<b>85</b>
Best Practices for vSphere Integration .....	85
Tips for vMaps .....	86
<b>Additional Sources of Information .....</b>	<b>87</b>
Documentation .....	87
How to Download Software and Release Notes from My Gigamon .....	89
Documentation Feedback .....	90
Contact Technical Support .....	91
Contact Sales .....	91
Premium Support .....	91
The Gigamon Community .....	91
<b>Glossary .....</b>	<b>93</b>

# GigaVUE Cloud Suite for VMware-GigaVUE-VM

GigaVUE Cloud Suite for GigaVUE-VM 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 Cloud Suite® Virtual Machine (GigaVUE-VM).

Topics:

- [GigaVUE-VM Overview](#)
- [Configure GigaVUE-VM on ESXi](#)
- [Configure GigaVUE-VM on NSX-V](#)
- [Configure GigaVUE-VM on NSX-T](#)

# GigaVUE-VM Overview

The GigaVUE-VM Virtual Traffic Visibility node extends GigaVUE Cloud Suite traffic distribution principles to the virtualized environments, allowing users to filter, monitor, and forward traffic on virtual machines to GigaVUE Cloud Suite nodes for distribution to monitoring and analysis tools. GigaVUE-VM nodes support vSphere Distributed Switch, vSphere Standard Switch, and the NSX vSwitch for maximum flexibility. Bundles of GigaVUE-VM nodes may be licensed separately within the GigaVUE-FM interface.

GigaVUE-FM is required for the deployment, configuration, and management of GigaVUE-VM nodes. You work with GigaVUE-VM nodes (through either IP address or DNS name) using the web-based GigaVUE-FM interface. Once you have provided GigaVUE-FM with the IP address and credentials of a VMware vCenter Server, GigaVUE-FM retrieves information on the existing virtual machines managed by the vCenters. Based on this information, GigaVUE-FM helps you manage the GigaVUE-VM nodes deployed throughout your virtual network.

**NOTE:** GigaVUE-FM is recommended for GigaVUE-VM deployment to avoid solution instability.

After you have deployed GigaVUE-VM nodes and GigaVUE-FM has discovered the virtual machines that exist in your virtual network, use GigaVUE-FM to configure **vMaps**. Similar to maps in the GigaVUE Cloud Suite H Series, vMaps let you configure packet-matching criteria that distribute matching packets to designated destinations. Virtual packets find their way to physical tool ports through a GigaSMART tunnel to a network port on a GigaSMART-enabled GigaVUE Cloud Suite H Series or G Series node. Once the traffic is de-tunneled at the receiving end of the tunnel, it is available for standard GigaVUE Cloud Suite traffic distribution to local and stacked tool ports.

Topics:

- [Communication with GigaVUE-FM](#)
- [GigaVUE-VM Features and Benefits](#)
- [GigaVUE-VM Rules and Notes](#)
- [GigaVUE-VM Licenses](#)

## Communication with GigaVUE-FM

After GigaVUE-VM is deployed using GigaVUE-FM, you must use the GigaVUE-FM Web interface to configure and manage virtual nodes and vMaps.

Due to the dynamic nature of the virtual environment, GigaVUE-FM must stay in constant communication with the vCenter server at all times. This allows GigaVUE-FM to be aware of vMotion events and manage an active inventory of all the virtual nodes in the vCenter. You should ensure that there is a GigaVUE-VM



present on each ESXi or NSX host in your virtual datacenter. In this way, you provide GigaVUE-FM with constant access to all virtualized traffic as your VMs move across physical hosts. GigaVUE-FM can support up to 10 vCenters and 1000 virtual nodes (total).

The entire standard GigaVUE-OS CLI interface is not supported by GigaVUE-VM. This is to ensure that all traffic management and configuration is managed through GigaVUE-FM.

**NOTE:** A GigaVUE-FM instance connected to one vCenter does not allow GigaVUE-VM to be configured on both the ESXi and NSX hosts.

## GigaVUE-VM Features and Benefits

GigaVUE-VM Visibility Fabric™ node 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 GigaVUE Cloud Suite® platforms, thereby eliminating any traffic blind spots.

The following table summarizes the major features and benefits of GigaVUE-VM:

Benefit	Descriptions
Visibility into VM Traffic	Intelligent selection, filtering, and forwarding of VM traffic to the monitoring and tool infrastructure; extend the reach and leverage of existing tools to monitor virtual network infrastructure; on-board virtual traffic visibility for n-tier application cluster.
Multi-Hypervisor Support	Supports the most popular private cloud hypervisors and VMware ESXi.
Support for Packet Slicing	Conserve production network backhaul and optimize monitoring infrastructure processing by slicing VM traffic at required offset, before forwarding it for analysis
Integration with Unified Visibility Fabric and GigaSECURE® Security Delivery Platform	Seamless end-to-end visibility across physical and virtual network infrastructure. Optimize monitoring infrastructure by enabling aggregation, replication, and sharing of traffic streams across multiple monitoring tools and IT teams. Additional Flow Mapping® and GigaSMART® intelligence can be applied on the virtual traffic before forwarding the tools.
Tunneling Support	Leverage the production network to tunnel and forward the filtered virtual traffic from the hypervisor to the GigaVUE Cloud Suite platforms; tenant-based IP Tunneling facilitates isolation, privacy, and compliance of monitoring traffic. Simplified virtual traffic policy creation to identify and select the physical tunnel termination end-point where the filtered and transformed virtual workload traffic is to be delivered.
Support for vMotion and LiveMigration	Ensure the integrity of visibility and monitoring policies in a dynamic infrastructure, have real-time adjustment of monitoring and security posture to virtual network changes, and the ability to respond to disasters/failures without losing NOC insight and control.
Virtual Switch Agnostic Solution	VMware: vNetwork Standard Switch (vSS), vNetwork Distributed Switch (vDS), and NSX-V.
Centralized Management	Manage and monitor the physical and virtual fabric nodes using GigaVUE-FM while also configuring the traffic policies to access, select, transform and deliver the traffic to the tools.

Benefit	Descriptions
Hotspot monitoring	Pro-actively monitor and troubleshoot GigaVUE-VM nodes by elevating Top-N and Bottom-N virtual traffic policies to the centralized dashboards.

## GigaVUE-VM Rules and Notes

The GVM solution has the following potential vulnerabilities:

- EOL/Obsolete Software: Apache HTTP Server 2.2.x Detected
- Apache httpd Server ap\_get\_basic\_auth\_pw() Authentication Bypass Vulnerability
- File Permissions (passwd, shadow and group) Are Not Properly Set
- OpenSSH AES-GCM Cipher Remote Code Execution Vulnerability.
- Linux Kernel Double Fetch Denial of Service Vulnerability

## GigaVUE-VM Licenses

GigaVUE-FM is provisioned by default with a Base License that allows you to add one physical node and one virtual node. To manage additional physical or virtual nodes, you must obtain and apply licenses, as described in this section.

To run only a single GigaVUE-VM node, there is no requirement to purchase additional licenses for GigaVUE-FM.

**NOTE:** To apply licenses and to know about the best practices when upgrading or downgrading license packages, refer to the “*Licenses*” chapter in the *GigaVUE Administration Guide*.

Topics:

- [GigaVUE-VM License Types](#)
- [GigaVUE-VM License Packages](#)
- [Retrieve Lost License](#)
- [Obtain New License](#)

## GigaVUE-VM License Types

GigaVUE-VM is available in multiple tiered options along with optional Add-On Features which are also available as a special license (add-on are included with the Prime Package as free-of-charge). GigaVUE-VM is available with base option and with base feature of 1 free physical node and 1 free virtual node and

10 virtual tap points for OpenStack, AWS and Azure. No licenses are required to activate this option.

Additional GigaVUE-VM licenses are available for purchase. The following tables summarizes the available packages and support features with each package.

**NOTE:** Similar to public cloud, NSX-T licensing is enforced on all the tap points (VMs).

Table 1: GigaVUE-VM Evaluation License Packages

License Types	Physical Nodes	Virtual Nodes	OpenStack/AWS/Azure/NSX-T	Features available	Notes
GigaVUE-VM Evaluation	1 (included as Base)	1	10 Virtual TAP Points	All features for the evaluation period.	License automatically expires after 45 days.

**NOTE:** Evaluation licenses are not recommended for deployment in production environment. At the end of the evaluation period, if the license is not upgraded to a fully licensed version, the features are disabled automatically. For an evaluation license, contact your Gigamon representative.

## GigaVUE-VM License Packages

The following table summarizes the GigaVUE-VM license packages.

Features	Base (Free-of-Charge)	10-Pack	50-Pack	100-Pack	250-Pack	1000-Pack
Virtual Node Count	1	Up to 10	Up to 50	Up to 100	Up to 250	Up to 1000
Audit, Events Logs	Yes	Yes	Yes	Yes	Yes	Yes
VM Dashboard	Yes	Yes	Yes	Yes	Yes	Yes
Reports	No	Yes	Yes	Yes	Yes	Yes
Trending Data	1 Day	1 Month	1 Month	1 Month	1 Month	1 Month

**NOTE:** To run only GigaVUE-VM, there is no requirement to purchase GigaVUE-FM package. However, you will be limited to 1 day of trending data for the dashboard and reports.

GigaVUE Cloud Suite virtual tap points (G-vTAP) are available in multiple tiered options for virtual monitoring. A virtual tap point is any end point that can be tapped. For example, a vNic in a VM. All GigaVUE-FM are available with the base option of 1 free G-vTAP. No license is required to activate this option.

Additional G-vTAPs are available for purchase. The following table summarizes the available G-vTAP license packages and supported features with each package.

Features	FM-Base (Free-of-Charge)	100-Pack	250-Pack	1000-Pack
Audit, Events Logs	Yes	Yes	Yes	Yes
Virtual Tap Points	1	Up to 100	Up to 250	Up to 1000
Trending Data	1 Day	1 Month	1 Month	1 Month

You must purchase an additional license to access the Gigamon Visibility Platform for AWS, which is provisioned with a monthly term license. There are two types of licenses you can purchase in AWS. The following table summarizes the available AWS/Azure/OpenStack license packages. For details about installing and configuring GigaVUE Cloud Suite for AWS, refer to the GigaVUE Cloud Suite for AWS Guide.

License Type	Description
100 Virtual TAP Points	Monthly Term license for traffic visibility up to 100 virtual TAP Points in AWS. Minimum Term is 3 months with a maximum of 12 months.
1000 Virtual TAP Points	Monthly Term license for traffic visibility up to 1000 virtual TAP Points in AWS. Minimum Term is 3 months with a maximum of 12 months.

## Obtain New License

Contact your Sales representative to obtain a new license for GigaVUE-FM or additional GigaVUE-VM Nodes (see [Contact Sales](#) or [Contact Technical Support](#) for assistance).

## Retrieve Lost License

If you lost an existing license, contact [Gigamon Technical Support](#) for assistance. You can also email Technical Support at [support@gigamon.com](mailto:support@gigamon.com).

## Virtual Dashboard

The Virtual Dashboard is similar to the Physical Dashboard and presents four widgets that provide information about GigaVUE-VM. It is only available if a GigaVUE-VM package or packages are purchased. There are no minimum requirements for the size of the pack purchased. However, the dashboard is not available in Basic mode where only one VM node is available.

From the Virtual Dashboard, you can do the following:

- Create multiple profiles using widgets
- Resize or reposition the windows
- Set the default profile as the landing page for the login
- Modify the trending for each widget

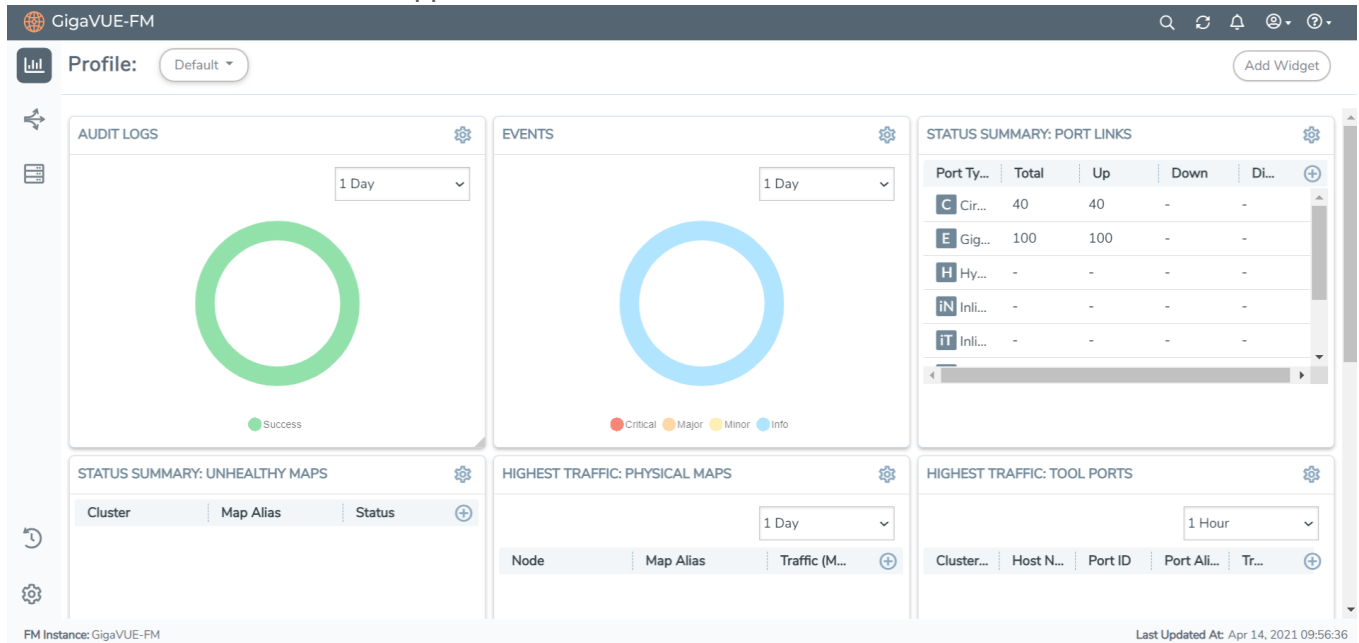
Topics:

- [Virtual Dashboard Profiles](#)
- [Virtual Dashboard Widgets](#)

## Virtual Dashboard Profiles

The Virtual Dashboard allows you to create multiple profiles. There are four widgets in the Virtual dashboard. You can create multiple profiles and customize the widgets to be displayed in each profile.

To create a new profile, refer to the "Physical Dashboard Profiles" in the *GigaVUE Fabric Management Guide*. The Virtual Dashboard appears as shown below.



**NOTE:** The time interval selected, depends on the GigaVUE-VM package selected. For the base package, only 1 day option is available as the data is not stored for more than 1 day. While the prime package users can select any option including 1 month.

## Virtual Dashboard Widgets

The widgets available on the Virtual Dashboard are:

- Highest Traffic widgets
- Lowest Traffic widgets

You can customize the widgets by creating and managing profiles. Refer to [Virtual Dashboard Profiles](#) for more information.

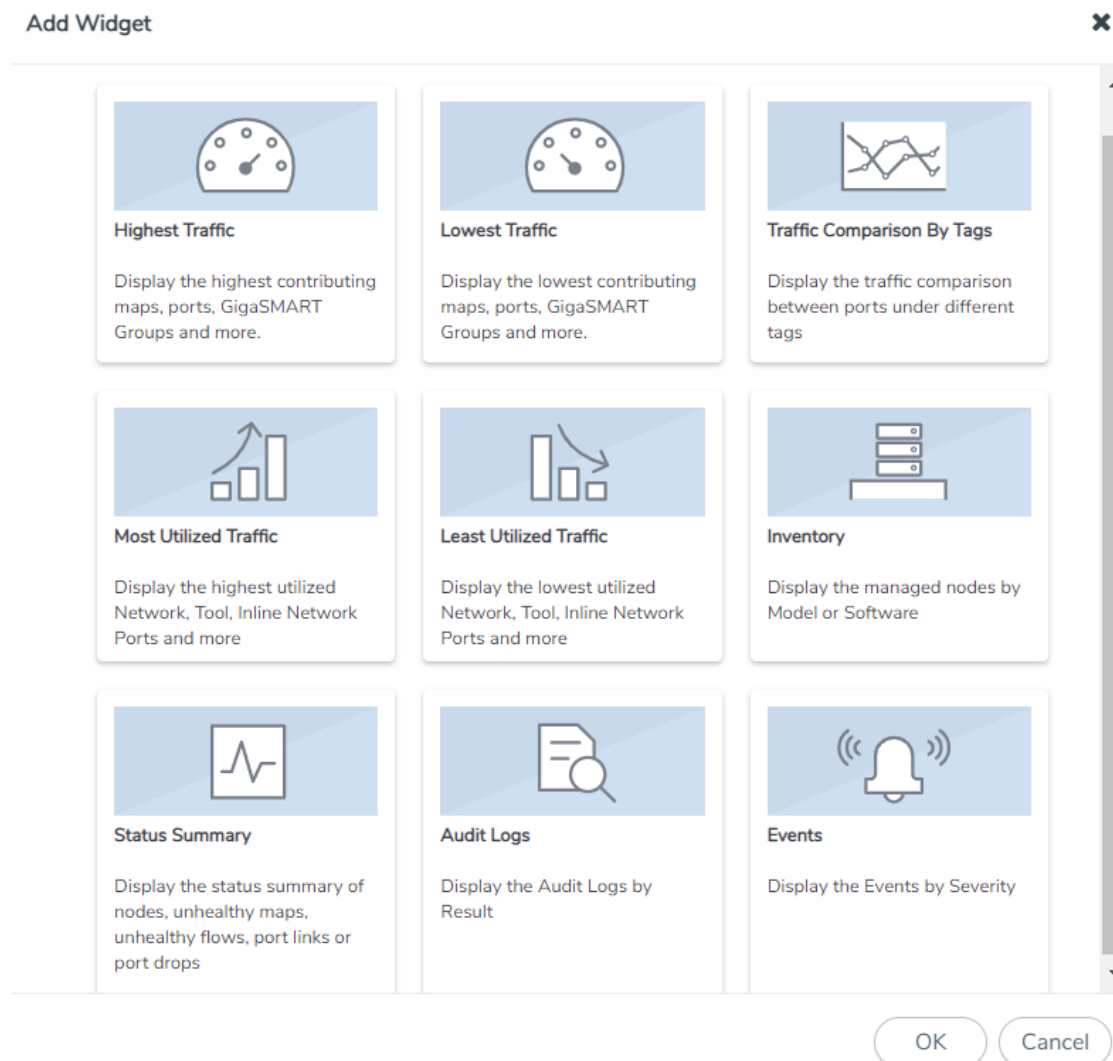
### Highest Traffic

The Highest Traffic widget lists the GigaVUE Cloud Suite-VMs with the highest traffic within a specified time. You can create as many Highest Traffic widgets as you want and list up to 5, 10, 15, 20, 50, or 100 items in each widget.

The traffic flowing through each GigaVUE-VM is displayed in megabytes per second (Mbps). You can specify the period over which the amount of traffic must be calculated. You can choose 1 hour, 1 day, 1 week, or 1 month.

To configure the Highest Traffic widget:

1. On the top navigation bar, click **Dashboard**.
2. On the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
3. Click **Add Widget**. The Add New Widget window is displayed.



4. In the Add Widget window, select **Highest Traffic** and click **OK**. The Highest Traffic configuration window is displayed.



**HIGHEST TRAFFIC**

**Traffic Type**  
Choose which type of traffic to show on this widget

Virtual

**Item Type**  
Which items do you want to show

GigaVUE VM Ports

**Tags**

TagKey Values + -

**Display Total**  
How many items do you want to display on this widget

5

OK Cancel

5. From the **Traffic Type** drop-down list, select Virtual.
6. From the **Item Type** drop-down list, select one of the following items:
  - o GigaVUE-VM Ports - displays the ports contributing to the highest traffic
  - o GigaVUE-VM Maps - displays the maps contributing to the highest traffic

**NOTE:** Sites are not applicable for GigaVUE Cloud Suite-VMs.

7. From the **Display Total** drop-down list, select the number of items to be displayed. By default, the number of items selected for display is 5.
8. Click **OK**.

## Lowest Traffic

The Lowest Traffic widget lists the GigaVUE Cloud Suite-VMs that contribute to the lowest traffic within a specified time. You can create as many Lowest Traffic widgets as you want listing up to 5, 10, 15, 20, 50, or 100 items in each widget.

The traffic flowing through GigaVUE Cloud Suite-VMs is measured in megabytes per second (Mbps). You can specify the period over which the amount of traffic is calculated. You can choose 1 hour, 1 day, 1 week, or 1 month.

The Lowest Traffic widget is configured the same way as the Highest Traffic widget. To configure the Lowest Traffic widget, refer to the configuration steps provided in [Highest Traffic](#).

# Configure GigaVUE-VM on ESXi

This chapter introduces GigaVUE-VM virtual traffic visibility node, describing the features and functions and summarizing the relationships between the products.

