GigaVUE-VM
User's Guide

Version 5.6

DOCUMENT REVISION — 3/29/19

Contents

1 About this Guide

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

This guide provides an overview of GigaVUE-VM and also describes how to install, deploy, and operate the GigaVUE® Virtual Machine (GigaVUE-VM) from Gigamon® Inc. Refer to the following sections for details:

2 GigaVUE-VM

This section describes the GigaVUE-VM Virtual Traffic Visibility in a virtual environment. This section covers the following topics:

- *GigaVUE-VM Overview* on page 10
- *GigaVUE-VM Configuration* on page 10
- *GigaVUE-VM Features and Benefits* on page 10

GigaVUE-VM Overview

The GigaVUE-VM Virtual Traffic Visibility node extends GigaVUE traffic distribution principles to the virtualized environments, allowing users to filter, monitor, and forward traffic on virtual machines to GigaVUE nodes for distribution to monitoring and analysis tools. GigaVUE-VM nodes support vSphere Distributed Switch, vSphere Standard Switch, NSX vSwitch, and the Cisco Nexus 1000V virtual switch 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.

Once 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 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 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 traffic distribution to local and stacked tool ports.

GigaVUE-VM Configuration

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

Because the virtual environment is so dynamic, 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).

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® 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 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), NSX-V and Cisco Nexus 1000V.
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.
Hotspot monitoring	Pro-actively monitor and troubleshoot GigaVUE-VM nodes by elevating Top-N and Bottom-N virtual traffic policies to the centralized dashboards.

3 Licensing GigaVUE-VM

This section describes how to obtain and apply licenses for GigaVUE-VM. It consists of the following main sections:

- *Licensing GigaVUE-VM* on page 14 describes the licenses available and how to obtain and apply them.

- *GigaVUE-VM License Types* on page 14 lists the available licenses and features available with each license type.

- *Applying Licenses* on page 16 describes the process to apply the licenses.

- *Upgrading and Downgrading License Packages* on page 18 covers the best practices when upgrading or downgrading license packages.

Licensing GigaVUE-VM

GigaVUE-FM is provisioned by default with a Base License that lets you 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.

Obtaining a New License

Contact your Sales representative to obtain a new license for GigaVUE-FM or additional GigaVUE-VM Nodes (see *Contacting Sales* for the contact information).

Retrieving a Lost License

If you lost an existing license, contact Gigamon Technical Support for assistance. For the contact information, refer to *Contacting Technical Support*.

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. 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.

Table 3-1: GigaVUE-FM and GigaVUE-VM Evaluation License Packages

License Types	Physical Nodes	Virtual Nodes	OpenStack/ AWS/Azure	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.

Table 3-2: 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 are no hard requirements to purchase GigaVUE-FM package. However, you will be limited to 1 day of trending data for the dashboard and reports.

Applying Licenses

Use the following procedure to license your products on the **License** page.

To obtain and apply the GigaVUE-VM license:

1. Locate the email sent to you by Gigamon containing the licensing information for your installation. This email contains one or more **GIK** (**G**igamon **I**nstallation **K**eys) values. You will use these GIKs to generate License Keys on the Gigamon Licensing Website.

2. Locate the MAC address of the virtual network adapter associated with the GigaVUE-FM installation. To locate the address, click **Administration** on the top navigation link. Refer to Figure 3-1 on page 16.
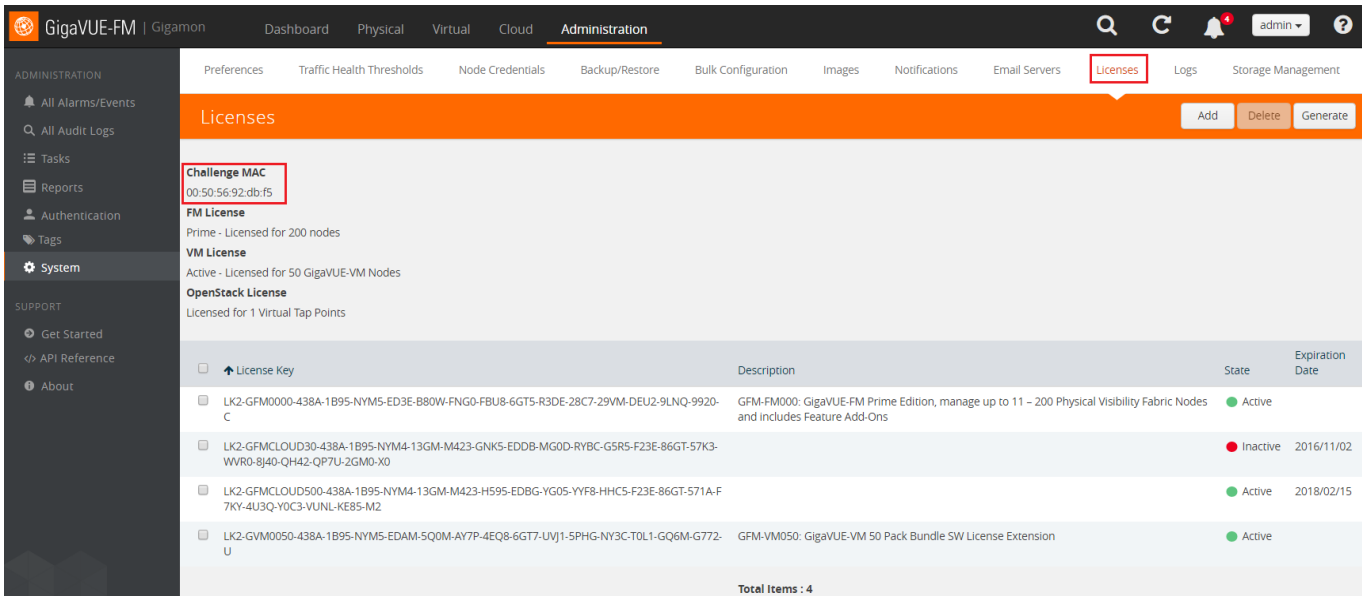
Figure 3-1: Locate the MAC Address

3. In the left navigation pane, select **System**.

4. Click **Licenses**. The Licenses page is displayed as shown in Figure 3-1 on page 16.

   Refer to the Challenge MAC displayed in the Licenses page. The license is only valid with the corresponding MAC address. If GigaVUE-FM is deleted or re-installed, contact Gigamon Support.

5. GigaVUE-VM licenses can be generated by clicking on **Generate** from the Licenses tab or by using the Gigamon Licensing Portal from the following location:

   https://licensing.gigamon.com

Figure 3-2: Gigamon Licensing Portal

6. Enter the MAC address and GIKs of the purchased licenses in the portal. Multiple GIKs can be entered by clicking the **+** button. Once all the information is entered and submitted, the license key(s) are displayed on the screen.

7. Write down the license key or keys.

8. Login to GigaVUE-FM as an administrator and navigate to the **Administration > System > License** page. Refer to .

9. Click the **+** (Add) button and enter the license key or keys provided by Gigamon into the dialog box that appears, and then click **Save** to apply the license.

Figure 3-3: Add License Page

Upgrading and Downgrading License Packages

- Upgrading of license packages is available at all times.

- To purchase a new license, please contact Gigamon Sales Representative.

- All licenses are perpetual therefore they carry in to any software upgrades without re-applying the licenses, except evaluation licenses are set for expiration. Software upgrades can be managed during valid evaluation period.

- Licenses can be upgraded from Base to either a 45 day evaluation or to paid version.

- If an evaluation license is upgraded to Express or Advanced version, the Add-on features are automatically disabled. To retain the Add-On features, please purchase the license for Add-On features such as FabricVUE Traffic Analyzer, or upgrade to the Prime Package.

- Purchased licenses cannot be downgraded.

- Licenses can be deleted and re-entered as long as the MAC address tied to the license is still valid.

In case of expiration of the evaluation license, GigaVUE-FM and GigaVUE-VM will revert back to supporting only 1 physical and 1 virtual node.

4 Virtual Dashboard

This chapter describes the Virtual Dashboard of GigaVUE-FM.