The chapter includes the following major sections:

- [Before You Install](#) describes the system requirements, such as the security privileges needed for the vCenter GigaVUE-VM users.
- [How to Use GigaVUE-VM vCenter Management](#) describes the tasks you must perform the first time you use GigaVUE-VM.
- [Deploy GigaVUE-VM Nodes](#) provides the procedure to deploy GigaVUE-VM nodes from GigaVUE-FM.
- [Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster](#) provides the procedure to deploy a single or multiple GigaVUE-VM nodes from GigaVUE-FM. The GigaVUE-VM nodes can be deployed on a data center or on a cluster within the data center.
- [Bulk Upgrade GigaVUE-VM Nodes](#) provides the procedure to upgrade a single or multiple GigaVUE-VM nodes from GigaVUE-FM.
- [Configure Virtual Maps for VMware vCenter](#) describes how to configure virtual maps when deploying GigaVUE-VM nodes.
- [Backup and Restore GigaVUE-FM for VMware](#) provides the steps for backing up and restoring GigaVUE-FM in a VMware environment.
- [Best Practices for vSphere Integration](#) provides tips on optimizing GigaVUE-FM and GigaVUE-VM settings for best performance.

## Before You Install

Before installing a GigaVUE-VM node, ensure the following each ESXi host that will be managed:

1. Install VMware vSphere ESXi Standard Version 5.x or greater for NSX-V, and Version 6.5 or greater for NSX-T on hardware that meets minimum requirements.

**NOTE:** VMware vSphere Enterprise Plus is required for vSphere Distributed Switch (vDS) deployments.

2. Install Virtual Switch. You can use either vSphere Distributed Switch (vDS) or vSphere Standard Switch (vSS) available with vSphere.
  - vSphere Distributed Switch. For versions, refer to [VMware ESXi System Requirements](#).

**NOTE:** The installation wizard does not prevent you from installing GigaVUE-VM on an ESXi host without a virtual switch installed. However, the virtual switch is required for GigaVUE-VM to access traffic.

3. Set the MTU larger than the largest packet expect from the virtual environment or enable fragmentation.

To transport packets of interest from the virtual environment to physical devices, GigaVUE-VM uses a tunneled network connection to a GigaSMART card on a physical appliance. (For information about the tunnel network, refer to [Configure Tunnel Endpoint](#).) Either the MTU of this tunnel **must be** larger than the size of the largest packet of interest that you expect to forward from the virtual environment to a physical appliance, or you **must** enable fragmentation. (For more information about fragmentation, refer to [Fragmentation](#).)

If your existing virtual networks use an MTU of 1500 bytes, and if you choose to increase the MTU for the entire network path of the tunnel, you must increase the tunnel MTU to 1600 bytes. This increase must take place on all of the network components from the virtual switch to the GigaSMART card. For NSX-T the MTU is required to be 1600 bytes or greater.

Failure to either increase the tunnel path MTU or use fragmentation will result in packets of interest being dropped by your network infrastructure before they can reach the GigaSMART card. Neither GigaVUE-FM nor GigaVUE-VM will indicate that these packets are being dropped.

## VMware ESXi System Requirements

Refer to the GigaVUE-VM Release Notes for the hardware requirements on which VMware ESXi runs GigaVUE-VM.

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

**NOTE:** TCP port 443 must be open from the GigaVUE-FM instance to host in the vCenter and upload the OVA image files.

## Privileges Required for VMware Virtual Center

Some minimum privileges are required for the GigaVUE-FM user in the Virtual Center. You can assign privileges to Virtual Center users by selecting **Administration > Access Control > Roles**, and then use the **Edit Role** dialog box in vCenter. Roles should be applied at the vSphere Virtual Center level and not the DataCenter or Host levels.

The following table lists the minimum required permissions for GigaVUE-FM to manage the virtual center.

Category	Required Privilege	Purpose
Host	Configuration <ul style="list-style-type: none"> <li>■ Network Configuration</li> </ul>	VSS Map
	Inventory	Pin GigaVUE-VM to the host in cluster configurations.

Category	Required Privilege	Purpose
	<ul style="list-style-type: none"> <li>Modify Cluster</li> </ul>	This prevents automatic migration.
<b>Datastore</b>	<ul style="list-style-type: none"> <li>Allocate space</li> </ul>	GigaVUE-VM Deployment
<b>Distributed Switch</b>	<ul style="list-style-type: none"> <li>VSPAN Operation</li> </ul>	VDS Map
<b>Network</b>	<ul style="list-style-type: none"> <li>Assign network</li> </ul>	GigaVUE-VM Deployment/VSS Map
<b>Resource</b>	<ul style="list-style-type: none"> <li>Assign virtual machine to resource pool</li> </ul>	GigaVUE-VM Deployment
<b>vApp</b>	<ul style="list-style-type: none"> <li>Import</li> <li>vApp instance configuration</li> </ul>	GigaVUE-VM Deployment
<b>Virtual machine</b>	<b>Configuration</b> <ul style="list-style-type: none"> <li>Add new disk</li> <li>Modify device settings</li> </ul>	GigaVUE-VM Deployment GigaVUE-VM Deployment/VSS Map
	<b>Interaction</b> <ul style="list-style-type: none"> <li>Device connection</li> <li>Power on</li> <li>Power Off</li> </ul>	GigaVUE-VM Deployment GigaVUE-VM Deployment GigaVUE-VM Deployment
	<b>Inventory</b> <ul style="list-style-type: none"> <li>Create from existing</li> <li>Remove</li> </ul>	GigaVUE-VM Deployment GigaVUE-VM Deployment
	<b>Provisioning</b> <ul style="list-style-type: none"> <li>Clone virtual machine</li> </ul>	GigaVUE-VM Deployment

## How to Use GigaVUE-VM vCenter Management

The first time you use the GigaVUE-VM vCenter Management there are a number of tasks that you need to do. The following table outlines those tasks:

Step	Task	Navigation	Notes
1	Connect to Virtual Center	From the left navigation pane, select <b>Inventory &gt; VIRTUAL &gt; VMware &gt; vCenter &gt; Management &gt; Virtual Centers</b>	GigaVUE-FM must first gain access to virtual center server database to see which physical nodes are present. Add virtual center login credential to connect to virtual center from GigaVUE-FM. Type in the DNS name or IP address for the vCenter that manages the host hypervisor.  GigaVUE-FM can only read and not write into the vCenter server.

Step	Task	Navigation	Notes
			Refer to <a href="#">Set up Connection between GigaVUE-FM and Virtual Center</a> .
2	Deploy GigaVUE-VM to multiple ESXi hosts	Under VMware vCenter, go to <b>Management &gt; Virtual Nodes &gt; Deploy Virtual Nodes</b>	To gain access to the virtual traffic, GigaVUE-VM needs to be deployed to the host where the monitoring needs to occur.  Only one ova file can exist on the GigaVUE-FM. Any new uploads over-write the existing file.  For deployment information refer to <a href="#">Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster</a> .
3	Configure a tunnel definition.	Under VMware vCenter, go to <b>Management &gt; Tunnel Library</b>	To add the already configured tunnel endpoint on GigaSMART to the GigaVUE-FM for use in virtual maps.  Refer to <a href="#">Configure Tunnel Endpoint</a> .
4	Verify deployed GigaVUE Cloud Suite-VMs and status	Under VMware vCenter, go to <b>Virtual Nodes</b>	To verify the GigaVUE-VM deployment status, check the status on the Virtual Nodes page.
5	Configure Virtual Maps/Rules	From the left navigation pane, select <b>Traffic &gt; VIRTUAL &gt; Virtual Maps &gt; VMware vCenter</b>	Virtual rules are created to access the traffic within the hypervisor. Rules consist of filter rules that match specific parameters. These rules specify what traffic is forwarded through the GigaSMART Tunnel to the Gigamon Visibility Fabric.  Refer to <a href="#">Configure Virtual Maps for VMware vCenter</a> .

## Set up Connection between GigaVUE-FM and Virtual Center

To set up the connection between GigaVUE-FM and the Virtual Center:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The Management page appears.

**NOTE:** GigaVUE-FM supports up to 10 Virtual Center connections.

- In the **Virtual Centers** page, click **Add**. The Add Virtual Center page appears.

## Add Virtual Center

Save

Cancel

Virtual Center	IP address/DNS
Username	username
Password	password

- Enter the IP address or DNS name for the Virtual Center.
- In the Username field, enter a username.
- In the Password field, enter a password.
- Click **Save**.

GigaVUE-FM uses the IP, username, and password to log in to the specified Virtual Center.

The vCenter user must have the proper privileges listed in [Privileges Required for VMware Virtual Center](#).

## Deploy GigaVUE-VM Nodes

GigaVUE-VM software package is distributed as a hardened OVA file.

Deploying GigaVUE-VM nodes on an **ESXi host** consists of the following major steps:

- Configure port-groups and port-profiles within vSphere. Refer to [Configure Port Groups/Port-Profiles](#).

**NOTE:** Set up the connection between the Fabric Manager and the Virtual Center. Refer to [Set up Connection between GigaVUE-FM and Virtual Center](#).

- Deploy GigaVUE-VM nodes using the Bulk Deploy feature in GigaVUE-FM. Bulk-deployed nodes are automatically added to GigaVUE-FM's list for management. Refer to [Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster](#).



- The Bulk Deploy process replaces the manual OVF package deployment procedure used to install GigaVUE-VM nodes in previous releases. Gigamon recommends using the Bulk Deploy feature for all GigaVUE-VM node installations.
- If the host is part of a DRS cluster, the GigaVUE-VM node is automatically pinned to the host if the permissions are available. Pinning the host avoids automatic migrations. The permission required for pinning the host is Host\Inventory\Modify Cluster.

## Configure Port Groups/Port-Profiles

GigaVUE-VM nodes use Port Groups (vSphere Standard Switch and vSphere Distributed Switch) for management, network, and tunneling traffic, as follows:

- One port group/port-profile for management communications with the GigaVUE-VM node.
- One port group/port-profile for network monitoring of traffic crossing the virtual switch.
- One port group/port-profile for the starting point of the GigaSMART tunnel used to forward virtual network traffic to the Gigamon Visibility Fabric nodes.

Before deploying GigaVUE-VM in a vSphere environment that uses the native standard switch implementation, you need to use the vSphere Client to configure port groups for management, tunneling, and network traffic. You select these port groups during deployment of the GigaVUE-VM node, so they must be configured before deploying the OVA file.

**NOTE:** It is important that the port group assigned to the GVM network ports are not uplinked.

The following table shows the GigaVUE-VM traffic and corresponding virtual switches used for port group/port-profile creation. **Yes** indicates that you can create a port group/port-profile for the GigaVUE-VM traffic, while **No** indicates no action is required.

GigaVUE-VM	vSS	vDS
Management	Yes	Yes
Tunnel	Yes	Yes
Network	No	Yes

Refer to the following sections for information on setting up Port Groups/Port-Profiles:

- [Configure Port Group/Port-Profile for GigaVUE-VM Management](#)
- [Configure Port Group/Port-Profile for GigaVUE-VM Tunnel](#)
- [Configure Port Group/Port-Profile for GigaVUE-VM Network](#)

### Configure Port Group/Port-Profile for GigaVUE-VM Management

You can configure a port group/port-profile for GigaVUE-VM Management traffic using:

- vSphere Standard Switch
- vSphere Distributed Switch

In general, the Management port group must be connected to a dedicated out-of-band network to ensure access. See [Best Practices for vSphere Integration](#).

For convenience, it is suggested that you use, **PG\_GVM\_Management** for the Management port group name to help you deploy multiple nodes using the GigaVUE-VM Bulk Deploy feature.

## Configure Port Group/Port-Profile for GigaVUE-VM Tunnel

You can configure a port group/port-profile for GigaVUE-VM Tunnel traffic using:

- vSphere Standard Switch
- vSphere Distributed Switch

In general, for optimal performance, you must maintain the IP interface on a dedicated VMNIC rather than sharing the same VMNIC as the Management or Network Ports. See [Best Practices for vSphere Integration](#).

For convenience, it is suggested that you use, **dvPG\_GVM\_Tunnel** for the Tunnel port group name to help you deploy multiple nodes using the GigaVUE-VM Bulk Deploy feature.

## Configure Port Group/Port-Profile for GigaVUE-VM Network

You can configure a port group/port-profile for GigaVUE-VM Network traffic using vSphere Distributed Switch

## Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster

You can deploy a single GigaVUE-VM node or multiple GigaVUE-VM nodes simultaneously using the **Bulk Deploy** feature. All nodes added using this feature are automatically added to the GigaVUE-VM's list of managed nodes available for review in the **Management** page for VMware vCenter.

Nodes deployed using the Bulk Deploy feature can either be assigned a static IP address or use DHCP to obtain an IP address. GigaVUE-FM automatically discovers the IP address assigned to the GigaVUE-VM node and displays it with the node's entry in the **Virtual Nodes** page.

**NOTE:** If for some reason the DHCP server is unable to allocate an IP address for a GigaVUE-VM node, the node will be listed in the **Virtual Nodes** page with an Unconfigured entry in the GigaVUE-VM IP column. If this occurs, make sure the DHCP server is up and accessible, and then go to **Virtual Nodes** page and click **Rediscover**.

**IMPORTANT:** Before you use the Bulk Deploy feature, make sure you have already added a Virtual Center server to GigaVUE-FM by selecting **Inventory > VIRTUAL > VMware > vCenter > Management > Virtual Centers** and adding the Virtual Center.

The following procedure explains how to use the Bulk Deploy feature:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management > Virtual Nodes**.
2. Click **Deploy Virtual Nodes**.



3. Open the OVA control plane and select the OVA image file to be used for the Bulk Deployment. Use the **Browse** and **Upload to Server** buttons to upload an image file from your local client computer to GigaVUE-FM, or use an **Existing File** that has already been uploaded to GigaVUE-FM.

If you upload a new OVA file, make sure that you do not exit the upload page until the file has completely uploaded. Leaving the page will cancel an upload in progress.

**Existing File** does not appear in the **File Name** field until after an image file has been uploaded to GigaVUE-FM.

4. **End User License Agreement**—after careful review of the EULA, select **I accept the End user License (“EULA”)**.

5. **Disk Provisioning**—select the provisioning policy to be used by the virtual disk for GigaVUE-VM nodes.

6. Open the Hosts Properties control plane, and then click **Select Hosts** to select the host where you want to deploy GigaVUE-VM nodes.

The wizard that appears automatically displays all available ESXi hosts associated with the selected data center or cluster (ESXi hosts with existing GigaVUE-VM nodes installed are not listed).

A cluster is defined in the data center as a group of hosts. GigaVUE-VM does not manage creation or modification of the cluster or clusters. It only reads the cluster information. If the Datacenter does not have any cluster, the option in the drop down for the cluster will state None while all the hosts are still available.

- o Select each host where you would like to deploy a GigaVUE-VM node. You can select all hosts by selecting the **Host Name** checkbox.
- o Select the virtual center, Datacenter, and cluster with the ESXi hosts to be provisioned with GigaVUE-VM nodes. The drop-down lists all Datacenters and clusters in the Datacenter, available on the virtual center server specified in the **Virtual Centers** page.
- o Once you have selected the hosts where you want to deploy GigaVUE-VM nodes, click **OK** to continue.

7. Next configure settings for the GigaVUE-VM nodes to be deployed, supplying a name and password and selecting the port groups for management, tunnel, and network ports.

**IMPORTANT:** Make sure you have configured port groups using the instructions in [Configure Port Groups/Port-Profiles](#) before assigning IP addresses to the Mgmt and IP interfaces using DHCP. This ensures that GigaVUE-VM nodes are deployed with a desired IP address.

## Set Bulk Values

**Set Bulk Value** feature makes it easy to apply the same template of settings to all GigaVUE-VM nodes selected for deployment:

1. Click the **Set Bulk Values** button and choose settings for each of the options.
2. After clicking the **OK** button, you will return to the list of hosts with the new bulk values applied to each host in the list.
3. Once you have applied bulk values, you can go back and edit any necessary settings for specific individual nodes. This can be a time saving feature when deploying a large number of nodes.

Regardless of whether you select **Set Bulk Values** or configure individual nodes, you set the same set of options described in [Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster](#).

GigaVUE-VM Node Option	Description
<b>Datstore</b>	Select the datastore on the target host where the GigaVUE-VM node should be installed.
<b>Power</b>	Choose whether to power on the GigaVUE-VM node after deployment.
<b>GigaVUE-VM Name</b>	Supply a name for the GigaVUE-VM node. The name supplied here will be used to identify the GigaVUE-VM instance in Virtual Center.  If you are applying bulk values, you choose a suffix to be used for individual hostnames, assuring that names are not duplicated. GigaVUE-FM automatically prepends the specified prefix with the ESXi hostname. DNS support for these hostnames is provided.
<b>Password</b>	Supply and confirm a password for the GigaVUE-VM node. Passwords must contain at least eight characters with one numerical character, one upper case character, one lower case character, and one special character (for example, \$, %, !, and so on). The maximum number of characters is 30.
Use the drop-down lists to select the port groups (vSphere Standard Switch) for the Management Port, IP interface, and Network Port for the GigaVUE-VM instance. The port groups you configured in <a href="#">Configure Port Groups/Port-Profiles</a> are available for assignment.	
<b>Management Switch/Port Group Management IP</b>	This is the port used for communications between GigaVUE-VM and GigaVUE-FM. This port does not carry monitored traffic. You can either assign a Static IP address or use DHCP. GigaVUE-FM automatically discovers the assigned address and displays it in the <b>Management &gt; Virtual Nodes</b> page.  If you are configuring bulk values, you can specify a range of static IP addresses to be used. Note that the range specified must consist of contiguous values (for example 10.1.1.25 to 10.1.1.50 with a subnet mask of 255.255.255.0) and must not overlap with a range specified for the Tunnel Port Group.
<b>Tunnel Switch/Port Group Tunnel IP</b>	This port that is used as the starting point for that GigaSMART tunnel that will carry packets matching a vMap to the Gigamon visibility fabric. The other end of the tunnel is a Network-Tunneled Port on a GigaVUE Cloud

GigaVUE-VM Node Option	Description
	<p>Suite-2404, or a GigaVUE H Series family with GigaSMART blade and tunneling encapsulation enabled.</p> <p>You can either assign a Static IP address or use DHCP. If you are configuring bulk values, you can specify a range of static IP addresses to be used. Note that the range specified must consist of contiguous values (for example 192.168.1.25 to 192.168.1.50 with a subnet mask of 255.255.255.0) and must not overlap with a range specified for the Management Port Group.</p> <p><b>Note:</b> For optimal performance, Gigamon recommends maintaining the IP interface on a separate subnet than that used by the management port or network ports.</p>
Network Switch/Port Group	These are the ports that GigaVUE-VM uses to monitor network traffic. All of the virtual switch traffic being monitored arrives at the GigaVUE-VM node via these ports.
Deployment folder	Parameter to indicate where GVM should be deployed (optional).

4. Click **Deploy** when you have finished configuring settings for GigaVUE-VM nodes. The wizard reminds you to disable automatic cluster migration for each GigaVUE-VM node. This prevents situations where migration could inadvertently cause a situation with two GigaVUE-VM nodes on the same host, which is not allowed. Refer to [Best Practices for vSphere Integration](#) for details and additional tips on configuring vSphere settings for GigaVUE-VM nodes.
5. Click **Finish** to launch the Bulk Deploy. To monitor the progress of the Bulk Deploy:
  - a. On the left navigation pane, select **Dashboard > SYSTEM > Events**. The **Events** page appears.

### Events Filter Manage

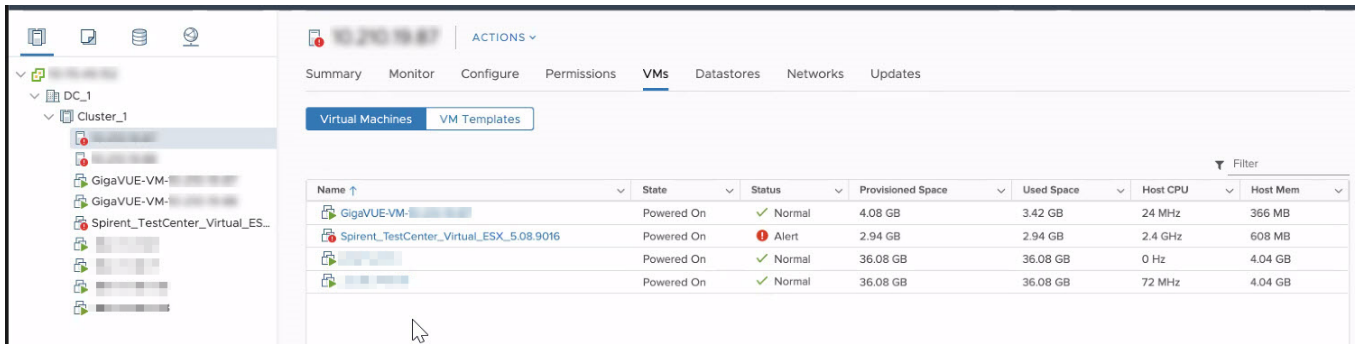
Events: 60 | Filter : none

Source	Time	Scope	Event Type	Severity	Affected Entity Type	Affected Entity	Description	Device IP	Host Name	Tags
VMM	202...	vNode	NodeUp	Info	Fabric Node Spec		Node Up ...			
VMM	202...	vNode	NodeReb...	Info	Fabric Node Spec		Reboot fo...			
VMM	202...	vNode	NodeUnr...	Info	Fabric Node Spec		Node Unr...			

|<
<
Go to page: 
of 9
>
>|
Total Records: 60

For example: Bulk Deploy takes place by deploying an initial OVF template to the first requested host. Once the initial OVF file is deployed, vSphere clones that template to all other requested hosts. Cloning takes place in waves of four GigaVUE-VM nodes at a time - if you request a Bulk Deploy of 21 GigaVUE-VM nodes, the OVF file is deployed to the first node in the list, followed by two successive waves of four cloned nodes.

6. Once the Bulk Deploy completes, log in to the vSphere Client and verify that there is only one GigaVUE-VM node installed per ESXi host. For example, after navigating to the **VMs > Virtual Machines** tab for the ESXi host on 10.210.17.11, we can see that there is only one GigaVUE-VM node installed.

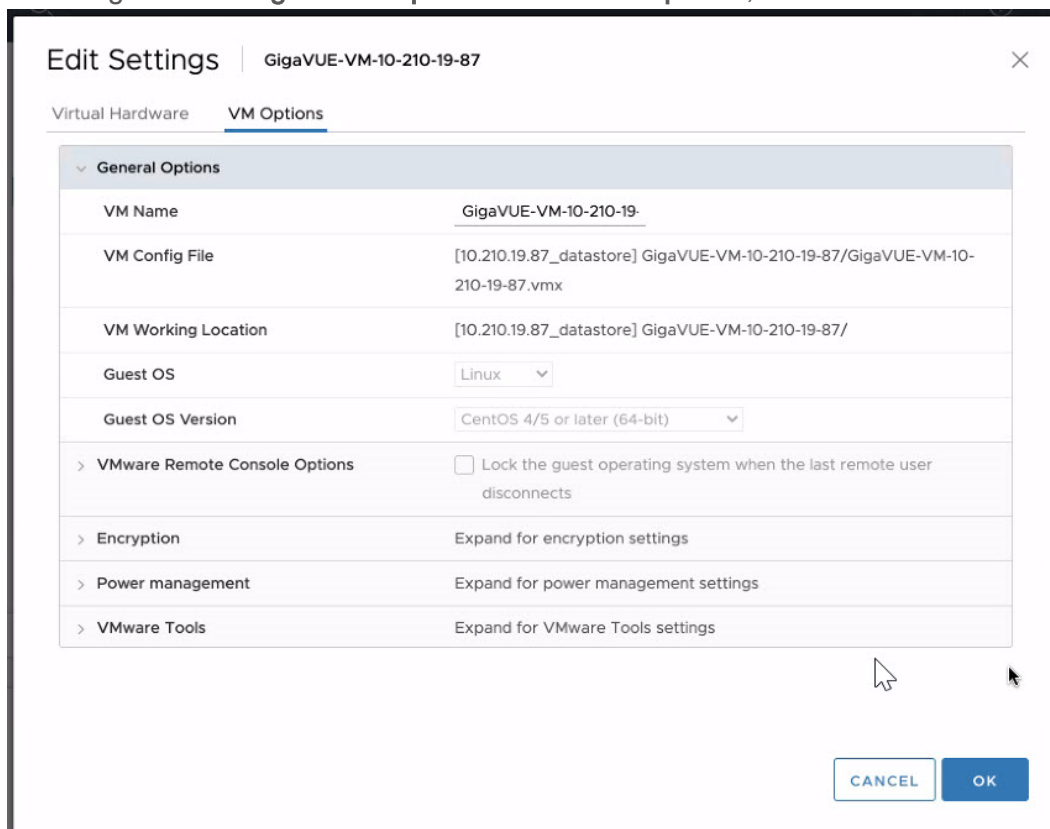


## GigaVUE-VM vApp Product Name

The installation wizard automatically configures all GigaVUE-VM nodes with a **Product Name** of **GigaVUE-VM**. GigaVUE-FM recognizes GigaVUE-VM nodes using this name. The Product Name must remain **GigaVUE-VM** at all times - do not change it to another value.

**NOTE:** The name is not case-sensitive, so you can change it to **gigavue-vm** if your environment requires lowercase names.

You can see the **Product Name** by right-clicking a GigaVUE-VM node in the vSphere Data Center and choosing **Edit Settings > VM Options > General Options**, as shown in the following figure:



The screenshot shows the 'Edit Settings' dialog for a VM named 'GigaVUE-VM-10-210-19-87'. The 'VM Options' tab is selected, and the 'General Options' section is expanded. The settings are as follows:

Setting	Value
VM Name	GigaVUE-VM-10-210-19-
VM Config File	[10.210.19.87_datastore] GigaVUE-VM-10-210-19-87/GigaVUE-VM-10-210-19-87.vmx
VM Working Location	[10.210.19.87_datastore] GigaVUE-VM-10-210-19-87/
Guest OS	Linux
Guest OS Version	CentOS 4/5 or later (64-bit)
VMware Remote Console Options	<input type="checkbox"/> Lock the guest operating system when the last remote user disconnects
Encryption	Expand for encryption settings
Power management	Expand for power management settings
VMware Tools	Expand for VMware Tools settings

At the bottom right of the dialog, there are 'CANCEL' and 'OK' buttons.

## Configure Tunnel Endpoint

Virtual packets find their way to physical tool ports through a GigaSMART tunnel. The tunnel starts at the GigaVUE-VM node and ends at a network port on a GigaSMART-enabled G Series or H Series node. In both cases, the receiving end of the tunnel must have a tunnel decapsulation GigaSMART Operation bound.

This section covers the following topics:

- [Tunnel Configuration Options](#)
- [Create Tunnel Endpoint](#)
- [Tunnel Validation](#)
- [Configure H Series IP Interfaces for the GigaVUE-VM Tunnel Library](#)
- [TCP Tunnel between GigaVUE-VM and GigaVUE Cloud Suite HC Series Nodes](#)

### Tunnel Configuration Options

This section describes the options available when configuring tunnel endpoint for GigaVUE-VM.

#### Tunnel End Points

When adding a tunnel endpoint in the Tunnels Library, you are provided with two options:

- **GigaVUE Cloud Suite**  
The GigaVUE Cloud Suite option lists all the IP interfaces available on the GigaVUE H Series nodes that are connected to the GigaVUE-FM.
- **Other**  
This option gives users the option to add a new IP interface that may not be listed in the GigaVUE Cloud Suite Tunnels Library. G-Series tunnel endpoints are not auto-discovered by the Tunnels Library. So use the Other option to add this tunnel.

Creating a GigaSMART tunnel requires configuration on both the sending and receiving ends:

Sending End of Tunnel	Receiving End of Tunnel
<p>When you provision a vMap for a GigaVUE-VM node through GigaVUE-FM, in addition to selecting the virtual traffic to be forwarded, you also specify the destination and source for traffic to be tunneled with the following settings:</p> <ul style="list-style-type: none"> <li>■ <b>Tunnel Destination IP</b> – The IP address of the tunneled network port on the receiving end of the tunnel for L2GRE. For GMIP, ERSPAN: The IP</li> </ul>	<p>The receiving end of the tunnel should be configured as follows:</p> <ul style="list-style-type: none"> <li>■ Configure a Network Tunneled port with an IP address, subnet mask, and default gateway. The IP address must match the destination IP address specified at the sending end of the tunnel.</li> <li>■ Create a GigaSMART operation with a tunnel decapsulation component. The Decapsulation settings</li> </ul>

Sending End of Tunnel	Receiving End of Tunnel
<p>address of the IP interface on the H Series device with GigaSMART (ERSPAN is only supported for VMware).</p> <ul style="list-style-type: none"> <li>■ <b>Tunnel Destination Port</b> – The listening UDP port at the destination end of the GigaSMART tunnel for GMIP only. This should be the port that is configured to receive traffic from the GigaVUE Cloud Suite-VMs.</li> <li>■ <b>Tunnel Source Port</b> – The port on the GigaVUE-VM from which mirrored traffic is originating. Enter 1 if this is not expected to be used.</li> </ul>	<p>include the same listening UDP port you specified as the destination port at the sending end of the tunnel.</p> <ul style="list-style-type: none"> <li>■ Bind the GigaSMART operation to the Network Tunneled port as part of a map that distributes arriving traffic to local tool ports for analysis with local tools.</li> </ul>

## DSCP

When configuring an IP interface in the Tunnels Library, you can specify a Differential Service Code Point (DSCP) value. (DSCP is only supported on GMIP and GRE tunnels.) This value is a 6-bit field in the IP header and specifies the Per-Hop Behavior (PHB). DSCP allows traffic to be classified so that each traffic class can be managed differently, ensuring preferential treatment for higher-priority traffic on the network.

For GigaVUE-VM traffic to receive preferential treatment in the network, a specific DSCP value can be chosen by the service provider per tunnel. The DSCP values fall into the following three categories:

- Default PHB—best effort traffic. Select a value of 0 for DSCP to specify Default PHB.
- Expedited Forwarding (EF) PHB—dedicated to low-loss, low-latency traffic. Select EF for DSCP to specify this PHB.
- Assured Forwarding (AF) PHB—gives assurance of delivery under prescribed conditions. There are four classes of AF vales and each class is further divided by drop probability. The classes are defined in [Table 1: AF Behavior Group Classes](#).

In addition to these three categories, values from 0 to 63 are allowed.

Table 1: AF Behavior Group Classes

Drop Probability	Class 1	Class 2	Class 3	Class 4
Low	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Medium	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
High	AF13 (DSCP14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

## Fragmentation

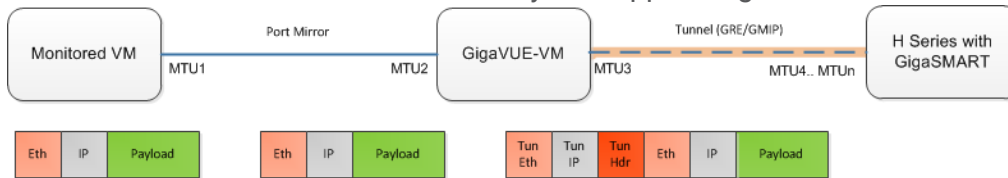
GigaVUE-VM allows fragment of packets leaving the tunnel. Fragmentation can be enabled or disabled per tunnel. Fragmentation is needed if the tunneled packet size plus the tunnel header size is greater than the tunnel MTU size. If fragmentation is not specified in this situation, the tunneled packet is dropped. IP

fragment reassembly occurs at the H Series nodes starting with GigaVUE-OS 4.6. For versions lower than version GigaVUE-OS 4.6, it is suggested that fragmentation be disabled on the GigaVUE-VM.

Support for fragmentation is as follows:

- Fragmentation is only supported for IPv4 packets.
- Fragmentation and reassembly is not supported on ERSPAN tunnels.
- Packets encapsulated with a GRE header on G-vTAP Agents do not undergo fragmentation in the current release.
- GigaVUE-VM does not reassemble GRE packets received from the G-vTAP Agent.
- Filtering on fragmented packets is from layer 2 to layer 3 because only the first fragment will have the transport header. In the current release, GigaVUE-VM does not support filtering on fragments for layer 4.

In VMware environments, packets can be dropped when the packet frame length is greater than the GigaVUE-VM tunnel MTU after adding the tunnel header. In this case, the packets are fragmented and sent out of the tunnel interface. However, it is not guaranteed that the packet will reach the GigaVUE H Series because intermediate devices may not support fragmentation.



## Create Tunnel Endpoint

The section provides the steps for creating a GigaVUE-VM tunnel to a GigaSMART device from a virtual environment.

To create a tunnel, do the following:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The Management page appears.
2. In the **Tunnels Library** tab, click **Add**. The **Add Tunnel Endpoint(wu)** page appears.
3. All the available GigaVUE Cloud Suite tunnels appears on the Add Tunnels Endpoint page.
  - a. Select the tunnel that is configured to receive traffic from the GigaVUE Cloud Suite-VMs.
  - b. Enter the **Tunnel Source Port**.  
This value can be used on the H Series GigaSMART device to associate which source port the mirrored traffic is originating from. Enter 1 if this is not expected to be used.  
For more information about tunnel source ports, refer to [Tunnel Configuration Options](#).
  - c. Click **OK**.



If the desired GigaVUE Cloud Suite tunnel was not discovered, the tunnel was not configured correctly for it to be eligible for a GigaVUE-VM endpoint. For information about correctly configuring the tunnel, refer to [Configure H Series IP Interfaces for the GigaVUE-VM Tunnel Library](#).

For non-Gigamon tunnels, you must enter the tunnel information manually by doing the following:

- a. Select **Other**.
- b. For **Type**, select **GMIP**, **L2GRE**, **ERSPAN**, or **GTCP**

If you select, ERSPAN, only the Destination Tunnel IP field is displayed. If you select, L2GRE, the Destination Tunnel IP, DSCP, and Fragmentation fields are displayed.

- c. Specify the following:

- **Destination Tunnel IP**
- **Tunnel Destination Port**
- **Tunnel Source Port**

If a tunnel source port is not expected to be used, enter 1.

For more information about the tunnel IP and the tunnel source and destination ports, refer to [Tunnel Configuration Options](#).

- d. (Optional) Select the **DSCP** value. For more information, refer to [DSCP](#).
- e. (Optional) Enable **Fragmentation** to allow GigaVUE-VM to fragment large packets. For more information on fragmentation, refer to [Tunnel Configuration Options](#).

4. Click **OK**.

## Tunnel Validation

Users are provided with the selection for tunnel validation. This ensures that the tunnels are terminating to a valid physical node and are configured correctly. This is especially important to ensure that the GigaVUE-VM traffic terminates at the appropriate location and is not dropped. GigaVUE-FM provides feedback if the tunnel is malfunctioning (for example, traffic is not correctly flowing to the end point) or if the IP interface is down or missing. This is to ensure timely and prompt debug of any issues relating to the tunneling of the GigaVUE-VM traffic.

A **Tunnel Validation** button is available on the Virtual Nodes page and Virtual Maps page for VMware vCenter. The following figures show the tunnel validation selection on the pages for VMware vCenter. Additionally from the Virtual Nodes page for VMware vCenter, you can select a node, and then select tunnel validation. This brings up the quick view for tunnel status that provides you with the option to ping or traceroute to valid the tunnel path. The purpose of this is to validate whether GigaVUE-VM eth1 can reach the tunnel endpoint.

**NOTE:** Tunnel status from G Series node will always show as Red. This does not imply that the port is inactive.

## Configure H Series IP Interfaces for the GigaVUE-VM Tunnel Library

The Tunnel Library allows you to add the tunnel endpoints into the Tunnels Library that are configured on GigaVUE Cloud Suite nodes. However, not every tunnel endpoint that is configured on a physical device is listed in the library. A tunnel endpoint is listed in the library based on the following criteria:

- The IP interface must be configured as a Network port.
- The Network Tunneled port must be configured as a source port in the map on a physical device.
- The GigaSMART Operation for the maps on the GigaVUE Cloud Suite nodes must have a Tunnel Decapsulation application defined. The GigaSMART Operation must also be linked to a GigaSMART Group.
- The Tunnel decapsulation application must support GMIP, ERSPAN, or L2GRE. However, make sure to define the port destination as a GMIP port.

To configure the tunnel endpoint, do the following:

1. Add a Physical Node to GigaVUE-FM.

For the steps to add a GigaVUE Cloud Suite node to GigaVUE-FM, refer to “Add New Physical Node or Cluster to GigaVUE-FM” in the *GigaVUE Fabric Management Guide*.

If you want to use the port on an physical node already added to GigaVUE-FM, do the following:

- a. From the left navigation pane, select **Inventory > PHYSICAL > Nodes**. The **Physical Nodes** page appears.

### Physical Nodes

Tags ▾ Actions ▾ Filter Create Cluster Add Delete Import Export ▾

Total Nodes: 50 | Filter : none

<input type="checkbox"/>	Cluster ID	Host Name	Task Status	Node Address	Role	Mode
<input type="checkbox"/>	c1c10000	dev1.c1.0000.proxy-c1-1		dev1.c1.0000.proxy-c1-1	Master	HC3
<input type="checkbox"/>	c1c10001	dev1.c1.0001.proxy-c1-2		dev1.c1.0001.proxy-c1-2	Master	HC3
<input type="checkbox"/>	c1c10002	dev1.c1.0002.proxy-c1-2		dev1.c1.0002.proxy-c1-2	Master	HC3

- b. Click the Cluster ID of a node/device on which you want to configure the tunnel end point by clicking the node’s IP address or DNS name.

2. Enable the port to use as an endpoint for the tunnel:

- a. In the Physical Node Overview page, navigate to **Ports > Ports > All Ports**.
- b. Select the port to define as an IP interface and click **Edit**.
- c. On the port configuration page, do the following:
  - (Optional) Enter a name in the **Alias** field to help identify the port.

- (Optional) Enter any additional comments in the **Comments** field.
  - **Enable** Admin.
  - Select **Network** for Type.
  - Set Duplex to **Full**.
  - **Enable** Autonegotiation.
  - Click **Save**.
3. Create a GigaSMART Group.
    - a. Select **GigaSMART Groups**.
    - b. Click **New**.
    - c. Enter a name for the GigaSMART Group in the **Alias** field.
    - d. Add an engine port in the **Port List** field.
    - e. Click **Save**.
  4. Configure the tunnel endpoint.
    - a. Select **Ports > IP Interfaces**.
    - b. Click **New**.
    - c. Configure the IP interface as follows:
      - In the **Alias** and **Comment** fields, enter the name and description for the IP interface.
      - Select the port configured in [Step 2](#) for **Port**.
      - Enter the **IP Address**, **IP mask**, **Gateway**, and **MTU**.
      - Select the **GigaSMART Group** configured in [Step 3](#).
    - d. Click **Save**.
  5. Configure the GigaSMART Operation.
    - a. Select **GigaSMART > GigaSMART Operations (GSOP)**.
    - b. Click **New** to add a new GSOP.
    - c. Configure the GSOP as follows:
      - Enter a name for the GSOP in the **Alias** field.
      - Select the **GigaSMART Group** configured in [Step 3](#).
      - Select **Tunnel Decapsulation** for the **GigaSMART Operations (GSOP)**.
      - Select the type for the tunnel decapsulation, which is ERSPAN, GMIP, or L2GRE. For ERSPAN, enter a Flow ID. For GMIP, enter the GMIP port. For L2GRE, enter the key.
    - d. Click **Save**.
  6. Create a map.

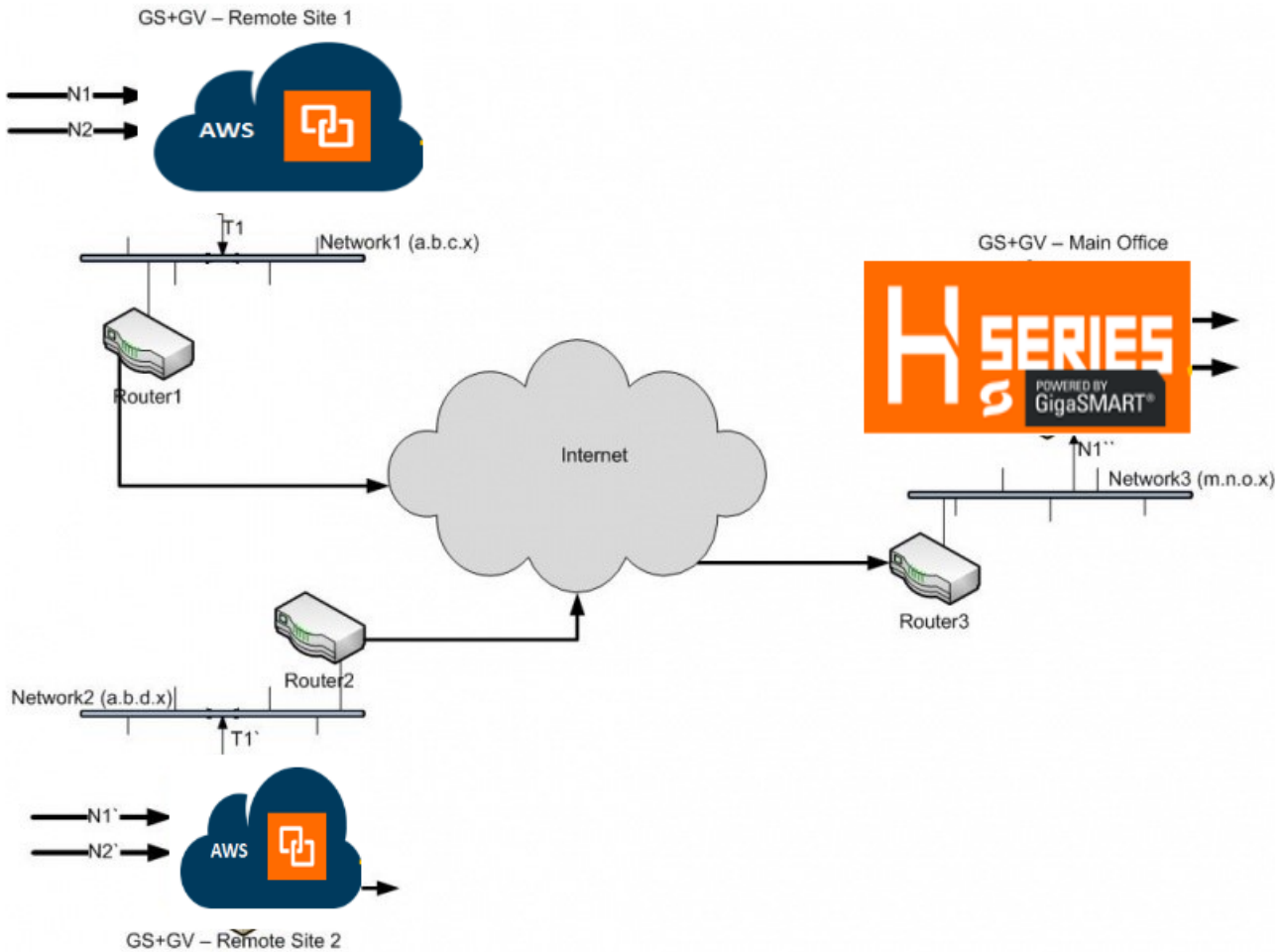
- a. Select **Maps > Maps**.
- b. Click **New**.
- c. Configure the map as follows:
  - Enter a name for the map in the **Alias** field.
  - For **Type**, select **Regular**. For **Subtype**, select **By Rule**.
  - For **Source**, select the port configured in [Step 2](#).
  - For **Destination**, select a tool port, tool port group or tool GigaStream.