This chapter covers the following topics:

Overview of the Virtual Dashboard

The Virtual Dashboard is similar to the Physical Dashboard, which is shown in Figure 4-1 on page 20. The Virtual Dashboard 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

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-FM User's Guide. The Virtual Dashboard is displayed as shown in Figure 4-1 on page 20.
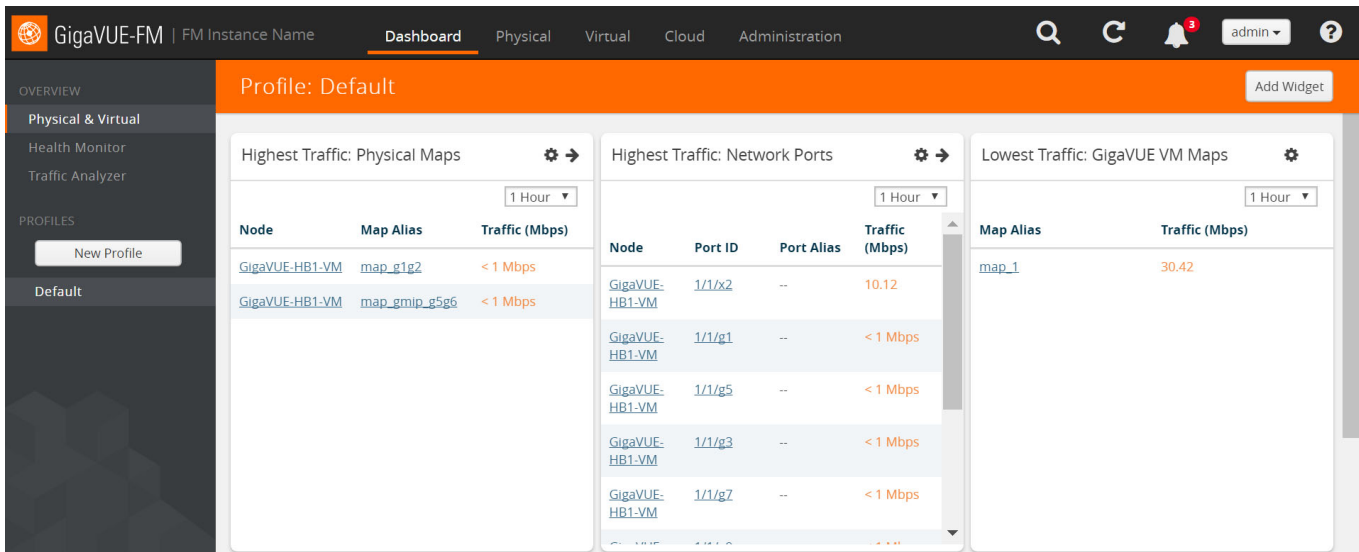
Figure 4-1: Virtual Dashboard

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

This section provides descriptions of each of the widgets available on the Virtual Dashboard. The widgets available are:

• Highest Traffic widgets

• Lowest Traffic widgets
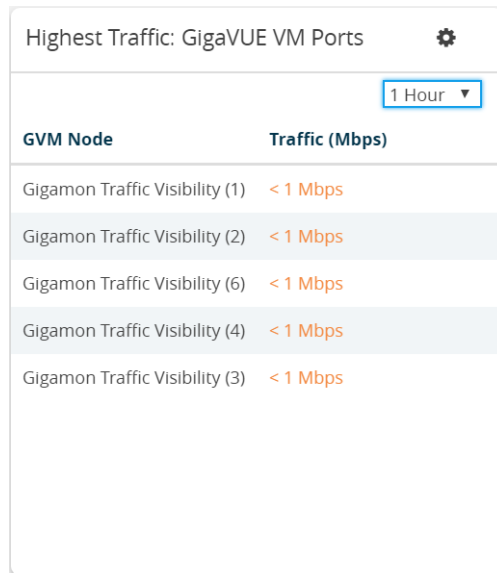
You can customize the widgets by creating and managing profiles. Refer to *Virtual Dashboard Profiles* on page 19 for more information.

Highest Traffic

The Highest Traffic widget lists the GigaVUE-VMs with the highest traffic within a specified time. You can create as many Highest Traffic widgets as you want listing 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.

The GigaVUE-VMs contributing to the highest traffic can be displayed as either a table or a graph. By default, a table is displayed. You can click the arrow to change the display to a graph as shown in Figure 4-2 on page 21.

Highest Traffic: GigaVUE VM Ports	⚙
	1 Hour ▼
GVM Node	**Traffic (Mbps)**
Gigamon Traffic Visibility (1)	< 1 Mbps
Gigamon Traffic Visibility (2)	< 1 Mbps
Gigamon Traffic Visibility (6)	< 1 Mbps
Gigamon Traffic Visibility (4)	< 1 Mbps
Gigamon Traffic Visibility (3)	< 1 Mbps

Figure 4-2: Highest Traffic Contributor: Physical Maps Example

In the graph view, each ring represents a GigaVUE-VM. You can hover your mouse over the graph to view the percentage of traffic handled by the GigaVUE-VM.

To configure the Highest Traffic widget:
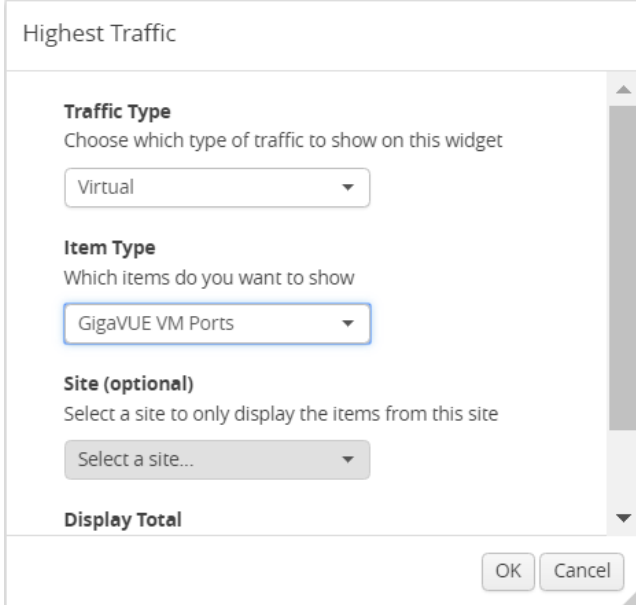
1. Click **Dashboard** on the top navigation link.

2. On the Physical & Virtual dashboard page, select the profile in which you want to add the widget.

3. Click **Add New Widget**. The Add New Widget window is displayed. Refer to Figure 4-3 on page 22.
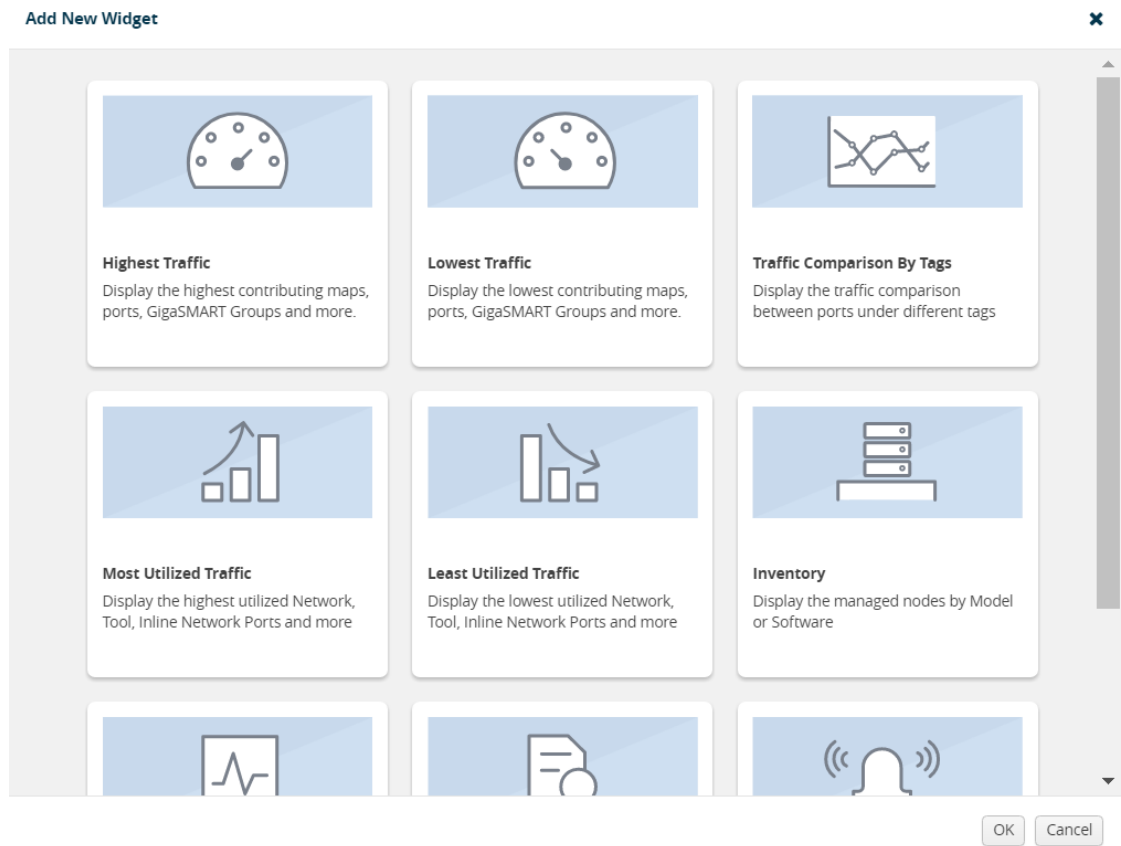
Figure 4-3: Add New Widget

4. In the Add New Widget window, select **Highest Traffic** and click **OK**. The Highest Traffic configuration window is displayed. Refer to Figure 4-4 on page 23.

Figure 4-4: Highest Traffic Configuration

5. From the **Traffic Type** drop-down list, select Virtual.

6. From the **Item Type** drop-down list, select one of the following items:

   - GigaVUE-VM Ports - displays the ports contributing to the highest traffic
   - GigaVUE-VM Maps - displays the maps contributing to the highest traffic

NOTE: Sites are not applicable for GigaVUE-VMs.
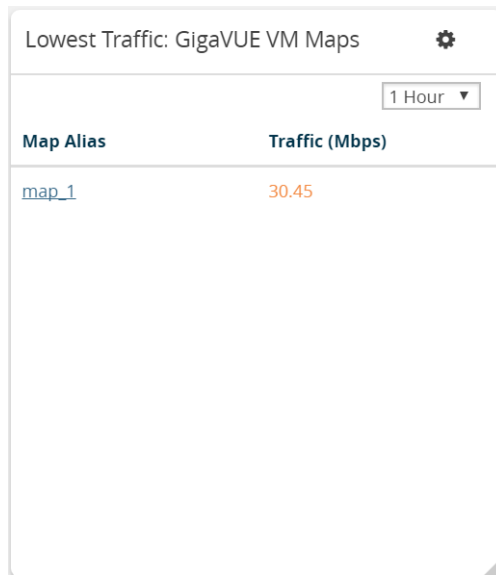
7. From the **Display Total** drop-down list, select the number of items to be displayed. By default, the number of items selected for display is 5.