**NOTE:** The Destination list displays the available tool ports, tool port groups or tool GigaStreams, including the port aliases and port IDs, as well as the port utilization status (percentage used) of any ports already in use. Utilization status support is available for Individual and Hybrid tool ports.

- Select the **GigaSMART Operation (GSOP)** created in [Step 5](#).
  - Use **Add a Rule** to a rule pass all IPv4 and a rule to pass all IPv6 traffic, depending on your requirements.
- d. Click **Save**.
7. Add the tunnel endpoint to GigaVUE-FM. Refer to [Create Tunnel Endpoint](#) for detailed information.

## TCP Tunnel between GigaVUE-VM and GigaVUE Cloud Suite HC Series Nodes

TCP tunnel feature routes the mirrored traffic from GigaVUE-VM to remote GigaVUE Cloud Suite HC Series nodes reliably and without any reorder issues. TCP tunnel encapsulation is supported in the GigaVUE-VM node and the TCP tunnel decapsulation is supported in the GigaVUE Cloud Suite HC Series node. Tunnel decapsulation can terminate more than one TCP connection initiated by the GigaVUE-VM node.



The following are the steps to configure TCP tunnel between GigaVUE-VM and GigaVUE Cloud Suite HC Series Nodes:

- Configure GigaVUE-VM For Encapsulation
- Configure vMap for VMware
- Configure HC Series Nodes for Decapsulation

### Create TCP Tunnel in GigaVUE-VM

The section provides the steps for creating a GigaVUE-VM tunnel to a GigaSMART device from a virtual environment. Before you create the tunnel refer to the following sections in this guide:

- [How to Use GigaVUE-VM vCenter Management](#)
- [Set up Connection between GigaVUE-FM and Virtual Center](#)
- [Bulk Deploy GigaVUE-VM Nodes in Standalone or Cluster](#)

To create a tunnel:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The Management page appears.
2. In the **Tunnels Library** tab, select **Add**. The **Add Tunnel Endpoint(wu)** page appears.
3. In the Add Tunnel Endpoint(wu), select **Other**.

## Add Tunnel Endpoint(wu)

OK

Cancel

Port:	<input type="radio"/> GigaVUE® <input checked="" type="radio"/> Other
Type	GTCP <input type="text"/>
Destination Tunnel IP	IP Address <input type="text"/>
Tunnel Destination Port	0 - 65535 <input type="text"/>
Tunnel Source Port	0 - 65535 <input type="text"/>
DSCP	select.. <input type="text"/>
Fragmentation	<input type="checkbox"/> Enabled

\* Note: You are adding a non-GigaVUE tunnel port to Library

4. For Type, select **GTCP** and specify the following:
  - Destination Tunnel IP
  - Tunnel Destination Port
  - Tunnel Source Port
5. Select the DSCP value. This is optional.
6. Enable Fragmentation to allow GigaVUE-VM to fragment large packets. This is optional.
7. Click **OK**.

## Configure Virtual Maps for VMware VCenter

To configure the virtual maps for VMWare VCenter, refer to the following section in this guide:

### [Configure Virtual Maps for VMware vCenter](#)

## Configure GigaVUE Cloud Suite HC Series Devices for Decapsulation through CLI

To configure GigaVUE Cloud Suite HC series devices for decapsulation:

1. Create a GigaSMART Group with the required engine.`gsgroup alias gsggrp1 port-list 1/1/e1`
2. Create an IP interface and attach the required network port. Add GigaSMART group to the IP interface.

```
ip interface alias ip1
```

```
attach 1/1/g1
ip address 2.2.2.3 /24
gw 2.2.2.5
gsgroup add gsgrp1
exit
```

3. Create a listener with type tunnel and I4 protocol tcp.

```
apps listener alias lis1
type tunnel
l4 port-list 3456
l4 protocol tcp
l3 protocol ipv4
l3 ttl 64
l3 dscp 0
mode l3 interface
exit
```

4. Create a tunnel-decap gsop with type tcp and add listener to the GSOP.  
`gsop alias decap_gsop tunnel-decap type tcp add lis1 port-list gsgrp1`
5. Designate the port connected to tool as tool-port.  
`port 1/1/x7 type tool`
6. Create a map with the above IP interface port as from port and tool connected port as tool port.
7. Use the above GSOP in the map.
8. Use map rules with base L4 port of listener as the portdst and source L4 port of the GVM as portsrc.

```
map alias decap
type regular byRule
roles replace admin to owner_roles
use gsop decap_gsop
rule add pass ipver 4 portdst 3456 portsrc 12346
to 1/1/x7
from 1/1/g1
exit
```

## Configure GigaVUE Cloud Suite HC Series Devices for Decapsulation through GigaVUE-FM

1. Configure the GigaSMART engine group.
2. Configure the IP interface on network port.
3. Validate the ARP state.

**Global Settings**   Security   Web   SNMP   SNMP v3 Users   SNMP Traps   SSH

Hostname   Logging   Event Notification   Email Notifications   ARP/NDP

Clear   Settings

**Settings**

ARP Refresh Time Interval (Seconds)   30

NDP Refresh Time Interval (Seconds)   30

**ARP Entries**

IP Address	Hardware Address	Age	State	Interface
1.1.1.1	00:1d:ac:7a:04:eb	00:00:04	Reachable	1/1/x7

4. Configure the listener profile.

**NOTE:** From your Physical Node Overview page, select **GigaSMART > TCP/IP Host > Listeners** to reach the Listener page.

**Listener**   OK   Cancel

Alias *	Description
Application Type	
Tunnel	
L3 Protocol	L4 Protocol *
IPv4	TCP
TTL	DSCP
1 - 255	0 - 63
L4 Port *	
1 - 65535	



5. Configure the GigaSMART operation.

**GigaSMART Operation (GSOP)**
OK Cancel

Alias	<input type="text" value="gsop1"/>
GigaSMART Group	<input type="text" value="gs1"/>
GigaSMART Operations (GSOP)	<input type="text"/>

**Tunnel Decapsulation** ✕

TCP

Listener Alias

lst1

6. Configure the Map as shown in the image.

**New Map** Dec 13, 2019 14:32:30
OK Cancel

▼ Map Source and Destination

Port Editor
Tool Finder

Source	<input type="text" value="N 1/1/x7"/>
Destination	<input type="text" value="T 1/1/x8"/>
Encapsulation Tunnel	<input type="text" value="None"/>
GigaSMART Operations (GSOP)	<input type="text" value="gsop1(gs1)"/>

▼ Map Rules

Quick Editor
Import
Add a Rule

✕ Rule 1   Pass  Drop  Bi-directional

Rule Comment

IP Version

Version

▼ Map Order

Priority

### Supported Devices

TCP tunnel decapsulation is supported in the following devices:

- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC3

## Limitations

The following are the limitation of the TCP tunnel decapsulation feature:

- On tunnel decap IP interface, MTU value should not be more than 1500.
- Only IPv4 is supported.
- GigaSMART engine grouping is not supported.
- TCP tunnel feature should not co-exist with GTP or iSSL.

## Configure Virtual Maps for VMware vCenter

To configure Virtual Maps on the virtual nodes for VMware, under VMware vCenter, go to **Virtual Maps** to view the Virtual Maps page.

**NOTE:** It is imperative that you create a tunnel prior to creating the maps. Verify that the tunnel is active by clicking **Tunnel Validation**. For information on how to create tunnels, refer to [Configure Tunnel Endpoint](#).

This page allows you to configure maps that define the traffic to be monitored on the virtual network adapters on different virtual machines. Before configuring maps, you first need to set up the connection between the Fabric Manager and the Virtual Center.

The Virtual Maps page has controls that allow you to create virtual maps and manage the information that appears on the table. The controls are described in the following table.

Table 2: Controls Available on the Virtual Maps Page

Controls	Description
<b>New</b>	Opens the Create Map dialog, allowing you to create a virtual map. (See <a href="#">Configure vMap for VMware</a> )
<b>Edit</b>	Opens the Edit Map dialog, allowing you to edit a virtual map.
<b>Delete</b>	Deletes the selected virtual map.
<b>Redeploy</b>	Redeploys the selected virtual map.
<b>Redeploy All</b>	Redeploys all of the virtual maps.
<b>Tunnel Validation</b>	Allows users to validate that an active tunnel exists between the GigaVUE-VM and IP interface on the Gigamon node.

The fields displayed on the virtual maps page are defined in the following table.

Table 3: Parameters Displayed in the Virtual Map Page for VMware vCenter

Column Parameter	Description
Map Alias	Alias for the virtual map that is unique and best if it describes the function of the vMap.
Virtual Center	Virtual Center where the GigaVUE-VM is deployed.
Comments	Brief description on the virtual map and its purpose.
VM Name	Name of the virtual machine that is using the virtual map. The virtual machines should belong to the virtual center listed in the 2nd column.
Deployment Status	<p>Deployment status of the map. The three states and conditions leading to the states are:</p> <ul style="list-style-type: none"> <li>■ <b>Success</b>—When the vMap is deployed in the vCenter environment as expected, which means: successfully created maps, gsops in GVMs, and necessary vssPG/ port mirror sessions in the vCenter.</li> <li>■ <b>Partial Success</b>—When any one of the aspect of creating a vMap fails, including failure to create maps or gsops in GVMs, or vssPG/ port mirror sessions in the vCenter.</li> <li>■ <b>Failure</b>—The status is unclear for FM. Click Redeploy to get the latest status is recommended. If the status does not change, contact Gigamon customer service to further identify the issue.</li> </ul> <p><b>NOTE:</b> The quick view provides information under the status tab about what part of the deployment has failed.</p>
Traffic	<p>Traffic column provides the status of the GigaVUE-VM traffic. The two states are:</p> <ul style="list-style-type: none"> <li>■ <b>Consistent</b>—When all the monitored vNIC are up and are able to transmit/receive traffic.</li> <li>■ <b>Inconsistent</b>—When one of the monitored vNIC is not able to transmit/receive traffic due to various possible reasons; for example, VM is powered off, vNIC is removed, or, vNIC is not connected.</li> </ul>
Tunnel Destination	Destination IP of the node where the tunnel terminates including the tunnel source port and destination port. This information is pulled directly from the IP interface that is created on the node and is available in the tunnels library.

When you select a map in the table, a quick view displays. The parameters covered in the quick view window are described in [Table 4: Parameters Displayed in the Virtual Map Quick View](#). By clicking on **Edit** on the quick view, you can review or update these parameters.

Table 4: Parameters Displayed in the Virtual Map Quick View

Parameters	Description
Virtual Map Info	The Virtual Center and Tunnel Destination information.
Status	The errors associated with the rule, if any. This will also list any issues that are preventing the deployment or traffic interruptions.
VM Map Rules	Map Rules defined for the virtual machine.
Network Adapters Monitored	Details relating to the vNIC.

## Configure vMap for VMware

To configure the vMap for VMware, do the following:

1. Click **New** to open the configuration page, which is shown in the following figure.

The screenshot shows the 'Virtual Map' configuration interface. At the top right are 'Save' and 'Cancel' buttons. The main area is divided into sections:

- VM Map Info:** Contains input fields for 'Alias', 'Comments', and a dropdown for 'Tunnel Destination'.
- Map Rules:** Features an 'Add a Rule' button. Below it, 'Rule 1' is configured with a dropdown menu, a checked checkbox for 'Bi-directional, Traffic flow', a 'from vNIC' dropdown, a 'Slicing' checkbox, and a text field containing '64-9000'. A detailed view of the rule shows fields for 'IPv4 Source', 'IPv4 Address', and 'Cidr(1-32)'.
- Virtual Machine Network Adapter:** Includes a 'Virtual Machine Browser' button.
- Table:** A table with columns for 'VM Name', 'Network Adapter', and 'Port Group'.

2. Enter an alias, comments (optional), and select the tunnel destination.

3. Add a rule or rules to the vMap by clicking **Add a Rule**. You can define a rule based on the following:

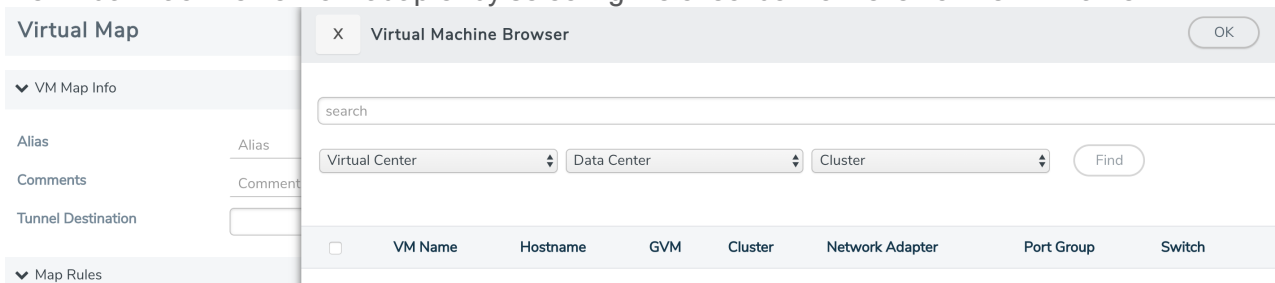
- Rule Type:
  - IPv4 Source
  - IPv4 Destination
  - IPv6 Source
  - IPv6 Destination
  - IPv6 Flow Label
- Protocol: TCP, UDP
  - Port Source
  - Port Destination
  - MAC Source
  - MAC Destination
  - VLAN

**NOTE:** If no rules are added to the vMap, then the vMap acts as a ‘pass all’ where in all the traffic coming from the vNIC are passed through the filter.

- Traffic Flow:
  - from vNIC
  - to vNIC

**NOTE:** For Virtual Map rules, the bidirectional option is always selected because traffic is always monitored in both directions while From vNic and To vNic options specify the filter criteria. The rule specifies the following on the GigaVUE-VM: monitor traffic that is coming from the vNIC and that is IPv4 Source. Because traffic is also monitored in the other direction, an additional rule will be created on the GigaVUE-VM, reversing the rule filter criteria appropriately. This rule will specify: monitor traffic that is going to the vNIC and that is IPv4 Destination.

4. Select a VM (Network Adapter) to associate with the vMap by clicking **Virtual Machine Browser**. This opens the Virtual Machine Browser where you can select the VM Network Adapter. Select the virtual center, data center, and optionally the cluster. Click **Find** to load the virtual machines. Select the virtual machine network adapter by selecting the checkbox to the left of the VM name.



5. Click **Save**.

**NOTE:** The vMap deployment may occasionally fail with error messages related to failed port mirroring session or failed vDS configuration. This is due to an orphaned port mirror session on vDS that is being configured. Using VMware or web client, identify and delete the orphaned port mirror session (with the name gvn2\_port number, where the referenced port number is not assigned to any interface) and redeploy the vMap.

## vMap Rules and Notes

Keep in mind the following rules when working with vMaps:

- Slicing can only be used together with other vMap rules. It cannot be used as the only criteria in a vMap.
- While editing a vMap's "Slicing" value in the GigaVUE-FM Virtual Map page, the vMap slicing field is validated to ensure you enter valid values (from 64 to 9000).
- After enabling slicing, you cannot disable it by editing the vMap; you must create a new vMap. You can edit the vMap later to adjust the Slicing offset values (within range); however, you cannot set them to an out-of-range value or disable Slicing after it has been enabled.

## Create vMap using a vNIC on vSS

When creating a vMap using a vNIC on vSS to monitor traffic, there are no additional actions to perform. The following occurs:

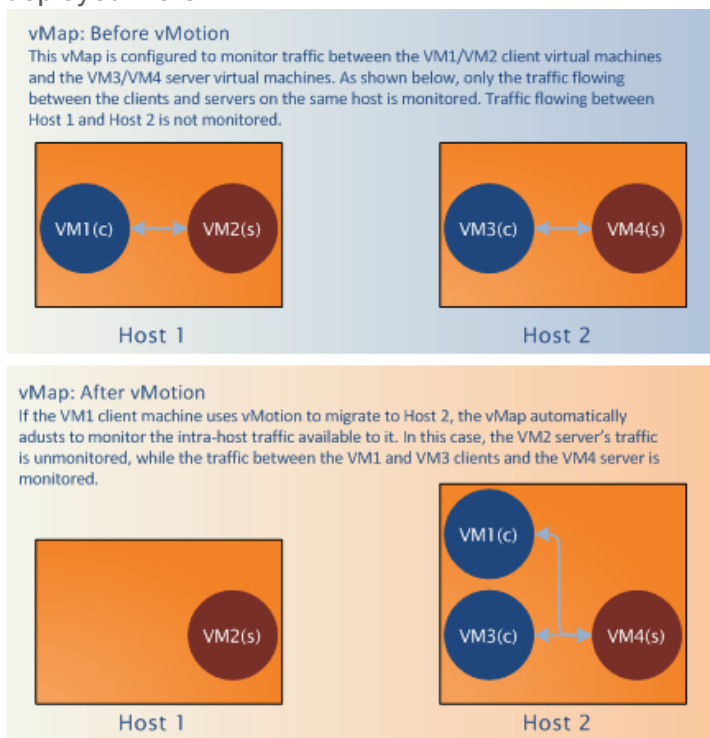
- GigaVUE-VM automatically creates a port group called, **GigaPG\_<vswitch name>** in order to monitor traffic.
- The port group is configured as **Promiscuous mode** with VLAN 4095.
- The port group is automatically deleted when deleting the vMap.

## vMaps and vMotion Migration

If a monitored virtual machine uses vMotion migration to move to a new host, GigaVUE-VM takes the following actions:

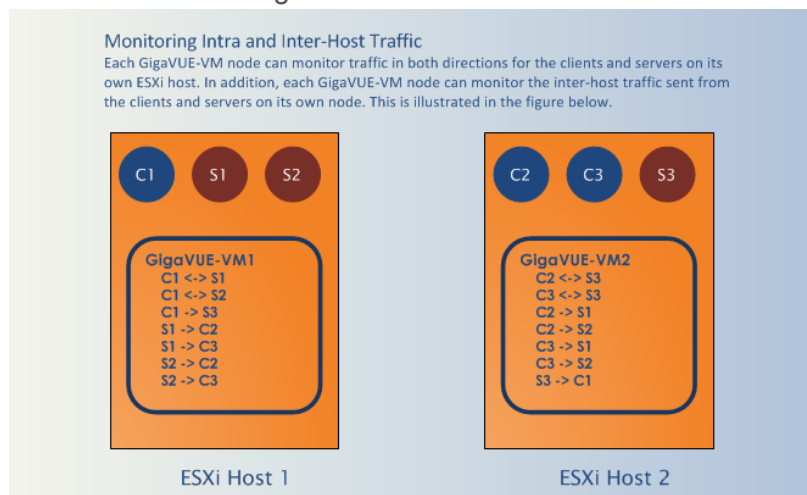
- Logs an entry in the Events page. To view the Events page, from the left navigation pane, go to **Dashboard > SYSTEM > Events**.