8. Click **OK**.

Lowest Traffic

The Lowest Traffic widget lists the GigaVUE-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-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 GigaVUE-VM maps and ports can be displayed as either a table or a graph. By default, a table is displayed. You can click the arrow to change the display to a graph as shown in Figure 4-5 on page 24.

Figure 4-5: Lowest Traffic

In the graph view, each ring represents a map or a port. You can hover your mouse over the graph to view the percentage of traffic flowing through the GigaVUE-VM's map or the port.

The Lowest Traffic widget is configured exactly the same way as the Highest Traffic widget. To configure the Lowest Traffic widget, refer to the configuration steps provided in *Highest Traffic* on page 20.

5 Configuring Visibility for VMware

This section 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* on page 26 describes the system requirements, such as the security privileges needed for the vCenter GigaVUE-VM users.

- *Using GigaVUE-VM VMware vCenter Management* on page 29 describes the tasks you must perform the first time you use GigaVUE-VM.

- *Deploying GigaVUE-VM Nodes* on page 30 provides the procedure to deploy GigaVUE-VM nodes from GigaVUE-FM.

- *Bulk Deploying GigaVUE-VM Nodes in Standalone or Cluster* on page 36 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 Upgrading GigaVUE-VM Nodes* on page 42 provides the procedure to upgrade a single or multiple GigaVUE-VM nodes from GigaVUE-FM.

- *Configure Virtual Maps for VMware vCenter* on page 45 describes how to configure virtual maps when deploying GigaVUE-VM nodes.

- *Backing Up and Restoring GigaVUE-FM for VMware* on page 50 provides the steps for backing up and restoring GigaVUE-FM in a VMware environment.

- *Best Practices for vSphere Integration* on page 51 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 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 or the Cisco Nexus 1000V.

   • vSphere Distributed Switch. For versions, refer to *VMware ESXi System Requirements* on page 26.

   • Cisco Nexus 1000V: Version 4.2(1)SV2.1.1, 5.2(1) configured with Port-Profiles.

   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 *Configuring the Tunnel Endpoint* on page 75.) 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* on page 77.)

   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.

   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: See the appropriate vendor documentation for information on installing VMware vSphere and Cisco Nexus 1000V.

Nexus 1000V, release 5.2 support requires the REST plugin to be loaded. The status of the REST plugin can be verified with the Nexus 1000V CLI command: **show plugin status**. It is recommended that for all versions of Nexus 1000V that the REST plugin be loaded. (That is, the Rest plugin in required for Release 5.2 and recommended for all other versions)

Working with Nexus 1000V

The Nexus 1000V switch does not establish a port binding until there is network traffic from the VM on the vNIC. GigaVUE-FM cannot create port mirror sessions for the monitored vNIC until a Nexus 1000V port binding is created. Ensure that all monitored vNICs have a port binding on the Nexus 1000V by generating application traffic or using the ping command prior to creating a virtual map. If a virtual map was created before there is a port binding for the vNIC on the Nexus 1000V, re-deploy the virtual map to address the issue.

The following Nexus 1000V CLI commands will show the port bindings:

- show port-profile virtual usage
- show interface virtual attach binding

Troubleshooting the Nexus 1000V

If you receive the message "Source ports on monitor session should not be empty" when configuring the vMap, this means that there is no network traffic from the VM on the vNIC. To resolve the problem, see the previous section *Working with Nexus 1000V*.

Refer to the GigaVUE-VM Release Notes for the virtual computing resources that the VMware ESXi server must provide for each GigaVUE-VM instance.

Required VMware Virtual Center Privileges

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

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

Category	Required Privilege	Purpose
Host	**Configuration** • Network Configuration	VSS Map
	Inventory • Modify Cluster	Pin GigaVUE-VM to the host in cluster configurations. This prevents automatic migration.
Datastore	• Allocate space	GigaVUE-VM Deployment
Distributed Switch	• VSPAN Operation	VDS Map

Category	Required Privilege	Purpose
Network	• Assign network	GigaVUE-VM Deployment/VSS Map
Resource	• Assign virtual machine to resource pool	GigaVUE-VM Deployment
vApp	• Import	GigaVUE-VM Deployment
	• vApp instance configuration	GigaVUE-VM Deployment
Virtual machine	**Configuration**	
	• Add new disk	GigaVUE-VM Deployment
	• Modify device settings	GigaVUE-VM Deployment/VSS Map
	Interaction	
	• Device connection	GigaVUE-VM Deployment
	• Power on	GigaVUE-VM Deployment
	• Power Off	GigaVUE-VM Deployment
	Inventory	
	• Create from existing	GigaVUE-VM Deployment
	• Remove	GigaVUE-VM Deployment
	Provisioning	
	• Clone virtual machine	GigaVUE-VM Deployment

Using GigaVUE-VM VMware 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	Click **Virtual** on the top navigation link. On the left navigation pane, under VMware vCenter go to **Management** > **Virtual Centers**	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. Refer to *Setting up the Connection between GigaVUE-FM and Virtual Center on page 35*.
2	Deploy GigaVUE-VM to multiple ESXi hosts	Under VMware vCenter, go to **Management** > **Virtual Nodes** > **Deploy Virtual Nodes**	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 *Bulk Deploying GigaVUE-VM Nodes in Standalone or Cluster on page 36*.
3	Configure a tunnel definition.	Under VMware vCenter, go to **Management** > **Tunnel Library**	Virtual traffic from the GigaVUE-VM is tunneled to the physical GigaSMART card. This step is used to add the already configured tunnel endpoint on GigaSMART to the GigaVUE-FM for use in virtual maps. Refer to *Configuring the Tunnel Endpoint on page 75*.
4	Verify deployed GigaVUE-VMs and status	Under VMware vCenter, go to **Virtual Nodes**	To verify the GigaVUE-VM deployment status, check the status on the Virtual Nodes page.
5	Configure Cisco Nexus 1000V	Under VMware vCenter, go to **Management** > **Virtual Switches**	This step is applicable only for Cisco Nexus switch. It provides the IP address of VSM so that GigaVUE-FM can communicate with N1KV.
6	Configure Virtual Maps/ Rules	Under VMware vCenter, go to **Virtual Maps**	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 *Configure Virtual Maps for VMware vCenter on page 45*.

Deploying GigaVUE-VM Nodes

GigaVUE-VM software package is distributed as a hardened OVA file. The following section describes how to deploy GigaVUE-VM nodes on an **ESXi host.**

Deploying GigaVUE-VM nodes consists of the following major steps:

1. Configure port-groups and port-profiles within vSphere. Refer to *Configuring Port Groups/Port-Profiles* on page 30.

2. Set up the connection between the Fabric Manager and the Virtual Center. Refer to *Setting up the Connection between GigaVUE-FM and Virtual Center* on page 35.

3. 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 Deploying GigaVUE-VM Nodes in Standalone or Cluster* on page 36.

Notes:

- 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.

Configuring Port Groups/Port-Profiles

GigaVUE-VM nodes use Port Groups (vSphere Standard Switch and vSphere Distributed Switch) or Port-Profiles (Cisco Nexus 1000V virtual 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	Nexus 1000V
Management	Yes	Yes	Yes
Tunnel	Yes	Yes	Yes
Network	No	Yes	Yes

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

- *Configuring Port Group/Port-Profile for GigaVUE-VM Management* on page 31
- *Configuring Port Group/Port-Profile for GigaVUE-VM Tunnel* on page 32
- *Configuring Port Group/Port-Profile for GigaVUE-VM Network* on page 33

Configuring 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
- Cisco Nexus 1000V

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* on page 51.

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.

Configuration of Management Port Group for vSS Example

You can use the following steps as an example of how to configure a virtual standard switch (vSS) port group. This procedure shows how to configure the management port group on a vSS. This example is also applicable for configuring a vSS for the Tunnel port group.

1. Log in to the vSphere client and add a vSphere Standard Switch to your Data Center, followed by populating it with Hosts and Network Adapters. Refer to the vSphere documentation for details.

2. Select the **Host > Configuration > Networking inventory** view.

3. Go to **Add Networking** and select **New Port Group**.

4. Supply the following **Properties** for the Management Port Group:

Name	Use a name that helps identify the purpose of the port group in GigaVUE-VM. For example, **vss_PG_GVM_Management**.
Number of Ports	Optional. Either enter the number of ports in the field or use the scroll up-down button to enter the value.
VLAN Type	Optional. Select one of the following: • None • VLAN • VLAN Trunking • Private VLAN

5. Click the **Next** button.

6. Click the **Finish** button.

   The new Network Port Group appears under the **Standard Switch** entry in the vSphere Client.

You will select the port groups for **Management**, but not for **Network**, that you created here in Step 3 of the GigaVUE-VM Bulk Deploy wizard.

Configuring 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

• Nexus 1000V

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* on page 51.

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.

Configuration of Tunnel Port Group for vDS Example

You can also use the following example to configure the Tunnel port group for the vSS and Nexus 1000V virtual devices. This procedure shows how to configure for a vDS:

1. Log in to the **vSphere Client** and add a vSphere Distributed Switch to your Data Center, followed by populating it with Hosts and Network Adapters. Refer to the vSphere documentation for details.

2. Select the **Networking inventory** view.

3. Right-click on the **Distributed Switch** entry and select **New Port Group**.

4. Supply the following **Properties** for the Tunnel Port Group:

Name	Use a name that helps identify the purpose of the port group in GigaVUE-VM. For example, **dvPG_GVM_Tunnel**.
Number of Ports	Optional. Either enter the number of ports in the field or use the scroll up-down button to enter the value.
VLAN Type	Optional. Select one of the following: • None • VLAN • VLAN Trunking • Private VLAN

5. Click **Next**.

6. Click **Finish**.

   The new Tunnel Port Group appears under the **Distributed Switch** entry in the vSphere Client.

Configuring 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

• Nexus 1000V

For information on vSS configuration for Network traffic, see *Creating a vMap using a vNIC on vSS* on page 34.

Configuration of Network Port-Profile for Nexus 1000V Example

NOTE: This example is also applicable for configuring Nexus 1000V for Management and Tunnel port groups.

Use this example to configure the Network port group for Nexus 1000V virtual devices:

1. Make sure the Cisco Nexus 1000V is already added to your Data Center and populated with Hosts and Network Adapters. Refer to the Cisco Nexus 1000V documentation for details.

2. Log in to the command line interface for the Cisco Nexus 1000V and use the port-profile command to add the necessary port-profiles.

Note: For each port-profile, choose a name that helps identify the purpose of the port group in GigaVUE-VM.

For example, **GVM-Mgmt** for the management traffic, **GVM-Tunnel** for the tunneling traffic, and so on. For example:

Port-Profile Type	Commands
Network Traffic Port-Profile	port-profile type vethernet GVM-Network
	vmware port-group
	switchport mode access
	switchport access vlan 1
	no shutdown
	system vlan 1
	state enabled

3. Perform a **copy running-config startup-config** command to save the port-profiles.

4. The new port-profiles automatically appear in the Networking Inventory of the Data Center that includes the Nexus 1000V virtual switch.

You will select the port groups you created here in Step 3 of the GigaVUE-VM Bulk Deploy wizard.

Creating a 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.

Setting up the Connection between GigaVUE-FM and Virtual Center

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

1. Click **Virtual** on the top navigation link.

2. On the left navigation pane, under VMware vCenter, go to **Management** > **Virtual Centers**.

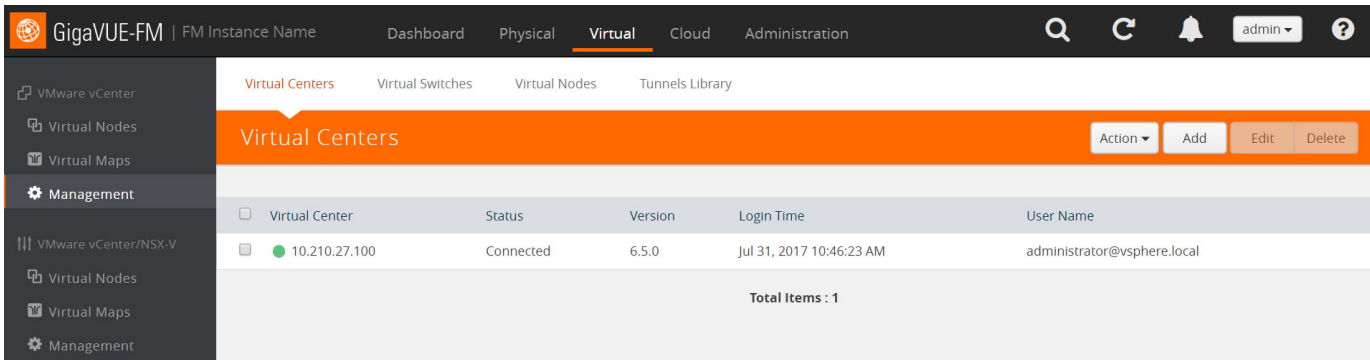   The VMware vCenter Virtual Centers page displays.

Figure 5-1: VMware vCenter Configuration

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

3. Click **Add**.

   The Virtual Center Connection dialog opens.

Figure 5-2: Add Virtual Center Page

4. Enter the IP address or DNS name for the Virtual Center.

5. In the Username field, enter a username.

6. In the Password field, enter a password.

7. 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 *Required VMware Virtual Center Privileges* on page 27.

# Bulk Deploying 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.

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

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

1. Click **Virtual** on the top navigation link.

2. On the left navigation link, under VMware vCenter, go to **Management > Virtual Nodes**.
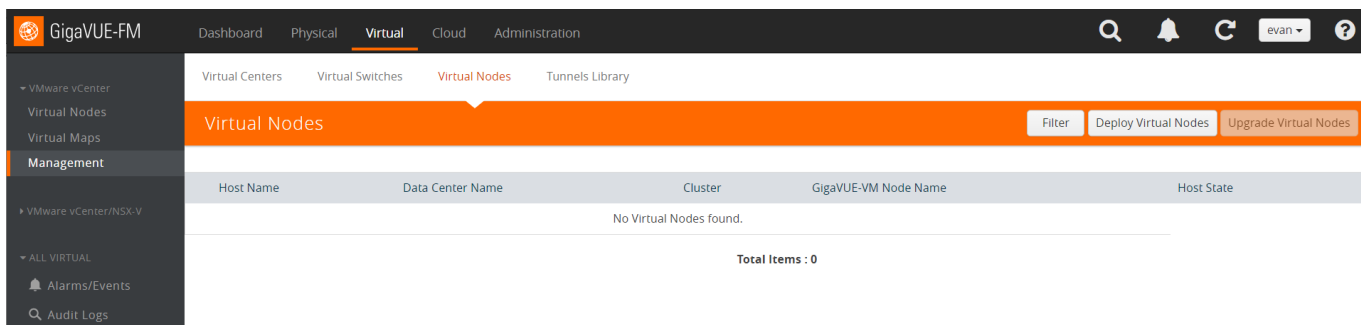
3. Click **Deploy Virtual Nodes**.

4. Open the OVA control plane and select the OVA image file to be used for the Bulk Deployment as shown in Figure 5-3 on page 37. 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.
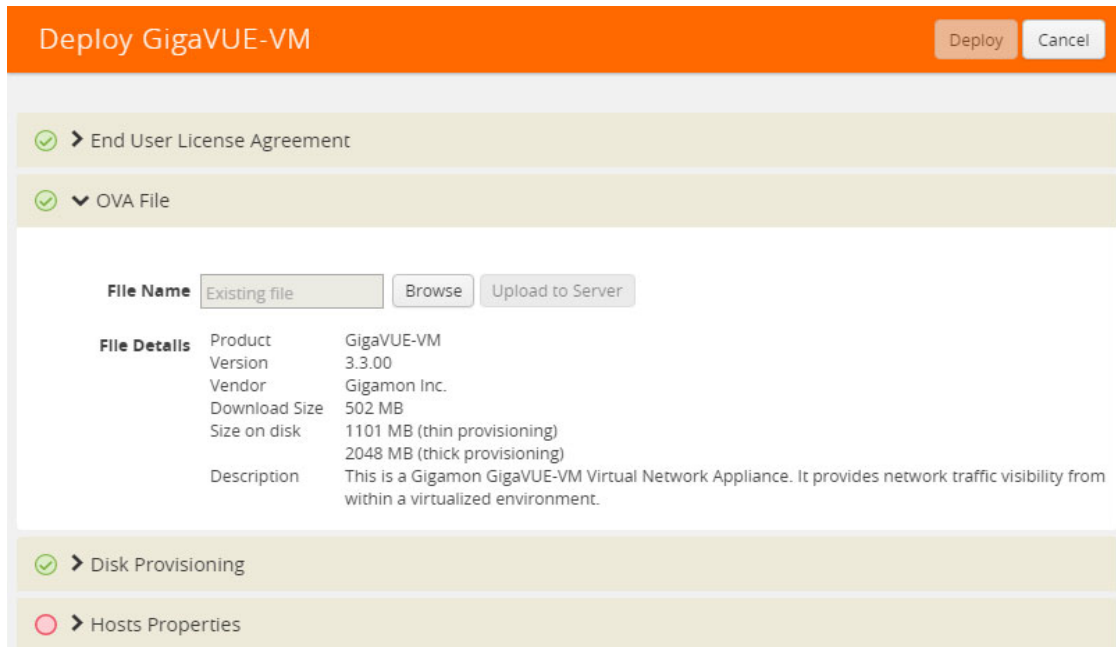
Figure 5-3: Virtual Node Deployment Page