- Reconfigures maps to use GigaVUE-VM to deploy on the new host for the monitored VM if there is one deployed there.



## GigaVUE-VM: Monitor Intra-Host and Inter-Host Traffic

GigaVUE-VM includes the ability to monitor inter-host traffic when both hosts are instrumented with GigaVUE-VM nodes. The following figure illustrates how this works, summarizing the traffic available for monitoring between the Server and Client Virtual Machines (S1-S3 and C1-C3) on two different ESXi hosts instrumented with GigaVUE-VM nodes.



## Changes in vDS Port ID Require vMap Redeployment

If the vDS Port ID for a vNIC changes, any vMaps using the vNIC must be redeployed before their traffic begins to flow from network ports to tool ports again. Changes in a vNIC's vDS Port ID can happen in the following situations:

- A vNIC used by a GigaVUE-VM node is swapped from a vDS Port Group to a vSS Port Group and then back to a vDS Port Group. When the vNIC returns to the vDS Port Group, it will have a new vDS Port ID.
- A vNIC used by a GigaVUE-VM node is deleted from a vDS Port Group and then added back to the vDS Port Group. When the vNIC is added back to the vDS Port Group, it will have a new vDS Port ID.

## Bulk Upgrade GigaVUE-VM Nodes

You can upgrade a single GigaVUE-VM node or multiple GigaVUE-VM nodes simultaneously using the **Upgrade Virtual Nodes** feature. All nodes upgraded using this feature are shown in the GigaVUE-VM's list of managed nodes with the latest software version.

The following procedure explains how to use the Bulk Upgrade feature:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management > Virtual Nodes**.
2. Click **Upgrade Virtual Nodes**.
3. Open the OVA control plane and select the OVA image file to be used for the Bulk Deployment. Use the **Browse** and **Upload to Server** buttons to upload an image file from your local client computer to GigaVUE-FM, or use an **Existing File** that has already been uploaded to GigaVUE-FM. If you upload a new OVA file, make sure that you do not exit the upload page until the file has completely uploaded. Leaving the page will cancel an upload in progress. **Existing File** does not appear in the **File Name** field until after an image file has been uploaded to GigaVUE-FM.
4. **End User License Agreement** – After careful review of the EULA, select **I accept the End user License ("EULA")**.
5. **Disk Provisioning** – Select the provisioning policy to be used by the virtual disk for GigaVUE-VM nodes.



6. Open the GigaVUE-VM Properties and perform the following:
  - a. Select the virtual center from the **Virtual Center** drop-down list. The **Datacenter** field appears.
  - b. From the **Datacenter** drop-down list, select the Virtual Center Data Center with the ESXi hosts to be provisioned with GigaVUE-VM nodes.
  - c. The list shows all data centers available on the Virtual Center Server specified on the **Virtual Centers** page. After selecting the data center the **Cluster** field appears.
  - d. From the **Cluster** drop-down list, select the cluster to upgrade.
  - e. In the **Enter Password** column, provide the existing node password for the GigaVUE-VM upgrade.
  - f. The Enter Password and Confirm Password columns are optional. Entering and confirming a password is only required if you want to change the password on the upgraded GigaVUE-VM.
  - g. Select the hosts where you want to upgrade GigaVUE-VM nodes. Click **Upgrade** to continue.
7. Click **Upgrade**.

## Backup and Restore GigaVUE-FM for VMware

To backup and restore GigaVUE-FM in a VMware environment, do the following:

1. Log in to GigaVUE-FM and make a backup of GigaVUE-FM.

For the steps to backup GigaVUE-FM, refer to the *“Data Saved When Backing Up GigaVUE-FM”* section in the *GigaVUE Administration Guide*.
2. Shut down the virtual machine.
3. Log in to the new GigaVUE-FM instance and restore the configuration.

For the steps to restore GigaVUE-FM, refer to the *“Restoring GigaVUE-FM Configuration Files”* in the *GigaVUE Administration Guide*.
4. Log in to vCenter and reboot the GigaVUE-FM instance. (In vCenter, select **Power > Power Off/Power On.**)
5. Reboot the GigaVUE Cloud Suite-VMs.
6. After GigaVUE-FM is up and running, redeploy the virtual maps from the Virtual Maps page.

For more information about vMaps in the VMware environment, refer to [Configure Virtual Maps for VMware vCenter](#).

**NOTE:** After restore, the licenses will no longer be valid for the new GigaVUE-FM.

## Events

The Events page displays all the events that occur in the GigaVUE-VM virtual traffic visibility node. An event is an incident that occur at a specific point in time. Examples of events include:

- Authentication failure

- G-vTAP Controller VM Installation status
- Port link status changed

Refer to the “Events” section in the *GigaVUE Administration Guide*.

To view the events:

1. Navigate to **Dashboard > SYSTEM > Events** to view the Events page.

## Events

Export ▾

Filter

Manage

Events: 10000 | Filter: none

Source	Time	Scope	Event ...	Severity	Affect...	Affect...	Devic...	Host ...	Tags	
FM	2021-...	FM	EmailF...	Info	FM Sy...					
FM	2021-...	FM	EmailF...	Info	FM Sy...					
FM	2021-...	FM	EmailF...	Info	FM Sy...					

For information about the parameters for each event, refer to the “Events” sections in the *GigaVUE Administration Guide*:

**NOTE:** The events can be purged or archived only from the Events page. For more information, refer to the “Archiving or Purging Event Records” section in the *GigaVUE Administration Guide*.

## Alarms

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. Examples of alarms include:

- GigaSMART CPU Utilization
- Power failure
- Unexpected shutdown of a module

The alarms broadly fall into the following categories: Critical, Major, Minor, or info.

Refer to the “Alarms” section in the *GigaVUE Administration Guide* for details.

## Audit Logs

With Audit Logs, changes and activities that occurred in the GigaVUE-VM virtual traffic visibility node due to user actions can be easily tracked for auditing. There are 10 results shown by default on every page. The logs can also be further filtered to view specific information.

For information about the parameters in the audit log page, refer to the “*Overview of Audit Logs*” section in the *GigaVUE Administration Guide*. Filtering the audit logs allows you to display specific type of logs. For more information, refer to the “*Filtering Audit Logs*” section in the *GigaVUE Administration Guide*.

### All Audit Logs

Filter Manage

Filter : none

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS		
2020-1...	admin	logout fmUser a...	User	fm			SUCCESS		
2020-1...	admin	login fmUser ad...	User	fm			SUCCESS		
2020-1...	admin	update configuration	Configuration	fm			SUCCESS		

Go to page: 1 of 16 Total Records: 106

# Configure GigaVUE-VM on NSX-V

GigaVUE-FM integrates with VMware NSX-V as a partner service, using NSX-V Service Insertion. Service Insertion allows partner services such as Gigamon Traffic Visibility to integrate with NSX-V. When the NSX-V Manager is registered in GigaVUE-FM, a Gigamon Traffic Visibility Service is registered with NSX-V. The Traffic Visibility Service is then installed on the NSX-V compute clusters through the vCenter UI. Installing the Gigamon Traffic Visibility Service deploys the GigaVUE-VM Service VMs to each host in the cluster. Security policies are then created that will make a copy of the network traffic and forward it to the Gigamon Traffic Visibility Service.

The chapter includes the following major sections:

- [Prerequisites for Integrating GigaVUE-VM with NSX-V](#)
- [Integrate GigaVUE-VM with NSX-V](#)
- [Upgrade GigaVUE-VM on NSX-V](#)
- [Remove Gigamon Service from NSX-V and GigaVUE-FM](#)

This chapter also describes the following steps for integrating GigaVUE-FM and VMware NSX-V:

- [Step 1: Create Users in VMware vCenter and GigaVUE-FM](#)
- [Step 2: Register NSX-V vCenter in GigaVUE-FM](#)
- [Step 3: Upload the GVM OVA Image](#)
- [Step 4: Register NSX-V Manager in GigaVUE-FM](#)
- [Step 5: Install Gigamon Traffic Visibility Service on vCenter Clusters](#)
- [Step 6: Configure GigaVUE-FM Tunnels and Virtual Maps](#)
- [Step 7: Create NSX-V Security Group and Security Policy](#)

**NOTE:** These steps assume that is installed and configured.

To upgrade GigaVUE-VM nodes on VMware NSX-V, refer to [Upgrade GigaVUE-VM on NSX-V](#).

## Prerequisites for Integrating GigaVUE-VM with NSX-V

The following are the prerequisites for integrating GigaVUE-VM with NSX-V:

- For VMware ESXi and NSX-V Hardware Requirements, refer to [VMware ESXi System Requirements](#).
- GigaVUE-FM 3.4 or later.
- GigaVUE Cloud Suite 4.5 or later node with GigaSMART to support tunnel configuration.
- VMware tools or open VM tools must be installed in VMs to tap the traffic.
- Shared storage is must to deploy GigaVUE-VM.

**NOTE:** To upgrade to NSX-V 6.2.4, you must perform a full NSX-V upgrade including host cluster upgrade (which upgrades the host VIBs to 6.2.4). For more information, refer to the NSX-V for vSphere 6.2.4 Release Notes.

## Integrate GigaVUE-VM with NSX-V

To integrate GigaVUE-VM with NSX-T, perform the following steps:

- [Step 1: Create Users in VMware vCenter and GigaVUE-FM](#)
- [Step 2: Register NSX-V vCenter in GigaVUE-FM](#)
- [Step 3: Upload the GVM OVA Image](#)
- [Step 4: Register NSX-V Manager in GigaVUE-FM](#)
- [Step 5: Install Gigamon Traffic Visibility Service on vCenter Clusters](#)
- [Step 6: Configure GigaVUE-FM Tunnels and Virtual Maps](#)
- [Step 7: Create NSX-V Security Group and Security Policy](#)

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

For VMware NSX-V and GigaVUE-FM to communicate, a GigaVUE-FM user must be created in VMware and an NSX-V user must be created in Gigamon-FM. Also, a GigaVUE-FM user must be created in VMware vCenter for GigaVUE-FM to perform vCenter inventory functions. For VMware NSX-V and GigaVUE Cloud Suite FM to communicate, users with the proper permissions must be created in both GigaVUE-FM and VMware NSX-V.

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

This section provides the steps for creating an GigaVUE-FM user in vCenter and creating an NSX-V callback user in GigaVUE-FM.

#### Create GigaVUE-FM User in NSX-V vCenter

For GigaVUE-FM to communicate with VMware NSX-V, you must first create a user with an NSX-V Administrator role in vCenter. This user will be the GigaVUE-FM user that VMware NSX-V uses to communicate with GigaVUE-FM.

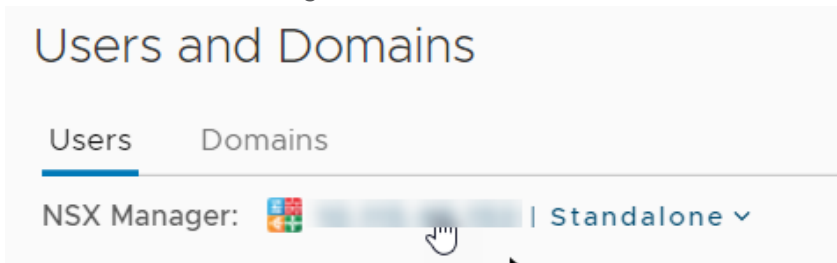
To add an NSX-V Administrator role for a user, do the following:

1. Create a user in vCenter using the standard procedure for creating vCenter users.
2. To add the NSX-V Administrator role to the user from the vCenter Web Client, do the following:

- a. Select **Networking and Security**.



- b. Select **System > Users and Domains**.
- c. Select an NSX-V Manager under Users.



- d. Select **Add**.
- e. Specify the user created in step 1, for example, `fm@vsphere.local`, and then click **Next**.
- f. Select the **NSX Administrator** role.
- g. Click **Finish**.

## Create VMware NSX-V user in GigaVUE-FM

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

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

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

Create User
✕

---

<b>Name</b>	Name
<b>Username</b>	Username
<b>Email</b>	Email
<b>Password</b>	Password <span style="float: right; color: #0070c0; font-size: 1.2em;">?</span>
<b>Confirm Password</b>	Confirm Password

Cancel
Save

- On the **Create User** page, specify the following for the new user:
  - In the **Name** field, enter the name of the call back user. For example, you can use NSX-V Manger Callback as the user name to help you associate this user with the NSX-V Manger.
  - In the **Username** field, enter a username for the user. For example, you can use NSX-V to help you remember that this user is associated with NSX-V.
  - 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, re-enter the password.

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

- Click **Save**.

## Step 2: Register NSX-V vCenter in GigaVUE-FM

There is a one-to-one mapping between vCenters and NSX-V Managers. Both the vCenter registered with the NSX-V Manager and the NSX-V Manager must be added to GigaVUE-FM.

When the NSX-V Manager is registered in GigaVUE-FM, it registers the Gigamon Traffic Visibility Service in NSX-V as a Network Introspection Service. The Gigamon Traffic Visibility Service is used to install GigaVUE-VM Service Virtual Machines and define profiles for forwarding traffic to the GigaVUE Cloud Suite visibility fabric.

To add the vCenter to GigaVUE-FM, do the following:

- From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The Management page appears.

- In the **Virtual Center** tab, click **Add**. The Add Virtual Center page displays.

## Add Virtual Center

Save

Cancel

<b>Virtual Center</b>	IP address/DNS
<b>Username</b>	username
<b>Password</b>	password

- On the Add Virtual Center page, do the following:
  - In the **Virtual Center** field, Enter the DNS name or IP address of the vCenter server.
  - In the **Username** field, enter the VMware vCenter username that has a minimum of the Read Only role or higher.
  - In the **Password** field, enter the password for vCenter.
- Click **Save**.

### Step 3: Upload the GVM OVA Image

The GVM OVA image must be uploaded to the Fabric Manager™ so that NSX-V can install the GVM when the Gigamon Traffic Visibility Service is installed on vCenter Clusters.

To upload the GVM OVA image, do the following in GigaVUE-FM:

- From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-V > Management**. The Management page appears.
- In the Management page, select **Image Upload** tab.
- Select the **I accept the End User License Agreement ("EULA")** check box.

Management    NSX Managers    Image Upload    Tunnels Library

Save    Cancel

End User License Agreement

**Gigamon Terms and Conditions**

PLEASE READ CAREFULLY: THE INDIVIDUAL ASSENTING TO THESE TERMS AND CONDITIONS ON BEHALF OF A CUSTOMER REPRESENTS AND WARRANTS THAT HE OR SHE HAS FULL AUTHORITY TO BIND THE CUSTOMER TO THESE TERMS AND CONDITIONS (THE AGREEMENT). THIS AGREEMENT GOVERNS CUSTOMER'S RIGHT TO ACTIVATE A SOFTWARE LICENSE, AND/OR DOWNLOAD, INSTALL AND USE THE GIGAMON PRODUCTS. BY ASSENTING TO THIS AGREEMENT (EITHER BY CLICKING ACCEPT, CHECKING A BOX, SUBMITTING A PURCHASE ORDER, OR DOWNLOADING, INSTALLING, ACCESSING OR USING A GIGAMON PRODUCT), THE CUSTOMER ASSENTS TO THIS AGREEMENT, WHICH WILL BE DEEMED A BINDING CONTRACT BETWEEN CUSTOMER AND GIGAMON INC. WITH A PRINCIPAL PLACE OF BUSINESS AT 3300 OLCOTT ST., SANTA CLARA, CA 95054 (GIGAMON). UNLESS CUSTOMER HAS ANOTHER VALID CONTRACT FOR THE PURCHASE AND USE OF GIGAMON'S PRODUCTS AND SERVICES. IF THE CUSTOMER DOES NOT AGREE TO OR CANNOT COMPLY WITH THIS AGREEMENT OR IF THE INDIVIDUAL DOES NOT HAVE AUTHORITY TO BIND THE CUSTOMER, THEN DO NOT ASSENT (AS DESCRIBED ABOVE) AND THE CUSTOMER WILL NOT BE AUTHORIZED TO DOWNLOAD, INSTALL OR USE THE PRODUCTS.

These Gigamon Terms and Conditions (the "Agreement") are a master agreement that covers all Gigamon products, but provisions regarding specific products apply only to the extent the Customer has purchased or used such products.

I accept the End User License Agreement ("EULA").

OVA File

Hosts Properties

- Click the **OVA File** link. Browse an OVA file and Upload to Server.
- Click **Browse**, navigate to the GVM OVA file, and click **Open**.



6. Click **Upload to Server**.
7. Click the **Hosts Properties** link.
8. In the **Password** field, enter the password you would like to set for the GVM administrator account.
9. In the **Confirm Password** field, reenter the same password.
10. Click **Save**.

## Step 4: Register NSX-V Manager in GigaVUE-FM

To register the NSX-V Manger with VMware vCenter, do the following:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-V > Management**. The Management page appears.
2. In the **NSX Managers** tab, click **Add**. The Add NSX Manager page displays.

3. Enter the information in the fields as follows:
  - o In the **NSX-V Manager** field, enter the hostname or IP address of the NSX-V Manager.
  - o In the **NSX-V Username** field, enter the user that FM uses to authenticate with NSX-V. This is the user created during the steps described in [Create GigaVUE-FM User in NSX-V vCenter](#).
  - o In the **NSX-V Password** field, enter the password for the NSX-V user.
  - o In the **FM User** field, enter in the user in GigaVUE-FM for NSX-V to communicate back with FM. This the user created in [Create VMware NSX-V user in GigaVUE-FM](#)
  - o In the **FM Password**, enter a password for the GigaVUE-FM user.
  - o In the **Connected vCenter** field, select the connected vCenter IP.
4. Click **Save**.

## Step 5: Install Gigamon Traffic Visibility Service on vCenter Clusters

The Gigamon Traffic Visibility service must be installed on each of the clusters in the NSX-V environment. Installing the Gigamon Traffic Visibility service installs the GigaVUE-VM Service VM on each of the hosts in the cluster. This Gigamon Traffic Visibility service installation should be performed by the Cloud Administrator.

To install the Traffic Visibility Service, do the following in vSphere:

1. In vSphere, select **Network & Security > Installation and Upgrade**.

2. Select the Service Deployments tab.
3. Click the **Add** button for New Service deployment.
4. On the Deploy Network & Security Services page, select the **Gigamon Traffic Visibility service**.
5. Click **Next**.
6. Select the clusters to install the Gigamon Traffic Visibility service. All the compute clusters where VMs to be monitored should be selected.
7. Select the shared Datastore. The datastore selected must be accessible by every host in the cluster for the install to succeed.
8. Select the Network. This network port group will be used for both the management and tunnel interfaces.
9. Select DHCP for the IP Assignment.  
DHCP and Static are currently supported for the management interface. For tunnels, it is only DHCP.
10. Click **Next**, and then **Finish**.

After you click the Finish, the installation will start. Once the installation is completed, if 'Installation Status' shows 'Succeeded', but the 'Service Status' shows 'Unknown', check to see if the 'Gigamon Traffic Visibility' service VMs received the IP addresses.

## Step 6: Configure GigaVUE-FM Tunnels and Virtual Maps

NSX-V traffic needs to be sent to the H-Series device. A tunnel must be created in the Tunnels Library that defines the destination port to which the traffic is sent.

Virtual maps are also needed to monitor NSX-V traffic. A separate map needs to be created for each separate GigaSMART tunnel destination to send NSX-V traffic, or if specific map rules or slicing is required. If the same parameters will be applied for all NSX-V traffic, only one map is needed to handle all NSX-V traffic. Creating a map creates a corresponding profile in NSX-V that will be used to associate the NSX-V traffic with the virtual map during security policy creation.

### Create Tunnel to GigaSMART Device

To create a tunnel, do the following in GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-V > Management**. The Management page appears.
2. In the **Tunnel Library** tab, click **Add** to open the Add Tunnel Endpoint page.

When the page opens, GigaVUE-FM should discover and display the GigaVUE Cloud Suite tunnels if the H-series device is a physical node. If the tunnel is displayed, do the following:

- a. Select the tunnel that is configured to receive traffic from NSX-V.

- b. Enter the Tunnel Source Port. This value will be used on the H-Series GigaSMART device to specify the source port from which the mirrored traffic is originating. The port range is from 0 to 65535.
- c. Click **OK**.

If the desired GigaVUE Cloud Suite tunnel was not discovered, the tunnel was not configured properly on the H Series device. For information on how to configure the tunnel, refer to [Configure Tunnel Endpoint](#).

## Create Virtual Maps

To create the virtual maps, do the following in GigaVUE-FM:

1. From the left navigation pane, select **Traffic > VIRTUAL > Virtual Maps > NSX-V**. The NSX Virtual Maps page appears.
2. On the **NSX Virtual Maps** page, click **New**. The NSX-V Virtual Map wizard appears.

The screenshot shows the 'NSX Virtual Map' configuration wizard. It has a title bar with 'NSX Virtual Map' and 'Save' and 'Cancel' buttons. Below the title bar is a section titled 'VM Map Info' with a dropdown arrow. This section contains four fields: 'Alias' with a text input field, 'Description' with a text input field, 'Tunnel Destination' with a dropdown menu, and 'vCenter' with a dropdown menu. Below this section is another section titled 'Map Rules' with a dropdown arrow. At the bottom of the 'Map Rules' section is a button labeled 'Add a Rule'.