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

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

7. 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). An example is shown in Figure 5-4.
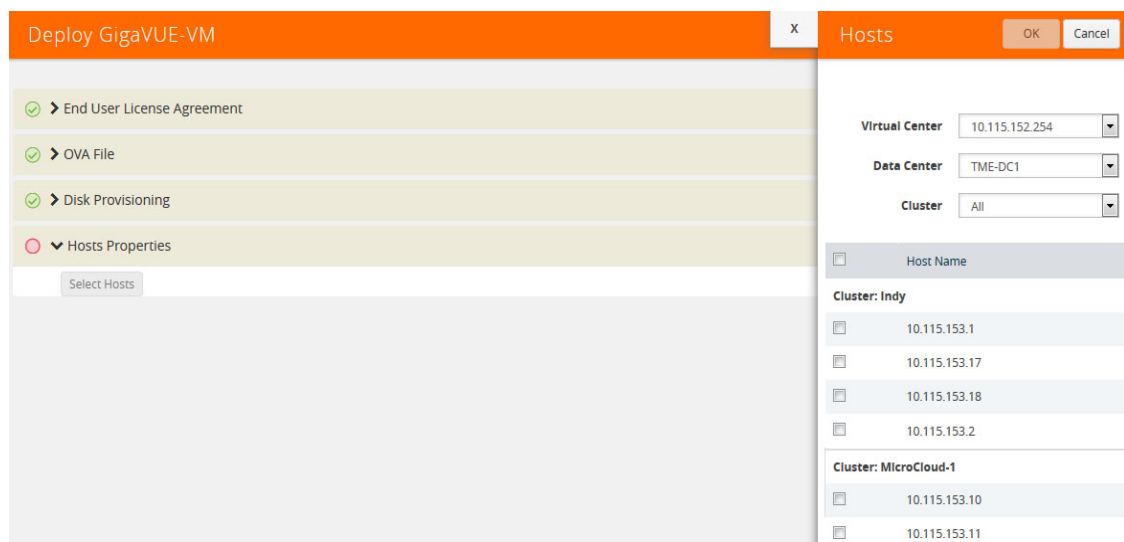

Figure 5-4: Bulk Deploy Hosts

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.

- Select each host where you would like to deploy a GigaVUE-VM node. You can select all hosts by selecting the **Host Name** checkbox.

- 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.

- Once you have selected the hosts where you want to deploy GigaVUE-VM nodes, click **OK** to continue.

8. 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 *Configuring Port Groups/Port-Profiles* on page 30 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.

Setting 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 described in Table 5-1 on page 39.

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.
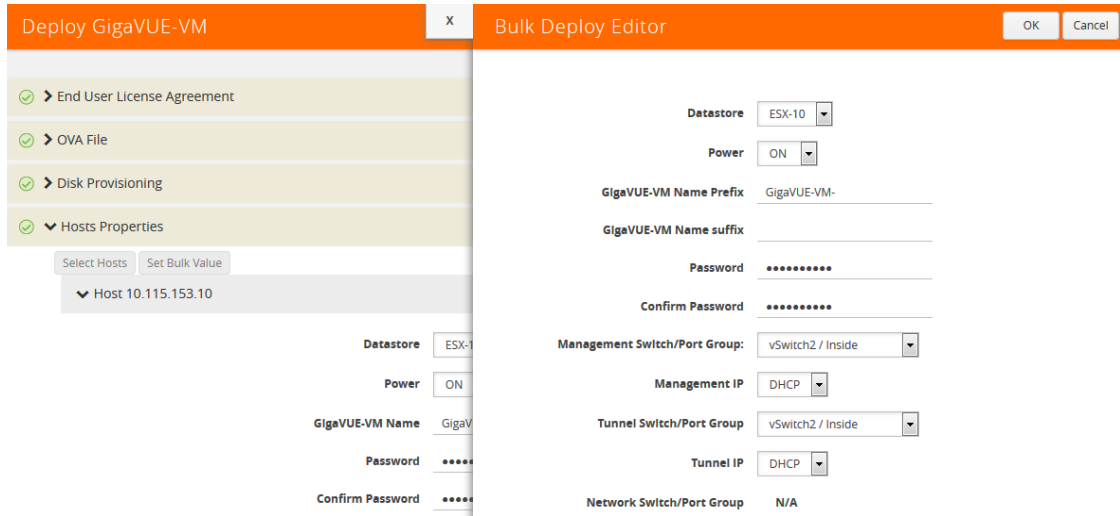

Figure 5-5: Bulk Deploy Editor

Regardless of whether you select **Set Bulk Values** or configure individual nodes, you set the same set of options described in Figure 5-3.

Table 5-1: GigaVUE-VM Node Options

GigaVUE-VM Node Option	Description
Datastore	Select the datastore on the target host where the GigaVUE-VM node should be installed.
Power	Choose whether to power on the GigaVUE-VM node after deployment.
GigaVUE-VM Name	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.
Password	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) or port-profiles (Cisco Nexus 1000V virtual switch) for the Management Port, IP interface, and Network Port for the GigaVUE-VM instance. The port groups you configured in *Configuring Port Groups/Port-Profiles* on page 30 are available for assignment.	

Table 5-1: GigaVUE-VM Node Options

GigaVUE-VM Node Option	Description
Management Switch/Port Group **Management IP**	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 **Management > Virtual Nodes** 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.
Tunnel Switch/Port Group **Tunnel IP**	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-2404, or a GigaVUE H Series family with GigaSMART blade and tunneling encapsulation enabled.
	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.
	Note: For optimal performance, Gigamon recommends maintaining the IP interface on a separate subnet than that used by the management port or network ports.
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.

5. Click **Finish** to launch the Bulk Deploy. You can monitor the progress of the Bulk Deploy in the **Administration > Alarms/Events** page. 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 **Related Objects > Virtual Machines** tab for the ESXi host on 10.210.17.11, we can see that there is only one GigaVUE-VM node installed here as shown in Figure 5-6.
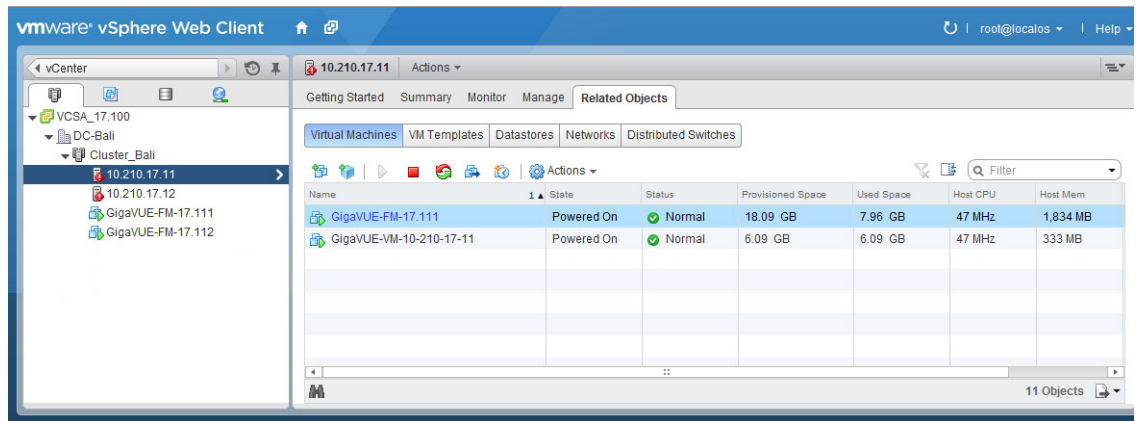
Figure 5-6: vCenter Client Showing the GigaVUE-VM Installation

DHCP Problems?

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**.

About the 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 > Options > vApp Options > Advanced**, as shown in the following figure:
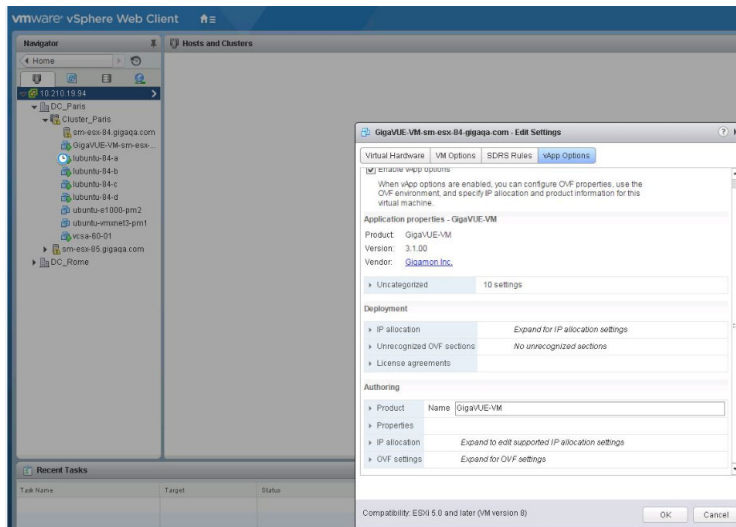
Bulk Upgrading GigaVUE-VM Nodes

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. Click **Virtual** on the top navigation link.

2. On the left navigation link, under VMware vCenter, go to **Management > Virtual Nodes**.

3. Click the **Upgrade Virtual Nodes**.

4. Open the OVA control plane and select the OVA image file to be used for the Bulk Deployment as shown in Figure 5-7 on page 43. 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.
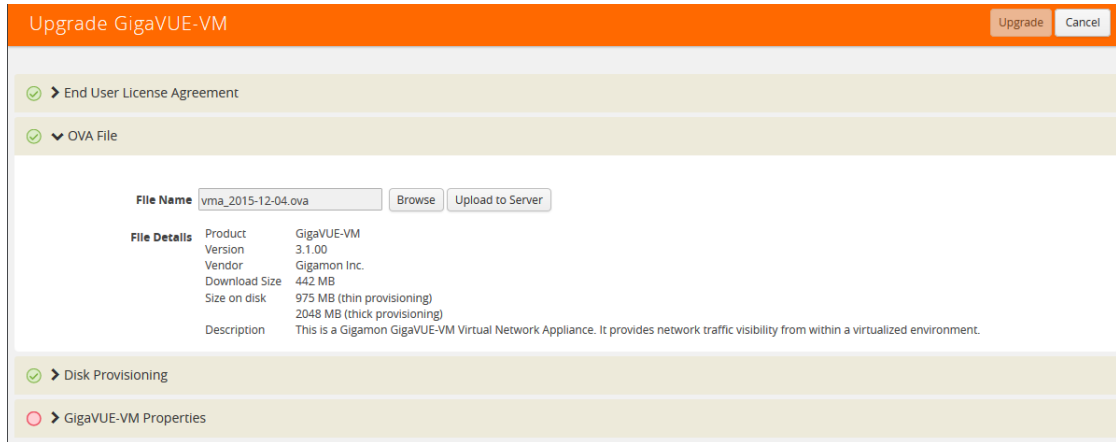

Figure 5-7: Software Version Upgrade on Virtual Nodes Page

5. **End User License Agreement** — After careful review of the EULA, select **I accept the End user License ("EULA")**.

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

7. Open the GigaVUE-VM Properties.
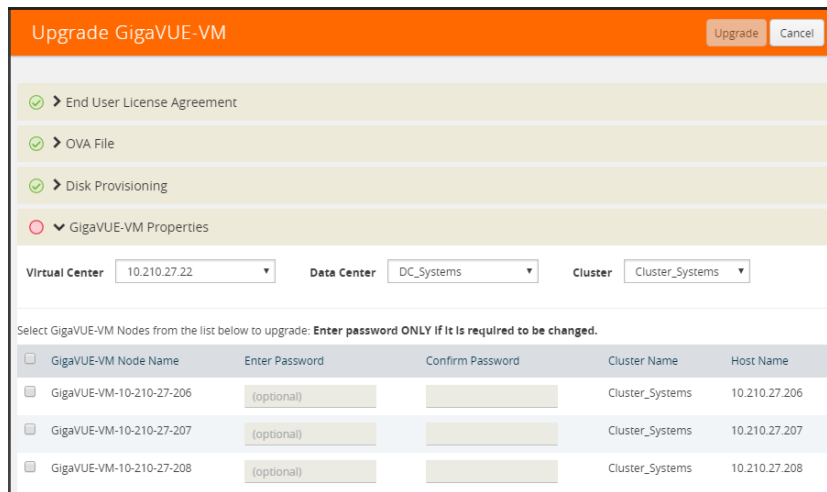
Figure 5-8: Upgrade Virtual Nodes Page

8. 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.

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.

c. From the **Cluster** drop-down list, select the cluster to upgrade. At this point the page should look similar to the page shown in .

d. In the **Enter Password** column, provide the existing node password for the GigaVUE-VM upgrade.

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.

e. Select the hosts where you want to upgrade GigaVUE-VM nodes. Click **Upgrade** to continue.

9. Click **Upgrade**.

Configure Virtual Maps for VMware vCenter

To configure Virtual Maps on the virtual nodes for VMware, under VMware vCenter, go to **Virtual Maps** to display the Virtual Maps page shown in Figure 5-9.

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 *Configuring the Tunnel Endpoint* on page 75.

Figure 5-9: Creating virtual maps for VMware using GigaVUE-FM

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 in the table. The controls are described in Table 5-2.

Table 5-2: Controls Available on the Virtual Maps Page

Controls	Description
New	Opens the Create Map dialog, allowing you to create a virtual map. (See *Configuring a vMap for VMware* on page 47)
Edit	Opens the Edit Map dialog, allowing you to edit a virtual map.
Delete	Deletes the selected virtual map.
Redeploy	Redeploys the selected virtual map.
Redeploy All	Redeploys all of the virtual maps.
Tunnel Validation	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 Table 5-3.

Table 5-3: 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	Deployment status of the map. The three states and conditions leading to the states are: • **Success**—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. • **Partial Success**—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. • **Failure**—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. The quick view provides information under the status tab about what part of the deployment has failed.
Traffic	Traffic column provides the status of the GigaVUE-VM traffic. The two states are: • **Consistent**—When all the monitored vNIC are up and are able to transmit/receive traffic. • **Inconsistent**—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.
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 5-4. By clicking on **Edit** on the quick view, you can review or update these parameters.

Table 5-4: 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.

Table 5-4: Parameters Displayed in the Virtual Map Quick View

Parameters	Description
VM Map Rules	Map Rules defined for the virtual machine.
Network Adapters Monitored	Details relating to the vNIC.

Configuring a vMap for VMware

To configure the vMap for VMware, do the following:

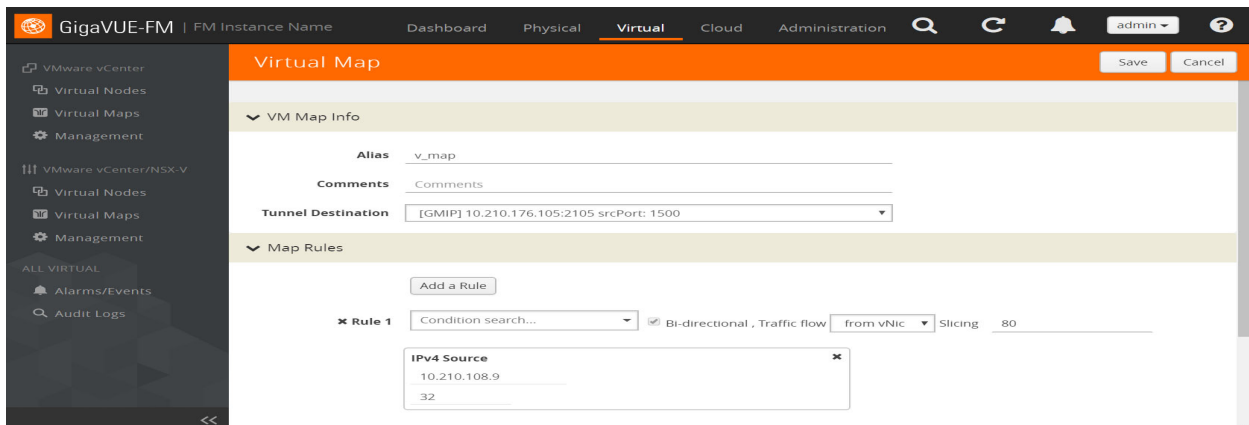1. Click **New** to open the configuration page, which is shown in Figure 5-10.

Figure 5-10: Virtual Map Configuration Page

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.

NOTE: passed through the filter.

- Traffic Flow:
  - from vNic
  - to vNic
- Slicing

Figure 5-11 shows a Virtual Map with one rule added.
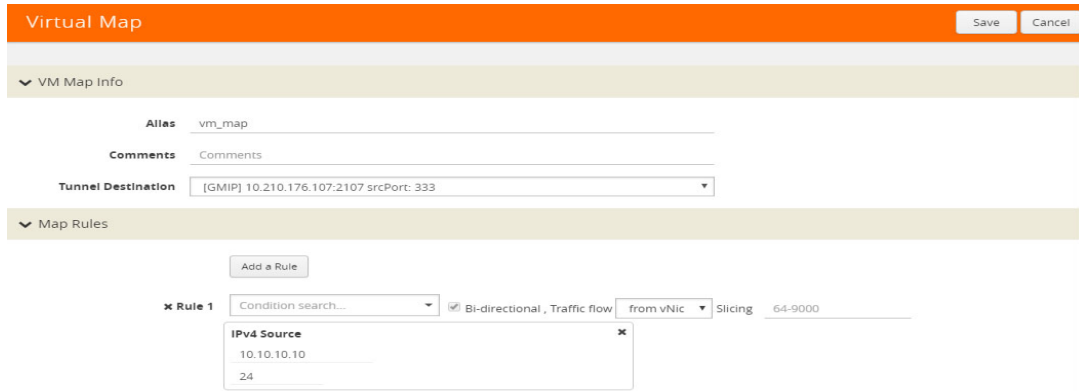
Figure 5-11: Virtual Map with a Rule

NOTE: For Virtual Map rules, the bi-directional option is always selected because traffic is always monitored in both directions while From vNic and To vNic options specify the filter criteria. In Figure 5-11, 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**. Refer to Figure 5-2.

This opens a 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.
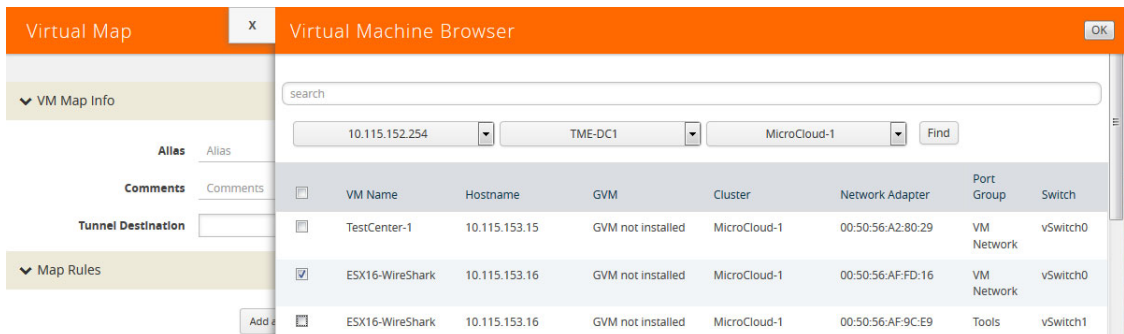
Figure 5-12: Selecting Virtual Machine Network Adapter

vMap Rules

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.