3. On the NSX Virtual Map wizard, do the following:
  - a. For **Alias**, enter an alias that will help you identify this map.
  - b. For **Tunnel Destination**, click in the field and select the GigaSMART tunnel destination to which NSX-V traffic will be sent.
  - c. For **Virtual Center**, select the VMware vCenter registered with the NSX-V Manager to be monitored.
  - d. (Optional) Click **Add a Rule** if you need slicing or filtering beyond what the NSX-V security filtering policy provides.
  - e. Click **Save**.

The GigaVUE-FM virtual maps will be distributed to every GigaVUE-VM installed in the NSX-V clusters. An NSX-V Profile will also be created for the map.

## Step 7: Create NSX-V Security Group and Security Policy

An NSX-V security group and security policy must be created to redirect network traffic to the Gigamon Traffic Visibility service. A security group defines which VMs will be monitored. The security policy associates the Gigamon Traffic Visibility service and map profile to the security group. The cloud tenant user should create the security group and security policy.

### Create Security Group

A security group should be created that contains the VMs to forward NSX-V network traffic to the Gigamon Traffic Visibility service.

To create the security group, do the following in the vCenter UI:

1. In vCenter, select **Networking & Security > Service Composer > Security Groups > + Add**.
2. Enter the Name and description.
3. Click **Next**.
4. Click **Select Objects** to include.
5. For the Object Type, select an Object Type from the drop-down list.
6. Move the desired Objects from the Available Objects column to the Selected Objects Column.
7. Click **Finish**.

The monitored Objects can also be selected using dynamic membership or any of the available object types.

For additional details on creating security groups, Refer to the “Service Composer” chapter of the *NSX-V Administration Guide*.

### Create Security Policy

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

To create the security policy, do the following in the vCenter UI:

1. In vCenter, select **Networking & Security > Service Composer**.
2. Select the **Security Policies** tab, and then click **+ Add**. Before you proceed to the next step, make sure that you specify the Guest Introspection and Firewall Rules.

3. On the new Security Policy page, do the following.
  - a. In the Name and Description fields, enter name and description for the security policy, respectively.
  - b. Click **Network Introspection Services** to select the Network Introspection Services tab.
  - c. Click **+ Add Network Introspection Service**.
  - d. In the Name and Description fields, enter a name and description.
  - e. For Action, select **Redirect to service**.
  - f. For Service Name, select **Gigamon Traffic Visibility**.
  - g. For Profile, select the profile corresponding to the desired virtual map. A profile is created for each virtual map.
  - h. Based on the required traffic type, select the Source and Destination as described in the following table.

Traffic	Source	Destination
Incoming	Any	Policy's Security Groups
Outgoing	Policy's Security Groups	Any

- i. For Service, If filtering based on ports is desired, click Change to select the service to filter on. A service defines tcp/udp ports to filter.
  - j. For State, select **Enabled**.
  - k. For Log, select **Do not log**.
  - l. Click **OK**.
4. On the New Security Policy page, click **Finish**.

## Map Security Policy to Security Group

The security policy is mapped to a security group by applying the security policy to one or more security groups. The steps presented in this section configure the Visibility Fabric to allow monitored traffic to flow to the H-Series chassis with GigaSMART. Monitored traffic can be observed using a tool that is connected to a tool port of the H-Series device.

To map the security policy to the security group, do the following in the vCenter UI:

1. In vCenter, select **Networking & Security > Service Composer**.
2. Select the **Security Policies** tab.
3. Select a Security Policy and click **Apply**.
4. Select the security groups to apply the security policy.
5. Click **OK**.

## Upgrade GigaVUE-VM on NSX-V

To upgrade the GigaVUE-VM Nodes on NSX-V, do the following:

- [Upload OVA file](#)
- [Upgrade Gigamon Traffic Visibility in the VMware vCenter](#)
- [View Upgraded GigaVUE-VM Nodes](#)

### Upload OVA file

To upload the OVA file:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-V > Management**. The Management page appears.
2. In the Management page, select **Image Upload** tab.

Management    NSX Managers    Image Upload    Tunnels Library

Save    Cancel

✓ End User License Agreement

Gigamon Terms and Conditions

PLEASE READ CAREFULLY: THE INDIVIDUAL ASSENTING TO THESE TERMS AND CONDITIONS ON BEHALF OF A CUSTOMER REPRESENTS AND WARRANTS THAT HE OR SHE HAS FULL AUTHORITY TO BIND THE CUSTOMER TO THESE TERMS AND CONDITIONS (THE AGREEMENT). THIS AGREEMENT GOVERNS CUSTOMER'S RIGHT TO ACTIVATE A SOFTWARE LICENSE, AND/OR DOWNLOAD, INSTALL AND USE THE GIGAMON PRODUCTS. BY ASSENTING TO THIS AGREEMENT (EITHER BY CLICKING ACCEPT, CHECKING A BOX, SUBMITTING A PURCHASE ORDER, OR DOWNLOADING (GIGAMON), ACCESSING OR USING A GIGAMON PRODUCT), THE CUSTOMER ASSENTS TO THIS AGREEMENT, WHICH WILL BE DEEMED A BINDING CONTRACT BETWEEN CUSTOMER AND GIGAMON INC. WITH A PRINCIPAL PLACE OF BUSINESS AT 3300 OLCOTT ST., SANTA CLARA, CA 95054 (GIGAMON), UNLESS CUSTOMER HAS ANOTHER VALID CONTRACT FOR THE PURCHASE AND USE OF GIGAMON'S PRODUCTS AND SERVICES. IF THE CUSTOMER DOES NOT AGREE TO OR CANNOT COMPLY WITH THIS AGREEMENT OR IF THE INDIVIDUAL DOES NOT HAVE AUTHORITY TO BIND THE CUSTOMER, THEN DO NOT ASSENT (AS DESCRIBED ABOVE) AND THE CUSTOMER WILL NOT BE AUTHORIZED TO DOWNLOAD, INSTALL OR USE THE PRODUCTS.

These Gigamon Terms and Conditions (the "Agreement") are a master agreement that covers all Gigamon products, but provisions regarding specific products apply only to the extent the Customer has purchased or used such products.

I accept the End User License Agreement ("EULA").

OVA File

Hosts Properties

3. Under End User License Agreement, select the **I accept the End User License Agreement ("EULA")** check box.
4. Click the OVA File link and click **Browse**. Navigate to the GVM OVA file, and click **Open**.
5. Once the upload is complete, a confirmation message is displayed.

- Click the Hosts Properties link. Enter the password in the **Password** field. Re-enter the same password in the **Confirm Password** field.

- Click **Save**.

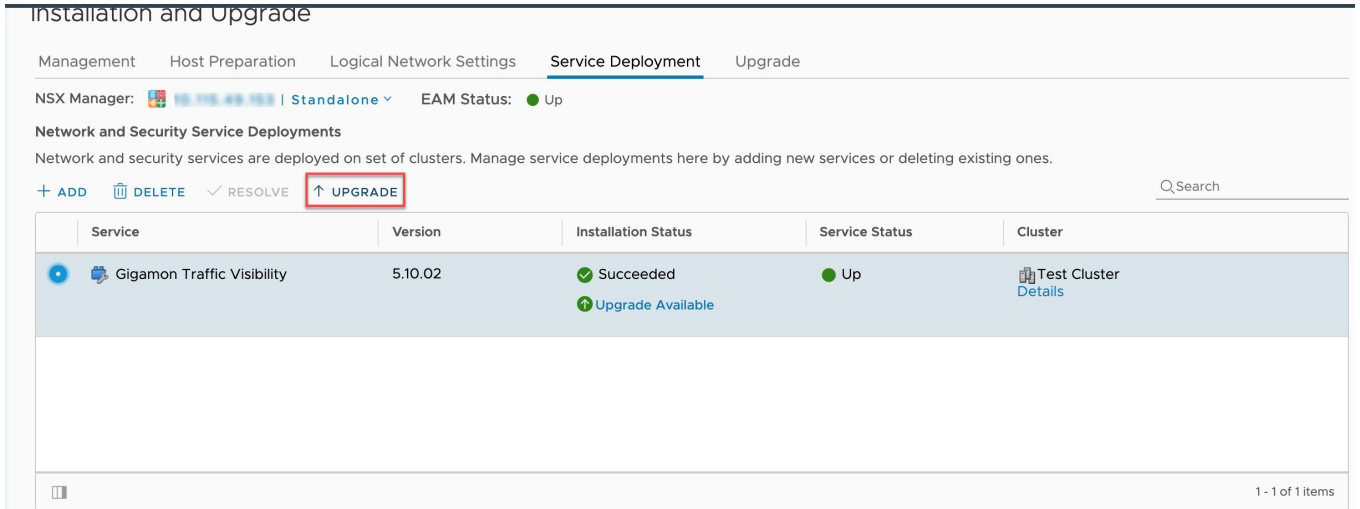
## Upgrade Gigamon Traffic Visibility in the VMware vCenter

To upgrade the Gigamon Traffic Visibility service in the VMware vCenter:

- Login to the VMware vCenter.
- Select **Networking & Security > Installation and Upgrade > Service Deployment**. The Gigamon Traffic Visibility service shows as **Upgrade Available**.

Service	Version	Installation Status	Service Status	Cluster
Gigamon Traffic Visibility	5.10.02	Succeeded Upgrade Available	Up	Test Cluster Details

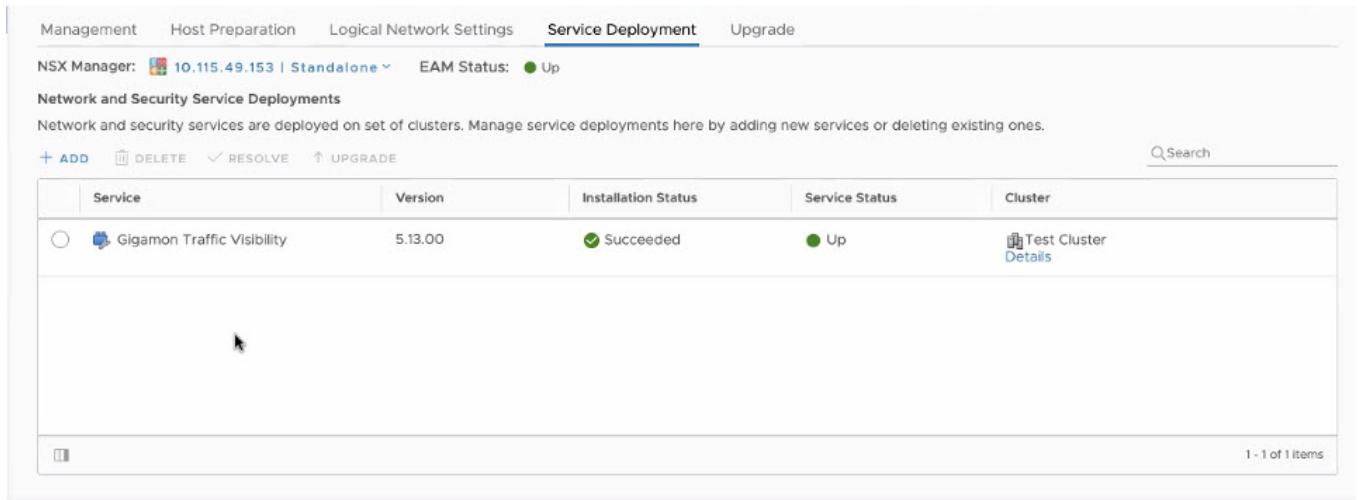
3. Select the Gigamon Traffic Visibility service and click the **Upgrade** icon.



4. To upgrade the GigaVUE Cloud Suite-VMs right away, select the **Upgrade now** radio button and click **OK**.

5. During the upgrade, the Installation Status goes through three stages:

- o Scheduled for upgrade
- o Enabling
- o Succeeded



The GigaVUE-VM upgrade is completed when the Installation Status displays the status as Succeeded and the Service Status displays the status as Up.

### View Upgraded GigaVUE-VM Nodes

To view the upgraded GigaVUE-VM Nodes:

1. Log back in to GigaVUE-FM.



- From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-V > Virtual Nodes**. The **NSX Virtual Nodes** page appears.

The GigaVUE-VM node names now show 'u' for the upgraded virtual nodes. The version displays the new upgraded version.

## Remove Gigamon Service from NSX-V and GigaVUE-FM

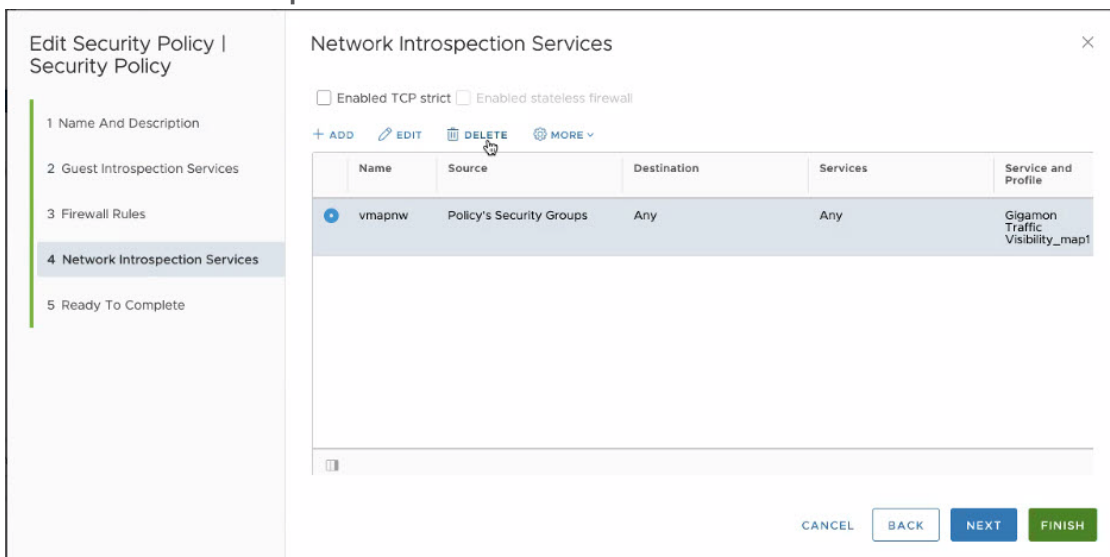
To clean up the Gigamon Visibility Platform from NSX-V and GigaVUE-FM, you must perform the following steps:

- **Step 1: Delete Network Monitoring Services**
- **Step 2: Delete NSX-V Virtual Maps from GigaVUE-FM**
- **Step 3: Delete Traffic Visibility Service from NSX-V**
- **Step 4: Delete NSX-V Manager from GigaVUE-FM**
- **Step 5: Delete Virtual Center from GigaVUE-FM**

### Step 1: Delete Network Monitoring Services

To delete the network introspection services:

- In vCenter, select **Networking and Security > Security > Service Composer**.
- Select the **Security Policies** tab.
- Select the security policy from which you wish to delete the network monitoring services.
- Click **Edit**. The Edit Security Policy page is displayed.
- Select **Network Introspection Services**.



6. Select the Network Introspection Services that you wish to remove from the security policy and click the red x (delete) icon.

## Step 2: Delete NSX-V Virtual Maps from GigaVUE-FM

To delete the NSX-V virtual maps from GigaVUE-FM:

1. From the left navigation pane, select **Traffic > VIRTUAL > Virtual Maps > NSX-V**. The NSX Virtual Maps page appears.
2. On the **NSX Virtual Maps** page, click **Delete**. The vendor template and the profile that corresponds to the map is deleted in NSX-V.

## Step 3: Delete Traffic Visibility Service from NSX-V

To delete the Traffic Visibility Service from each cluster:

1. In vSphere, select **Network and Security > Installation and Upgrade**.
2. Select the **Service Deployments** tab.
3. From the table, select the service you wish to delete and click **Delete**. The selected service is deleted from all the hosts in the cluster.

## Step 4: Delete NSX-V Manager from GigaVUE-FM

To delete the NSX-V Manager:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-V > Management**. The **Management** page appears.
2. Under NSX Managers, select the IP address of the NSX Manager that you wish to delete and click **Delete**.

## Step 5: Delete Virtual Center from GigaVUE-FM

To delete the Virtual vCenter:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The **Management** page appears.
2. Under **Virtual Centers** tab, select the IP address of the virtual center you wish to delete and click **Delete**.

# Configure GigaVUE-VM on NSX-T

GigaVUE-FM integrates with VMware NSX-T as a service definition, using NSX-T Service Insertion. Service Insertion allows service definitions such as GigaVUE Cloud Suite to integrate with NSX-T. When the NSX-T Manager is registered in GigaVUE-FM, a GigaVUE Cloud Suite is registered as a service with NSX-T. The GigaVUE-VMs can then be deployed as a Service Instances to specific clusters. Service Chains are then created that will make a copy of the network traffic and forward it to the GigaVUE-VM.

The chapter includes the following major sections:

- [Prerequisites for Integrating GigaVUE-VM with NSX-T](#)
- [Integrate GigaVUE-VM with NSX-T](#)
- [Remove Gigamon Service from NSX-T and GigaVUE-FM](#)

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

## Prerequisites for Integrating GigaVUE-VM with NSX-T

The following are the prerequisites for integrating GigaVUE-VM with NSX-T:

- For VMware ESXi and NSX-T Hardware Requirements, refer to [VMware ESXi System Requirements](#).
- GigaVUE-FM 5.8 or later.
- Shared storage is must to deploy GigaVUE-VM.
- GigaVUE-VM image (.ova) must be extracted to an **Image Host Server** so that `http://<Server_IP>/GigaVUE-VM file2.ovf` is accessible from GigaVUE-FM, NSX Manager, and vCenter.

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

## Integrate GigaVUE-VM with NSX-T

To integrate GigaVUE-VM with NSX-T, perform the following steps:

- [Step 1: Create Users in VMware vCenter and GigaVUE-FM](#)
- [Step 2: Register NSX-T vCenter and NSX-T Manager in GigaVUE-FM](#)
- [Step 3: Deploy GigaVUE-VM on vCenter Clusters](#)
- [Step 4: Configure GigaVUE-FM Tunnels and Virtual Maps](#)
- [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-T inventory functions. For NSX-T and GigaVUE Cloud Suite FM to communicate, users with the proper permissions must be created in both GigaVUE-FM and VMware NSX-T. Refer to [Privileges Required for VMware Virtual Center](#) for more information on user roles and privileges.

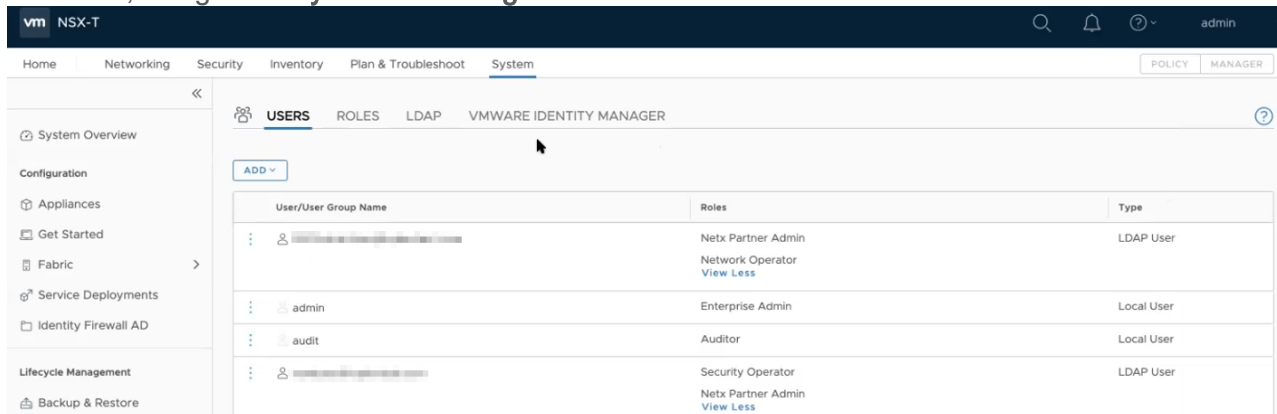
**NOTE:** GigaVUE-FM connects to NSX-T Manager that supports TLSv1.0, TLSv1.1, and TLSv1.2.

### Create GigaVUE-FM User in NSX-T manager

For GigaVUE-FM to communicate with NSX-T, you must first create a user with the minimum required role in NSX-T manager. This user will be a GigaVUE-FM user that the GigaVUE-FM uses to communicate with NSX-T Manager.

To create a user in NSX-T:

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



2. On the **USERS** tab, click **ADD** and then from the drop-down list,
  - for **NSX-T version 3.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.

Create User
✕

---

<b>Name</b>	Name	
<b>Username</b>	Username	
<b>Email</b>	Email	
<b>Password</b>	Password	<span style="color: #0070c0; font-size: 1.2em;">?</span>
<b>Confirm Password</b>	Confirm Password	

Cancel
Save

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: Register NSX-T vCenter and NSX-T Manager in GigaVUE-FM

Before adding a NSX-T Manager, you must add a vCenter to GigaVUE-FM .

When the NSX-T Manager is registered in GigaVUE-FM, it registers the GigaVUE Cloud Suite in NSX-T as a Network Monitoring Service. The GigaVUE Cloud Suite is used to install GigaVUE-VM Service Virtual Machines and define profiles for forwarding traffic to the GigaVUE Cloud Suite visibility fabric.

### Add vCenter Registered with NSX-T to GigaVUE-FM

To add the vCenter to GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The Management page appears.
2. In the **Virtual Center** tab, click **Add**. The Add Virtual Center page displays.

## Add Virtual Center

Save
Cancel

---

<b>Virtual Center</b>	IP address/DNS
<b>Username</b>	username
<b>Password</b>	password

3. On the Add Virtual Center page, do the following:
  - o In the **Virtual Center** field, Enter the DNS name or IP address of the vCenter server.
  - o In the **Username** field, enter the VMware vCenter username that has a minimum of the Read Only role or higher.
  - o In the **Password** field, enter the password for vCenter.
4. Click **Save**.

## Add a NSX-T Manager in GigaVUE-FM

To add a NSX-T Manger with VMware vCenter, do the following:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-T > Management**. The Management page appears.
2. In the **NSX-T Managers** tab, click **Add**. The **NSX-T Manager** page appears.

## NSX-T Manager

Save
Cancel

---

<b>Virtual Center</b>	Enter IP address
<b>NSX-T Manager</b>	Enter IP address or Hostname
<b>NSX-T Username</b>	Enter the NSX-T Manager username
<b>NSX-T Password</b>	Enter the NSX-T Manager password
<b>FM Username</b>	Enter the FM username
<b>FM Password</b>	Enter the FM password
<b>Image Host</b>	Enter IP address

3. Enter the information in the fields as follows:

- In the **Virtual Center** field, enter the IP address of the vCenter.
- In the **NSX-T Manager** field, enter the hostname or IP address of the NSX-T Manager.
- In the **NSX-T Username** field, enter the user that FM uses to authenticate with NSX-T. This is the user created during the steps described in [Create VMware NSX-T user in GigaVUE-FM](#).
- In the **NSX-T Password** field, enter the password for the NSX-T user.
- In the **FM Username** field, enter in the user in GigaVUE-FM for NSX-T to communicate back with FM. This the user created in [Create GigaVUE-FM User in NSX-T manager](#).
- In the **FM Password**, field enter a password for the GigaVUE-FM user.
- In the **Image Host**field, enter the IP address of the Image Host. Refer to [GigaVUE-VM image \(.ova\) must be extracted to an Image Host Server so that http://<Server\\_IP>/GigaVUE-VM file2.ovf is accessible from GigaVUE-FM, NSX Manager, and vCenter.](#) for more information.

4. Click **Save**.

**NOTE:**

- A GigaVUE-FM managing a NSX-T environment cannot be used to manage vCenter or NSX-T environment.
- You cannot connect more than one GigaVUE-FM to a NSX-T manager simultaneously.

## 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.

The screenshot shows the NSX-T Deployment page. At the top, there are tabs for 'DEPLOYMENT', 'SERVICE INSTANCES', and 'CATALOG'. Below the tabs, there is a 'Partner Service' dropdown set to 'GigaVUE Cloud Suite' and a 'VIEW SERVICE DETAILS' link. A 'DEPLOY SERVICE' button is visible. The main form area has a table with columns: Service Deployment Name, Compute Manager, Cluster, Host, Data Store, Networks, Service Segments, and Status. The 'Service Segments' column has a red box around it. Below the table, there are fields for 'Deployment Specification', 'Deployment Template', 'Deployment Type' (set to 'Clustered'), and 'Clustered Deployment Count'. At the bottom, there is a 'NOTE' and 'SAVE'/'CANCEL' buttons.

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.

Service Segment ×

**ADD SERVICE SEGMENT** Q Search

Name	Transport Zone (Overlay)	Status
<input type="text" value="Enter Name"/> *	<input type="text"/>	<input type="text"/>

**SAVE** **CANCEL**

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

### Step 3: Deploy GigaVUE-VM on vCenter Clusters

The GigaVUE-VM must be installed on each of the clusters in the NSX-T environment. Installing the GigaVUE-VM installs the GigaVUE-VM Service on each of the hosts in the cluster. This GigaVUE-VM installation must be performed by the GigaVUE-FM Administrator.

To deploy GigaVUE-VM in GigaVUE-FM:



1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-T > Management**. The Management page appears.
2. Select **GVM Deployment** tab, . The GVM Deployment page appears.

Management      NSX-T Managers      GVM Deployment      Tunnels Library

Deploy GVM

---

Virtual Center	Select Virtual Center...
Cluster	Select Cluster...
Datastore	Select Datastore...
Management Network	Select Management Network...
Service Attachment	Select Service Attachment...
Deployment Type	Clustered
Deployment Count	1

3. Enter or select the required information as follows:
  - **Virtual Center**—select the IP address of the vCenter.
  - **Cluster**—select a cluster where you want to deploy the GigaVUE-VM.
 

**NOTE:** Only Cluster-based deployment is supported in NSX-T
  - **Datastore**—select a network datastore shared among all ESXi hosts.
 

**NOTE:** You must configure at least one shared datastore across all hosts in any cluster where you want to deploy the GigaVUE Cloud Suite-VMs.
  - **Management Network**—select a Management Network. For GigaVUE-VM, VM Network is the management network.
 

**NOTE:** Only DHCP is supported on GigaVUE-VM's network
  - **Service Attachment**—select a Service Attachment (created on NSX-T before GigaVUE-FM configuration).
  - **Deployment Count**—enter number of nodes where the GigaVUE-VM is required to be deployed. Deployment count must be lesser than or equal to the number of ESX hosts.
4. Click **Deploy GVM**. Then the specified number of GigaVUE Cloud Suite-VMs are deployed in the hosts of vCenter.

To view the status of the GigaVUE-VM deployment in GigaVUE-FM:

- Navigate to **Inventory > VIRTUAL > VMware > NSX-T > Virtual Nodes**. The **Virtual Node** page appears with the deployed GigaVUE-VM.

To view the status of the GigaVUE-VM deployment in NSX-T:

1. Navigate to **System > Service Deployment > DEPLOYMENT**.
2. On the DEPLOYMENT tab, for **Partner Service**, select GigaVUE Cloud Suite and then click **VIEW SERVICE DETAILS**. A list of active service instances appears.

**NOTE:** You can view the status of the deployed GigaVUE Cloud Suite-VMs and wait for the status to be **Up**.

## Step 4: Configure GigaVUE-FM Tunnels and Virtual Maps

NSX-T traffic needs to be sent to the H-Series device. A tunnel must be created in the Tunnels Library that defines the destination port to which the traffic is to be sent.

Virtual maps are also needed to monitor NSX-T traffic. A separate map needs to be created for each separate GigaSMART tunnel destination to send NSX-T traffic, or if a specific map rule or slicing is required. If the same parameters are applied for all NSX-T traffic, only one map is required to handle all NSX-T traffic. Creating a map creates a corresponding profile in NSX-T that is used to associate the NSX-T traffic with the virtual map during service chain creation.

### Create Tunnel to GigaSMART Device

To create a tunnel in GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > NSX-T > Management**. The Management page appears.
2. In the **Tunnel Library** tab, click **Add** to open the **Add Tunnel Endpoint** page. The page displays a list of available GigaVUE Cloud Suite tunnels, if the H-series device is a physical node. If the list of tunnels is displayed, do the following:
  - a. Select the tunnel that is configured to receive traffic from NSX-T.
  - b. Enter the Tunnel Source Port. This value will be used on the H-Series GigaSMART device to specify the source port from which the mirrored traffic is originating. The port range is from 0 to 65535.

If the desired GigaVUE Cloud Suite tunnel was not discovered, the tunnel was not configured properly on the H Series device. For information on how to configure the tunnel, refer to [Configure Tunnel Endpoint](#).

3. Click **OK**. A Tunnel Endpoint is created.

To view the status of the virtual nodes, navigate to **NSX-T > Virtual Nodes**. The **NSX-T Virtual Nodes** page displays the list of GigaVUE Cloud Suite-VMs and respective details.

### Create Virtual Maps in GigaVUE-FM

To create a virtual map:

1. From the left navigation pane, select **Traffic > VIRTUAL > Virtual Maps > NSX-T**. The NSX-T Virtual Maps page appears.
2. On the **NSX-T Virtual Maps** page, click **New**. The NSX-T Virtual Map wizard appears.

The screenshot shows the 'NSX-T Virtual Map' configuration wizard. At the top, there are 'Save' and 'Cancel' buttons. The main section is titled 'VM Map Info' and contains the following fields:

- Alias:** A text input field with the placeholder text 'Alias'.
- Comments:** A text input field with the placeholder text 'Comments'.
- Tunnel Destination:** A dropdown menu with the placeholder text 'Select a tunnel destination.⌵'.
- vCenter:** A dropdown menu with the placeholder text 'Select a virtual center.⌵'.

Below the 'VM Map Info' section is a section titled 'Map Rules' which contains an 'Add a Rule' button.

3. On the NSX-T Virtual Map page, do the following:
  - a. For **Alias**, enter an alias that will help you identify this map.
  - b. For **Comments**, enter any additional comments for the Virtual Map.
  - c. For **Tunnel Destination**, click in the field and select the GigaSMART tunnel destination to which NSX-T traffic will be sent.
  - d. For **vCenter**, select the VMware vCenter registered with the NSX-T Manager to be monitored.
  - e. (Optional) Click **Add a Rule** if you need slicing or filtering beyond what the NSX-T security filtering policy provides.
  - f. Click **Save**. A Virtual Map is created and you can view the Virtual Map in the SERVICE PROFILES tab of Network Introspection (E-W) page in NSX-T.

The GigaVUE-FM virtual maps is distributed to every GigaVUE-VM installed in the NSX-T clusters and an NSX-T Profile is also created for the map.

**NOTE:** GigaVUE-FM verifies the NSX-T license while creating or updating the Virtual Map.

## Step 5: Create NSX-T Group and Service Chain

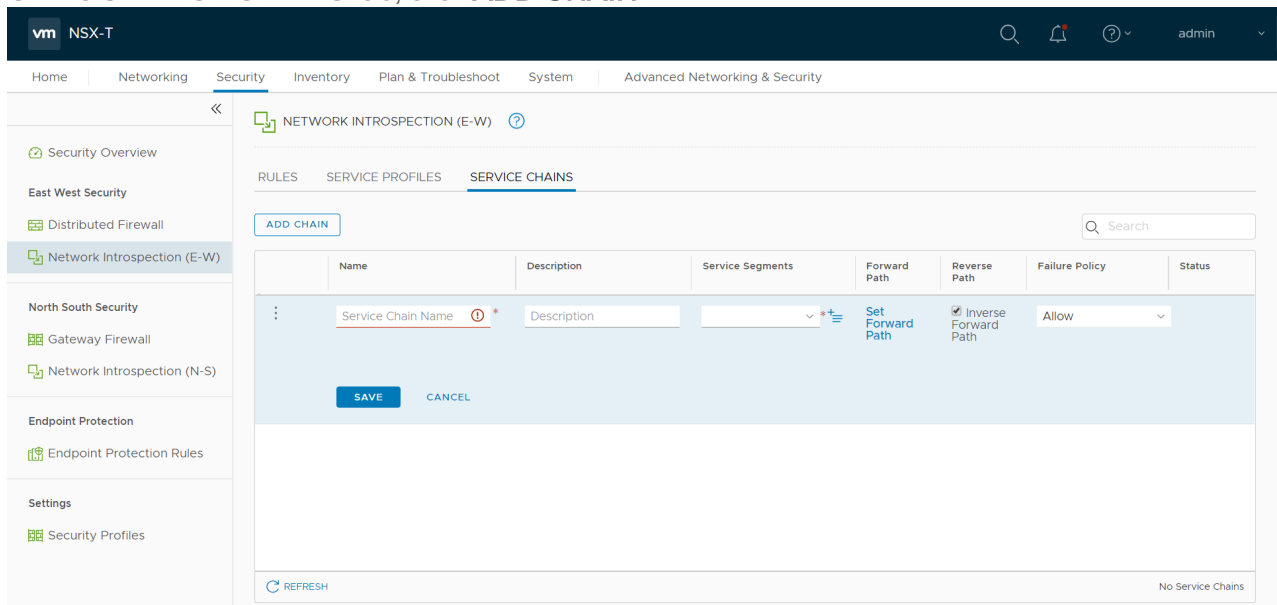
An NSX-T group and service chain must be created to redirect network traffic to the GigaVUE Cloud Suite. An NSX-T group defines which VMs will be monitored. The service chain associates the GigaVUE Cloud Suite and map profile to the group.

### 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**.

The screenshot shows the NSX-T web interface. The top navigation bar includes 'vm NSX-T' and user 'admin'. The main navigation menu has 'Home', 'Networking', 'Security', 'Inventory', 'Plan & Troubleshoot', 'System', and 'Advanced Networking & Security'. The left sidebar shows 'Inventory Overview', 'Services', 'Groups', 'Context Profiles', and 'Virtual Machines'. The main content area is titled 'Groups' and features an 'ADD GROUP' button. Below the button is a form with the following fields: 'Group Name' (with a red error icon and a 'Set Members' link), 'Description', and 'Tags' (with a 'Tag (Required)' and 'Scope (Optional)' dropdown and a '+' icon). At the bottom of the form are 'SAVE' and 'CANCEL' buttons. A 'REFRESH' button is located at the bottom left of the main content area, and 'No Groups' is displayed at the bottom right.

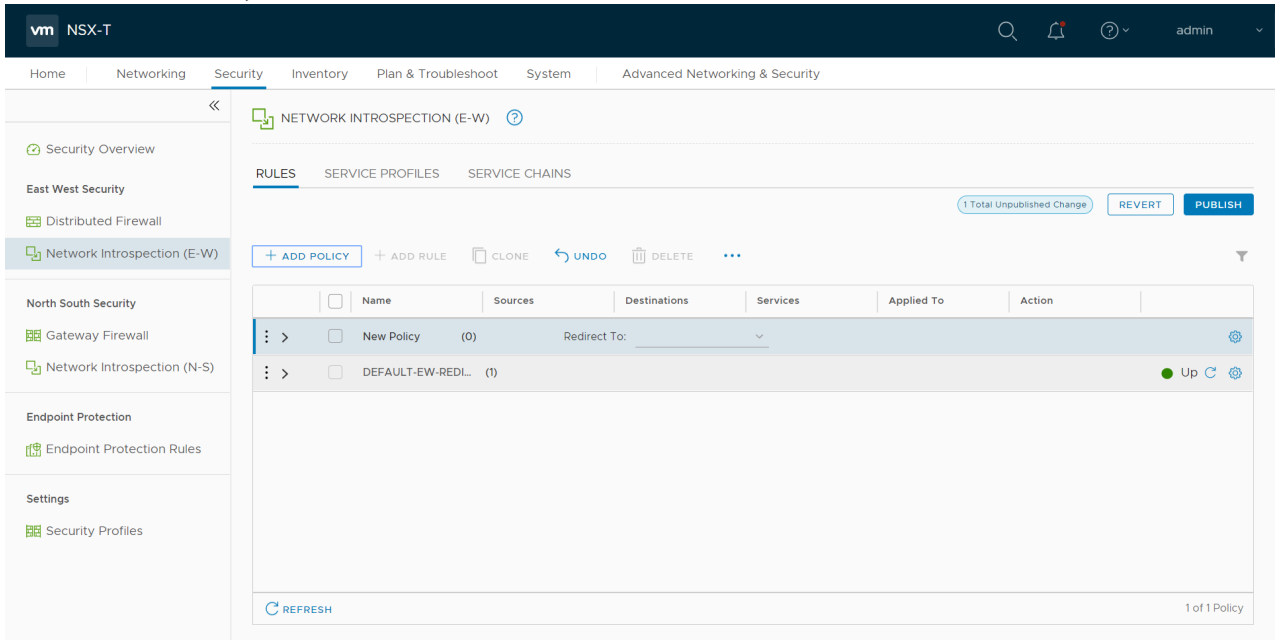
3. On the New Group, enter or select the values as follows.
  - a. Enter a name for the new group.
  - b. Click **Set Members** and the **Select Members** dialog box appears.
    - Add or select Membership Criteria, Members, IP/MAC Addresses, and AD Groups.
  - c. Enter the description for the group.
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 GigaVUE-VM 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:

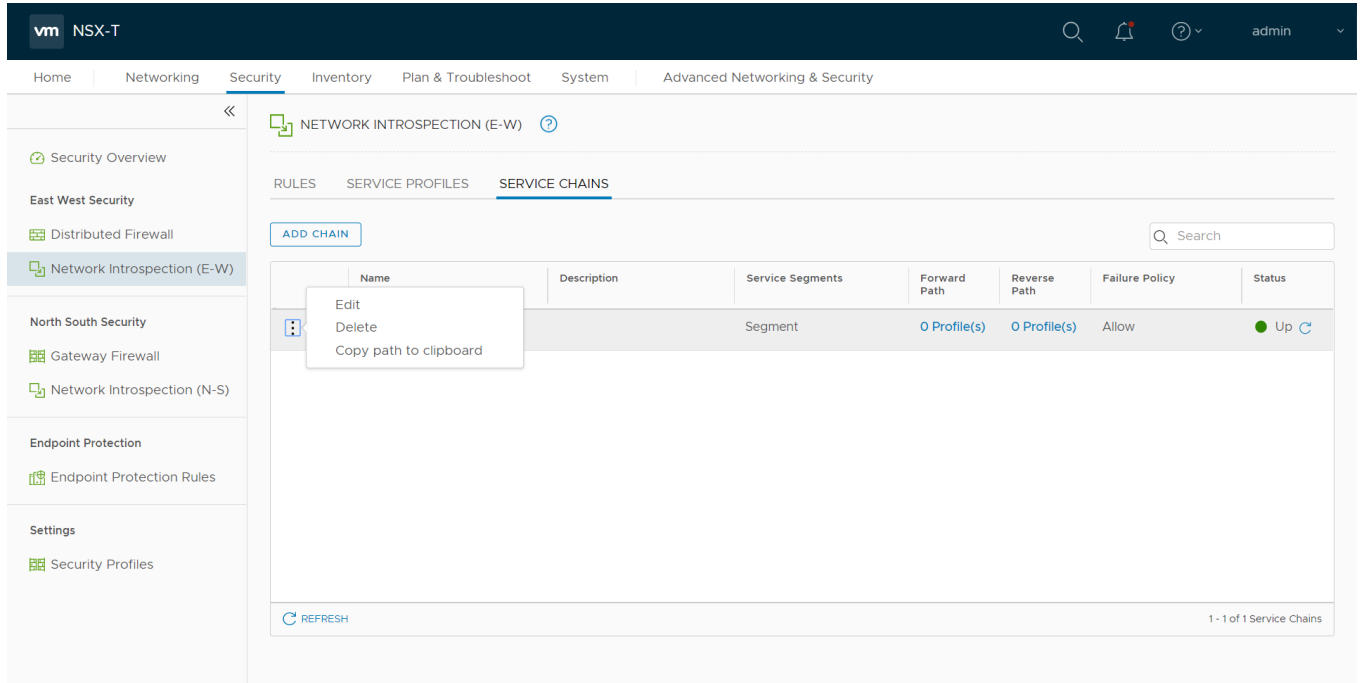
- [Step 1: Remove the Service Chains](#)
- [Step 2: Delete the vMaps](#)
- [Step 3: Undeploy GigaVUE Cloud Suite-VMs](#)
- [Step 4: Delete the NSX-T manager and vCenter connections](#)

### 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 vMaps

To delete the Virtual Maps from GigaVUE-FM:

1. From the left navigation pane, select **Traffic > VIRTUAL > Virtual Maps > NSX-T**. The NSX-T Virtual Maps page appears.
2. On the **NSX-T Virtual Maps** page, click **Delete**. The service profile and the profile that corresponds to the map is deleted in NSX-T.

## Step 3: Undeploy GigaVUE Cloud Suite-VMs

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

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Virtual Nodes**. The Virtual Nodes page appears.
2. On the **Virtual Nodes** page, select the appropriate virtual node (GigaVUE-VM) that you wish to delete and then click **Delete**.

## 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 > NSX-T > Management**. The Management page appears.
2. On the **NSX-T Managers** tab, select the appropriate NSX-T Manager that you wish to delete and then click **Delete**.

To delete the Virtual Center from GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > VMware > vCenter > Management**. The Management page appears.
2. On the **Virtual Centers** tab, select the appropriate virtual center that you wish to delete and then click **Delete**.