Creating a 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 Alarms/Events page. To view the Alarms/Events page, go to **Virtual** > **Alarms/Events** or **Administration > All Alarms/Events** page.
- Reconfigures maps to use GigaVUE-VM to deploy on the new host for the monitored VM if there is one deployed there.
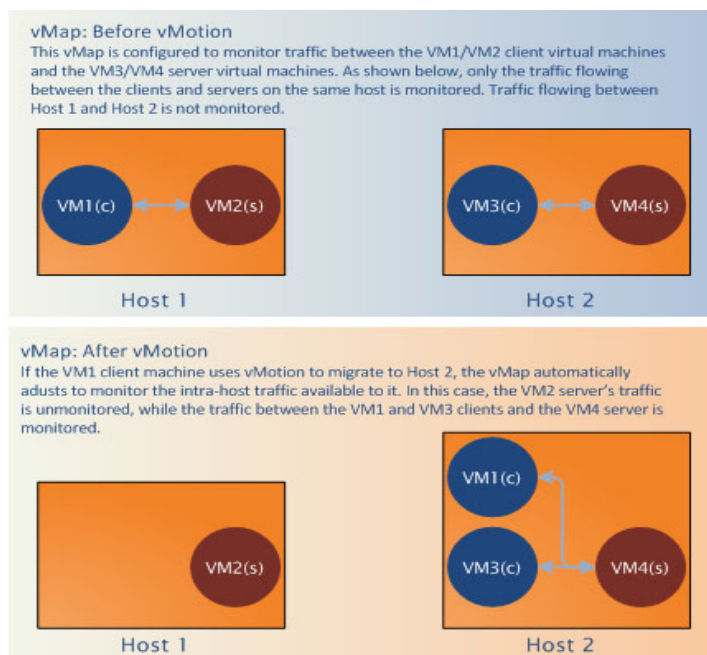
Figure 5-13: Figure summarizing vMotion

GigaVUE-VM: Monitoring 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. Figure 5-14 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.
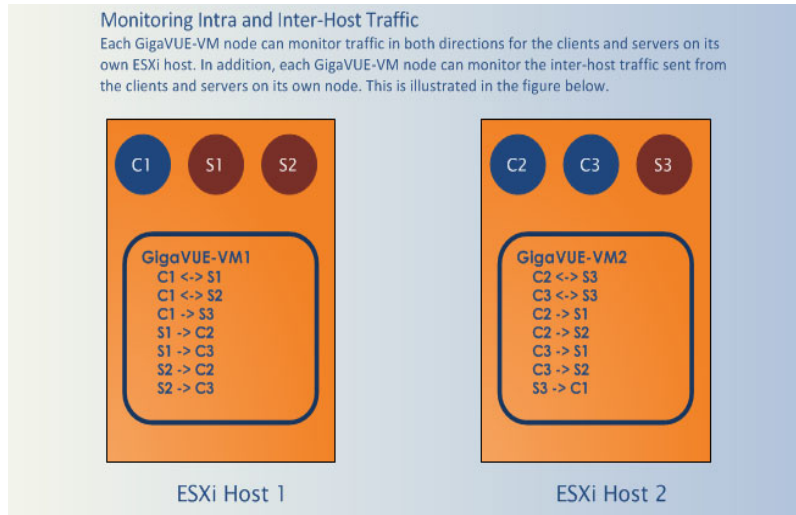

Monitoring Intra and Inter-Host Traffic
Each GigaVUE-VM node can monitor traffic in both directions for the clients and servers on its own ESXi host. In addition, each GigaVUE-VM node can monitor the inter-host traffic sent from the clients and servers on its own node. This is illustrated in the figure below.

GigaVUE-VM1
C1 <-> S1
C1 <-> S2
C1 -> S3
S1 -> C2
S1 -> C3
S2 -> C2
S2 -> C3

GigaVUE-VM2
C2 <-> S3
C3 <-> S3
C2 -> S1
C2 -> S2
C3 -> S1
C3 -> S2
S3 -> C1

ESXi Host 1   ESXi Host 2

Figure 5-14: Monitoring Intra-Host and Inter-Host Traffic

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.

Backing Up and Restoring 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 section *Data Saved When Backing Up GigaVUE-FM* on page 1303 in th GigaVUE-FM User's 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 *Restoring GigaVUE-FM Configuration Files* on page 1304 in the GigaVUE-FM User's Guide.

4. Log in to vCenter and reboot the GigaVUE-FM instance. (In vCenter, select **Power > Power Off/Power On**.)

5. Reboot the GigaVUE-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* on page 45.

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

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:

Using 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

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.

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.

Preventing Migration of GigaVUE-VM Nodes Operating in Clusters

GigaVUE-FM supports a maximum of one GigaVUE-VM node per ESXi host. Because of this, you will want to configure GigaVUE-VM nodes operating in clusters to prevent them from migrating automatically when a host becomes unavailable, possibly resulting in multiple GigaVUE-VM nodes on the same ESXi host. The procedure is slightly different depending on whether the node is deployed in a High-Availability (HA) cluster or a DRS cluster.

Notes:

• Make sure that the GigaVUE-VM nodes that you are applying bulk values is powered **Off**.

• If the host is part of a DRS cluster, the GigaVUE-VM node is automatically pinned to the host if the permissions are available. For information about setting the permission, refer to *Required VMware Virtual Center Privileges* on page 27.

1. Open the vSphere client, select the vSphere Cluster with the GigaVUE-VM nodes, and select **Edit Settings**.

2. Select **vSphere HA > Virtual Machine Options**.

3. Sort the **Virtual Machine** column by name and select all GigaVUE-VM nodes.

4. Set the **VM Restart Priority** option to **Disabled**.

To prevent GigaVUE-VM node migration in DRS Clusters:

1. Open the vSphere client, select the vSphere Cluster with the GigaVUE-VM nodes, and select **Edit Settings**.

2. Select **vSphere DRS > Virtual Machine Options**.

3. Sort the **Virtual Machine** column by name and select all GigaVUE-VM nodes.

4. Set the **Automation Level** option to **Disabled**.

Configuring GigaVUE-VM Nodes to Restart Automatically After a 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 **Configuration** tab.

3. Select **Properties**.

4. Select **Allow virtual machines to start and stop automatically 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 node, its virtual machines are automatically shut down. When a host exits the maintenance mode, its virtual machines are turned back on by GigaVUE-FM.

Shaping 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

Alarms and Events

The Alarms and Events page displays all the alarms and 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

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 and events broadly fall into the following categories: Critical, Major, Minor, or info.

Click **Virtual** on the top navigation link. On the left navigation pane, the **Alarms/Events** page is selected by default. Refer to Figure 5-15 on page 53.

Figure 5-15: Virtual - Alarms and Events
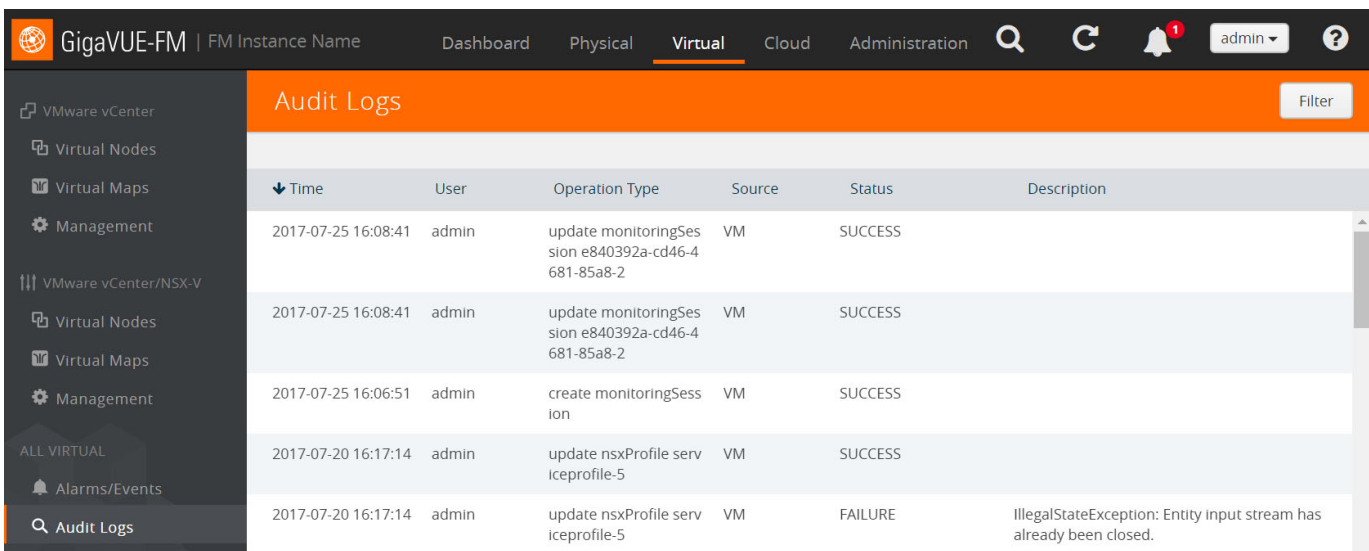
For information about the parameters for each alarm or event, refer to *All Alarm/Event Parameters* on page 1268. For filtering the alarms and events, refer to *Filtering Alarms/ Events* on page 1270.