## GigaVUE-VM Deployment Clean up

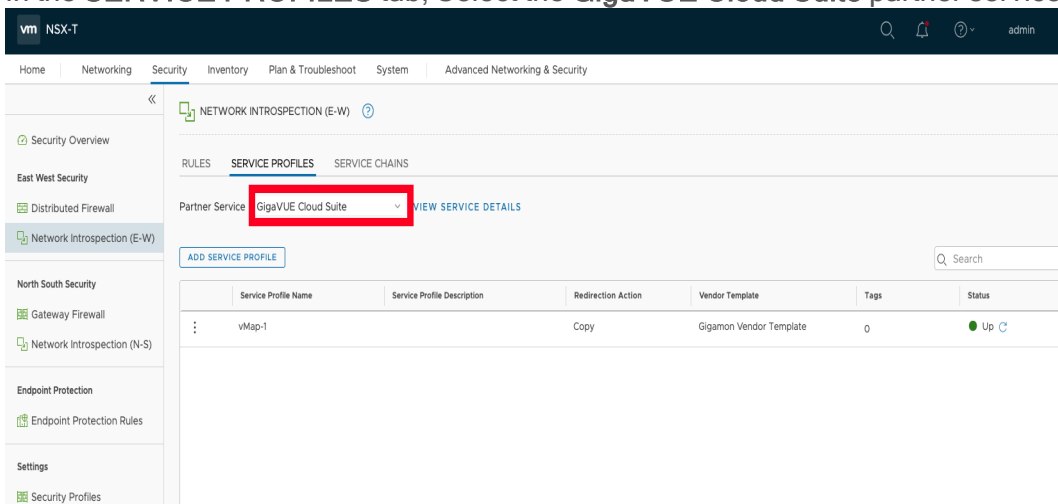
On installation failure or incomplete service removal, you must clean up GigaVUE-VM before reattempting the installation. To clean up the GigaVUE-VM deployments from NSX-T and GigaVUE-FM, perform the following steps:

- [Remove Service Profiles](#)
- [Remove Service Deployments](#)
- [Remove Service Reference](#)
- [Remove Service Manager](#)
- [Remove Vendor Template and Service Definition](#)

### Remove Service Profiles

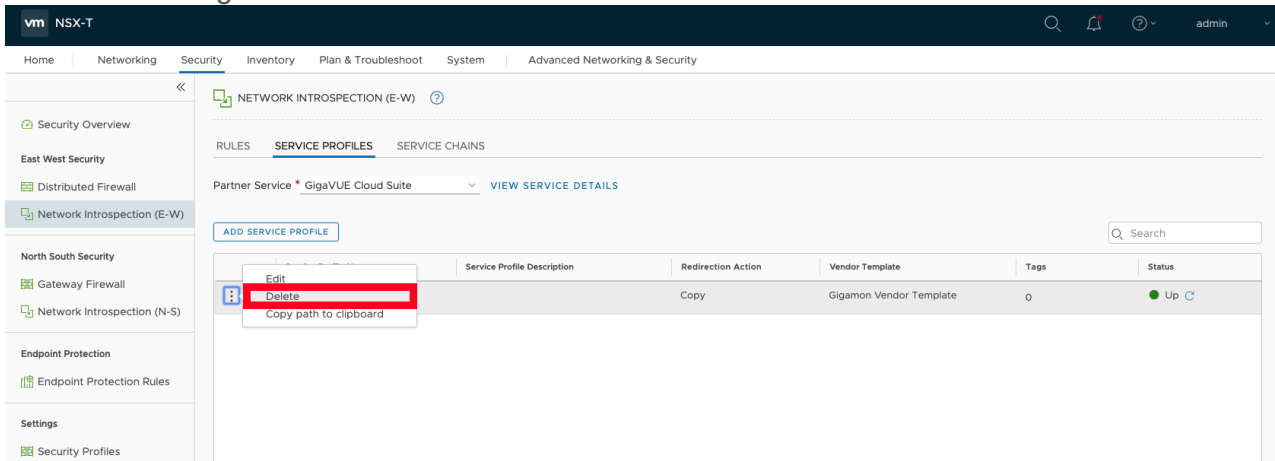
To remove Service Profiles:

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.





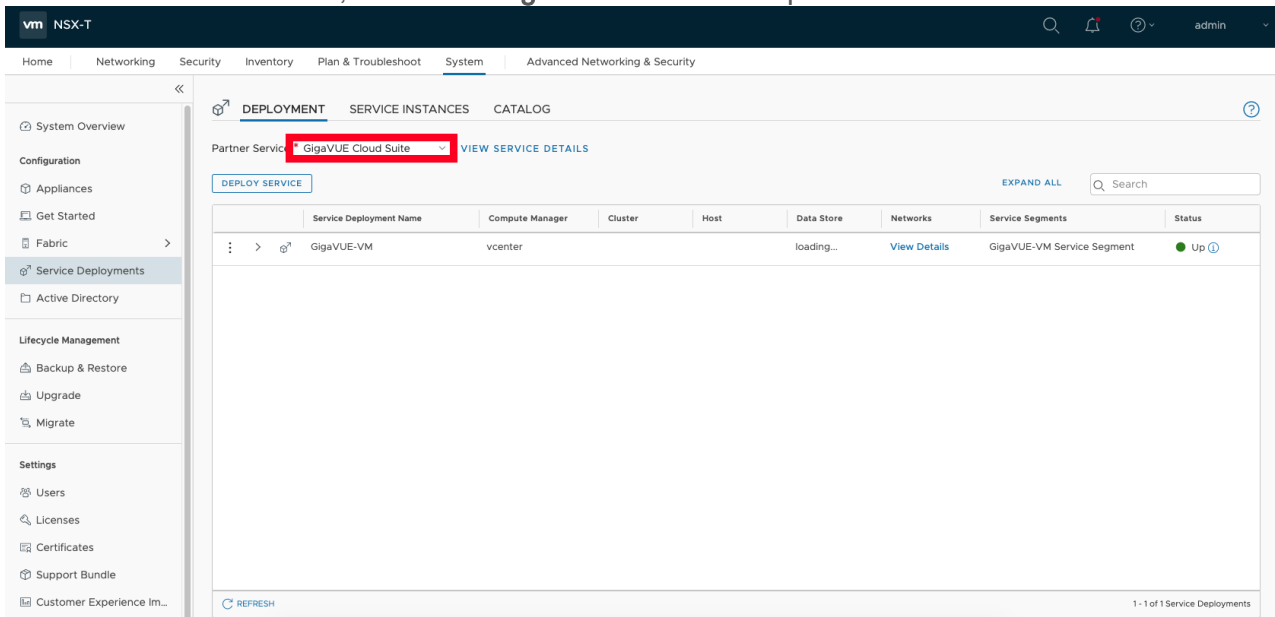
### 3. Delete all existing Service Profiles.



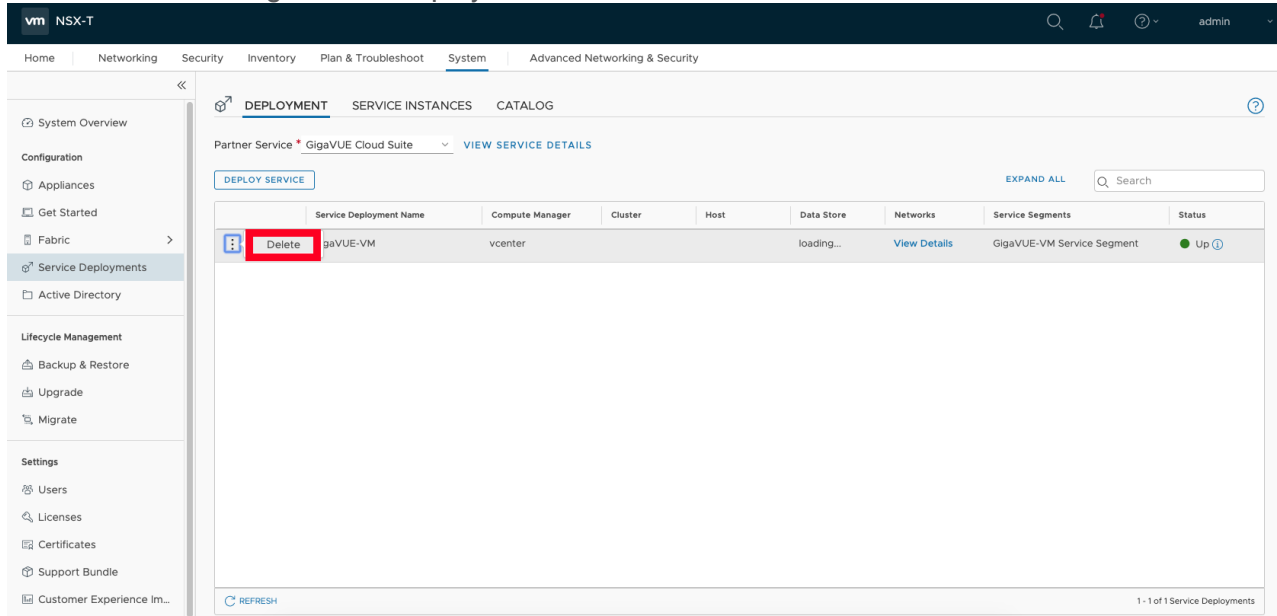
## Remove Service Deployments

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.

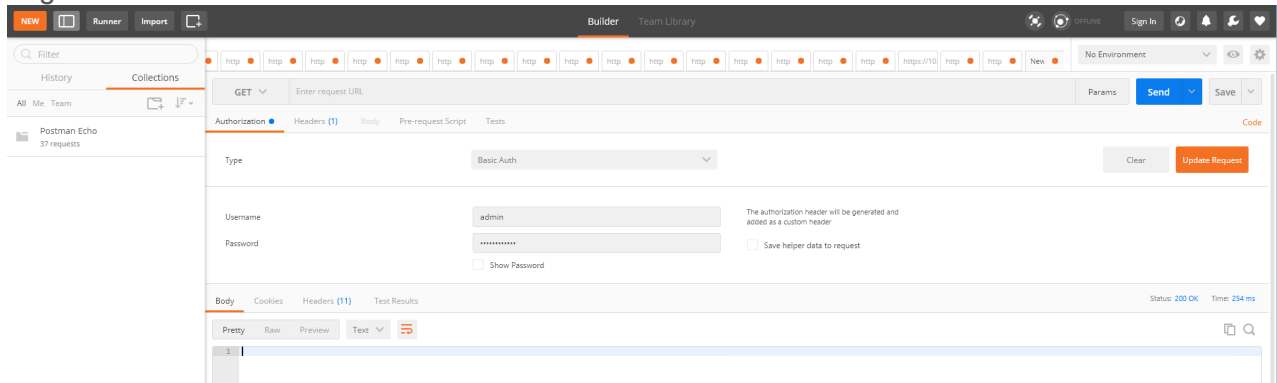


### 3. Delete all the existing Service Deployments.



To remove the Service Deployments through NSX-T API:

#### 1. Login to Postman.

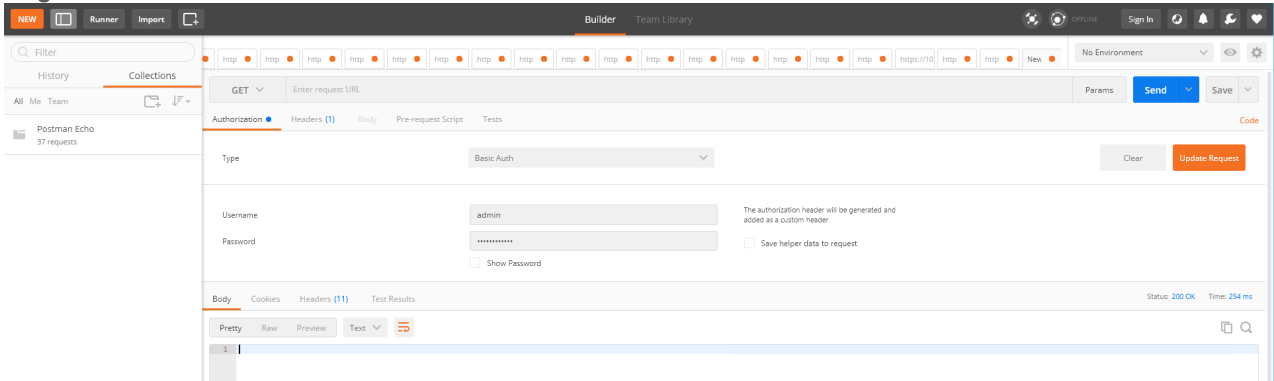


2. Get the Service ID. **GET** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/`
3. Get the Service Deployments' ID. **GET** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/`
4. Delete all Service Deployments. **DELETE** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/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

## Remove Service Reference

To remove Service References through NSX-T API:

## 1. Login to Postman.

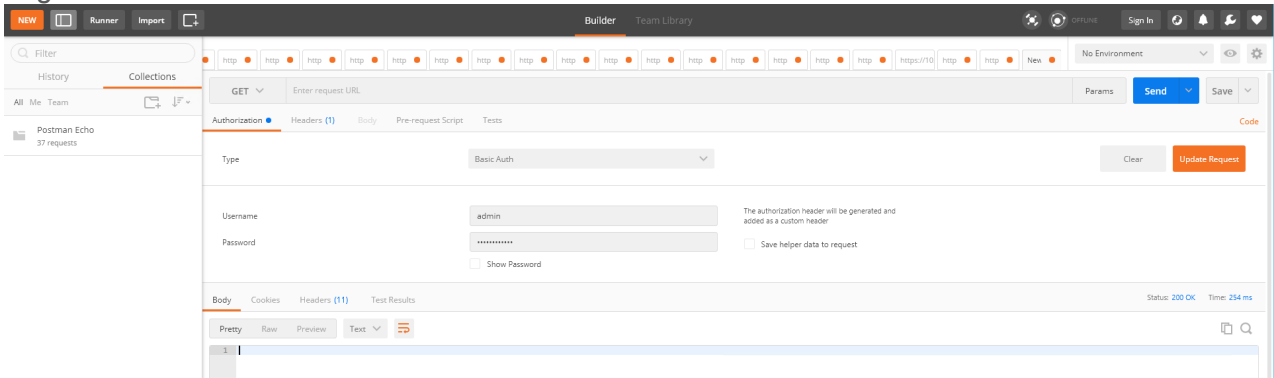


2. Get the Service Reference ID. **GET** `https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/`
3. Delete the Service Reference. **DELETE** `https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/<Service_Reference_ID>`

## Remove Service Manager

To remove Service Manager through NSX-T API:

### 1. Login to Postman.

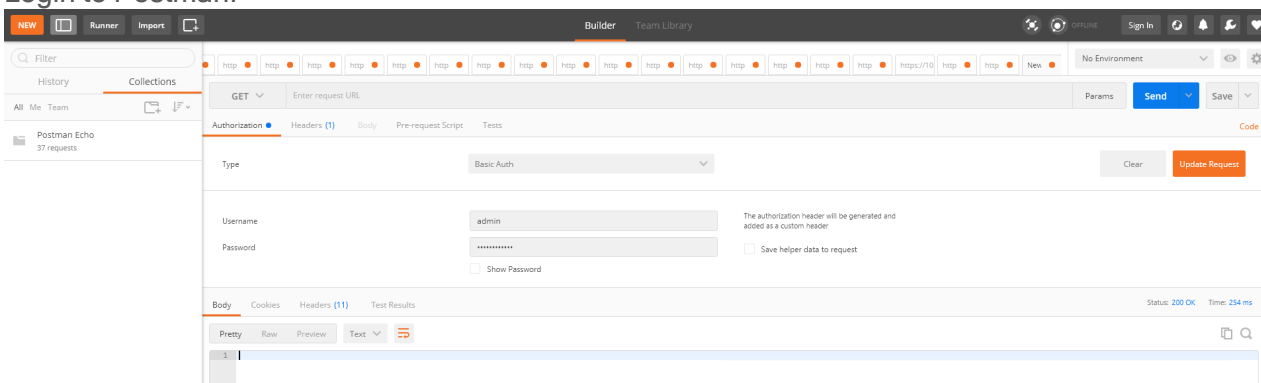


2. Get the Service Manager ID. **GET** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/service-managers/`
3. Delete the Service Manager. **DELETE** `https://<NSX_Manager_IP>/api/v1/serviceinsertion/service-managers/<Service_Manager_ID>`

## Remove Vendor Template and Service Definition

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

## 1. Login to Postman.



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

# GigaVUE-VM Reference

This section provides additional references useful for GigaVUE-VM.

The following topics are included in this section:

- [Best Practices for vSphere Integration](#)
- [Tips for vMaps](#)

## Best Practices for vSphere Integration

Gigamon recommends the following best practices to ensure smooth operations of GigaVUE-FM and GigaVUE-VM in the vSphere environment:

### How to Use Jumpstart Configuration for making changes

Always use jumpstart when there are no maps or gsops configured. Using jumpstart will clear any pre-existing configurations. Additionally, use the command write memory to save all the changes

### How to Use Out-of-Band Networks for Management Port

Gigamon recommends deploying the GigaVUE-VM node's Management port on a network that is out-of-band from that used by the IP interface or Network Ports.

### How to Use Dedicated VMNIC for IP Interface

For optimal performance, Gigamon recommends maintaining the IP interface on a dedicated VMNIC rather than sharing the same VMNIC as the Management or Network Ports.

### Configure GigaVUE-VM Nodes to Restart Automatically After Reboot

In addition to preventing GigaVUE-VM nodes operating in clusters from migrating automatically when an ESXi host reboots, you can also configure them to restart automatically when the ESXi host is back up. After making the changes listed above to prevent automatic migration, do the following to ensure the GigaVUE-VM nodes restart automatically with the ESXi host:

1. Select the ESXi host where the GigaVUE-VM node is deployed.
2. Select the **Virtual Machine Startup/Shutdown** option in the **Configure** tab.
3. Select **Edit**.
4. Select **Automatically start and stop the virtual machines with the system**.

5. In the **Startup Order** section, move the GigaVUE-VM node to the **Automatic Startup** section.

## GigaVUE-VM Nodes and Maintenance Mode

Maintenance Mode is a commonly used vSphere feature used for host servicing. When a host enters the maintenance mode, its virtual machines are automatically shut down. When a host exits the maintenance mode, its virtual machines are turned back on by GigaVUE-FM.

## How to Shape Tunnel Traffic

Depending on the amount of traffic to be tunneled by a GigaVUE-VM node and any other traffic on the VMNIC, bandwidth constraints can become a concern. You can tune traffic rates using the vSphere Distributed Switch (vDS) Traffic Shaping features for the Network port-group:

- Enable the Traffic Shaping Egress option for the Network port-group (not the Tunnel port-group).
- Track the ratio of tunneled traffic to other traffic on the VMNIC to avoid contention.
- You can also send Tunneled traffic to a dedicated VMNIC to avoid contention issues using either of the following techniques:
  - NIC Teaming Load Balancing policies
  - Dedicated VMNICs for Tunnel traffic

## Tips for vMaps

### Can I configure a vMap with Slicing disabled?

There are rare cases, such as in test environments, where you may want to configure a vMap with Slicing disabled. Here is how you can do that:

- **To define a vMap without enabling slicing**, you must delete the current vMap and create a new one, leaving the "Slicing" offset field empty.
- **To later enable slicing**, edit the vMap and enter a valid slicing offset value (from 64 to 9000) and save the vMap. You can edit the vMap later to adjust the Slicing offset values (within range); however, you cannot set them to an out-of-range value or disable Slicing after it has been enabled.

# 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
<p><b>DID YOU KNOW?</b> 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 <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p><b>Hardware</b></p> <p>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</p>
<b>G-TAP A Series 2 Installation Guide</b>
<b>GigaVUE-HC1 Hardware Installation Guide</b>
<b>GigaVUE-HC2 Hardware Installation Guide</b>
<b>GigaVUE-HC3 Hardware Installation Guide</b>
<b>GigaVUE M Series Hardware Installation Guide</b>
<b>GigaVUE TA Series Hardware Installation Guide</b>
<b>GigaVUE-OS Installation Guide for DELL S4112F-ON</b>
<b>Software Installation and Upgrade Guides</b>
<b>GigaVUE-FM Installation, Migration, and Upgrade Guide</b>

## GigaVUE Cloud Suite 5.14 Hardware and Software Guides

### GigaVUE-OS Upgrade Guide

#### 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



## GigaVUE Cloud Suite 5.14 Hardware and Software Guides

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

### Release Notes

#### GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;  
important notes regarding installing and upgrading to this release

**NOTE:** Release Notes are not included in the online documentation.

**NOTE:** Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software & Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

### In-Product Help

#### GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

#### 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](mailto:documentationfeedback@gigamon.com)

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

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

## Contact Technical Support

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

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

Email Technical Support at [support@gigamon.com](mailto: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](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

## Premium Support

Email Gigamon at [inside.sales@gigamon.com](mailto: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](https://community.gigamon.com)**

**Questions?** Contact our Community team at [community@gigamon.com](mailto: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)