NOTE: The alarms and events can be purged or archived only from the All alarms/ events page. For more information, refer to *Archiving or Purging Alarm/Event Records on page 1271*.

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 *Overview of Audit Logs on page 1274*. Filtering the audit logs allows you to display specific type of logs. For more information, refer to *Filtering Audit Logs on page 1274*.

Figure 5-16: Virtual - Audit Logs

GigaVUE-VM User's Guide

6 Configuring Visibility with NSX

GigaVUE-FM integrates with VMware NSX as a partner service, using NSX Service Insertion. Service Insertion allows partner services such as Gigamon Traffic Visibility to integrate with NSX. When the NSX Manager is registered in FM, a Gigamon Traffic Visibility Service is registered with NSX. The Traffic Visibility Service is then installed on the NSX 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:

The prerequisites for integration are described in *Prerequisites for GigaVUE-VM NSX Integration* on page 56.

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

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

To upgrade GigaVUE-VM nodes on VMware NSX, refer to *Upgrading GigaVUE-VM on NSX* on page 66.

Prerequisites for GigaVUE-VM NSX Integration

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

- For VMware ESXi and NSX-V Hardware Requirements, refer to *VMware ESXi System Requirements* on page 26.

- FM 3.4 or later.

- GigaVUE 4.5 or later node with GigaSMART to support tunnel configuration.

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

Integrating GigaVUE-VM with NSX

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

For VMware NSX and GigaVUE-FM to communicate, a Gigamon-FM user must be created in VMware and an NSX 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 and GigaVUE FM to communicate, users with the proper permissions must be created in both GigaVUE-FM and VMware NSX.

NOTE: GigaVUE-FM connects to NSX 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 callback user in GigaVUE-FM.

Creating the GigaVUE-FM User in NSX vCenter

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

To add an NSX 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 Administrator role to the user from the vCenter Web Client, do the following:
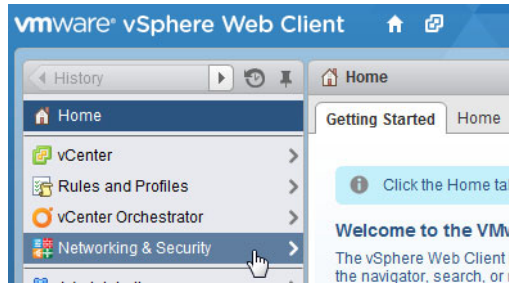
a. Select **Networking & Security**.

Figure 6-1: VMware vSphere Home Page

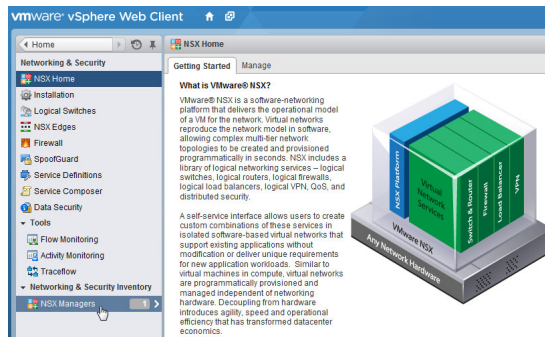**b.** Select **Networking & Security Inventory** > **NSX managers**.

Figure 6-2: Networking & Security Page

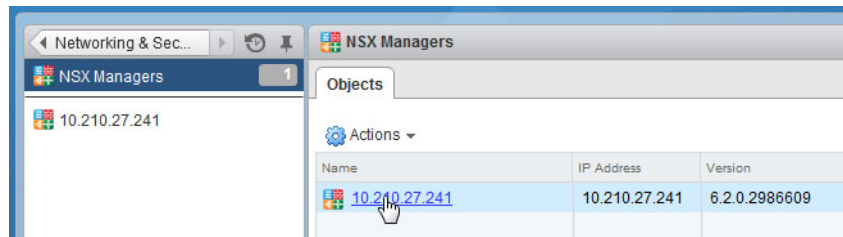**c.** Select an NSX Manager.

Figure 6-3: NSX Managers Page

d. Select **Manage > Users > 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**.

Creating the VMware NSX user in GigaVUE-FM

For VMware NSX 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. Click **Administration** on the top navigation link.
2. On the left navigation pane, select **Authentication > FM Users**.
3. Click **Add**.
4. On the FM Users 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 Manger Callback as the user name to help you associate this user with the NSX Manger.
   - In the **Username** field, enter a username for the user. For example, you can use nsx to help you remember that this user is associated with NSX.
   - In the **Password** field, enter the password for the user specified in the **Name** and **Username** fields.
   - In the **Role** field, enter the user's role. Enter fm_admin in this field.

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

FM Users nsx

Name	NSX Manager Callback
Username	nsx
Password	••••••••
Confirm Password	••••••••
Role	fm_admin

Figure 6-4: FM Users NSX Page

5. Click **Save**.

Step 2: Register the NSX vCenter and NSX Manager in GigaVUE-FM

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

When the NSX Manager is registered in GigaVUE-FM, it registers the Gigamon Traffic Visibility Service in NSX 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 visibility fabric.

Adding the vCenter Registered with NSX to GigaVUE-FM

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

1. Click **Virtual** on the top navigation link.

2. On the left navigation pane, under VMware vCenter, select **Management > Virtual Centers**.

3. Click **Add**. The Add Virtual Center page displays.

Figure 6-5: Add Virtual Center Page

4. 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.

Registering the NSX Manager in GigaVUE-FM

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

1. Click **Virtual** on the top navigation link.

2. On the left navigation pane, under VMware vCenter/NSX-V, select **Management > NSX Managers**.

3. Click **Add**. The Add NSX Manager page displays.

Figure 6-6: Add NSX Manager Page

4. Enter the information in the fields as follows:

- • In the **NSX Manager** field, enter the hostname or IP address of the NSX Manager.

- • In the **NSX Username** field, enter the user that FM uses to authenticate with NSX. This is the user created during the steps described in *Creating the GigaVUE-FM User in NSX vCenter* on page 56.

- • In the **NSX Password** field, enter the password for the NSX user.

- • In the **FM User** field, enter in the user in GigaVUE-FM for NSX to communicate back with FM. This the user created in *Creating the VMware NSX user in GigaVUE-FM* on page 57.

- • In the **FM Password**, enter a password for the GigaVUE-FM user.

- • In the **Connected vCenter** field, select the connected vCenter IP.

5. Click **Save**.

Step 3: Upload the GVM OVA Image

The GVM OVA image must be uploaded to the Fabric Manager™ so that NSX 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:

1. Click **Virtual** on the top navigation link.

2. On the left navigation pane, under VMware vCenter/NSX-V, go to **Management > Image Upload**.

3. Select the **I accept the End User License Agreement ("EULA")** check box.

4. Click the **OVA File** link.

5. 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: Install the Gigamon Traffic Visibility Service on vCenter Clusters

The Gigamon Traffic Visibility service must be installed on each of the clusters in the NSX 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**.

2. Select the Service Deployments tab.

3. Click the green **+** 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 5: Configuring GigaVUE-FM Tunnels and Virtual Maps

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

Creating a Tunnel to the GigaSMART Device

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

1. Click **Virtual** on the top navigation link.

2. On the left navigation pane, under VMware vCenter, select **Management > Tunnels Library**.

3. Click **Add** to open the Add Tunnel Endpoint page.

   When the page opens, GigaVUE-FM should discover and display the GigaVUE 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.

   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 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 *Configuring the Tunnel Endpoint* on page 75.

Creating the Virtual Maps

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

1. Click **Virtual** on the top navigation link.

2. On the left navigation pane, under VMware vCenter/NSX-V, select **Virtual Maps** and then click **New**.

3. On the NSX Virtual Map page, 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 traffic will be sent.

   c. For **Virtual Center**, select the VMware vCenter registered with the NSX Manager to be monitored.

   d. (Optional) Click **Add a Rule** if you need slicing or filtering beyond what the NSX security filtering policy provides.

   e. Click **Save**.

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

Step 6: Create the NSX Security Group and Security Policy

An NSX 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.

Creating the Security Group

A security group should be created that contains the VMs to forward NSX 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 > + New Security Group**.

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 Administration Guide*.

Creating the 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 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 + Create Security Policy.

Before you proceed to Step 3, 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 "4 Network Introspection Services" to select the Network Introspection Services tab.

   c. Click + Add Network Introspection Service.

   d. In the Name and Description fields, enter any 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. For Source, select Policy's Security Groups.

   i. For Destination, select Any.

   j. 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.

   k. For State, select **Enabled**.

   l. For Log, select **Do not log**.

   m. Click **OK**.

4. On the New Security Policy page, click **Finish**.

Mapping the Security Policy to the 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 the security policy.
4. Select **Actions > Apply Security Policy**.
5. Select the security groups to which to apply the security policy.
6. Click **OK**.

Upgrading GigaVUE-VM on NSX

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

- *Uploading the OVA file* on page 66
- *Upgrading the Gigamon Traffic Visibility in the VMware vCenter* on page 68
- *Viewing the Upgraded GigaVUE-VM Nodes* on page 70

Uploading the OVA file

To upload the OVA file:

1. Login to GigaVUE-FM.

2. Click **Virtual** on the top navigation link. Under VMware vCenter/NSX-V, go to **Management** > **Image Upload**. Refer to .
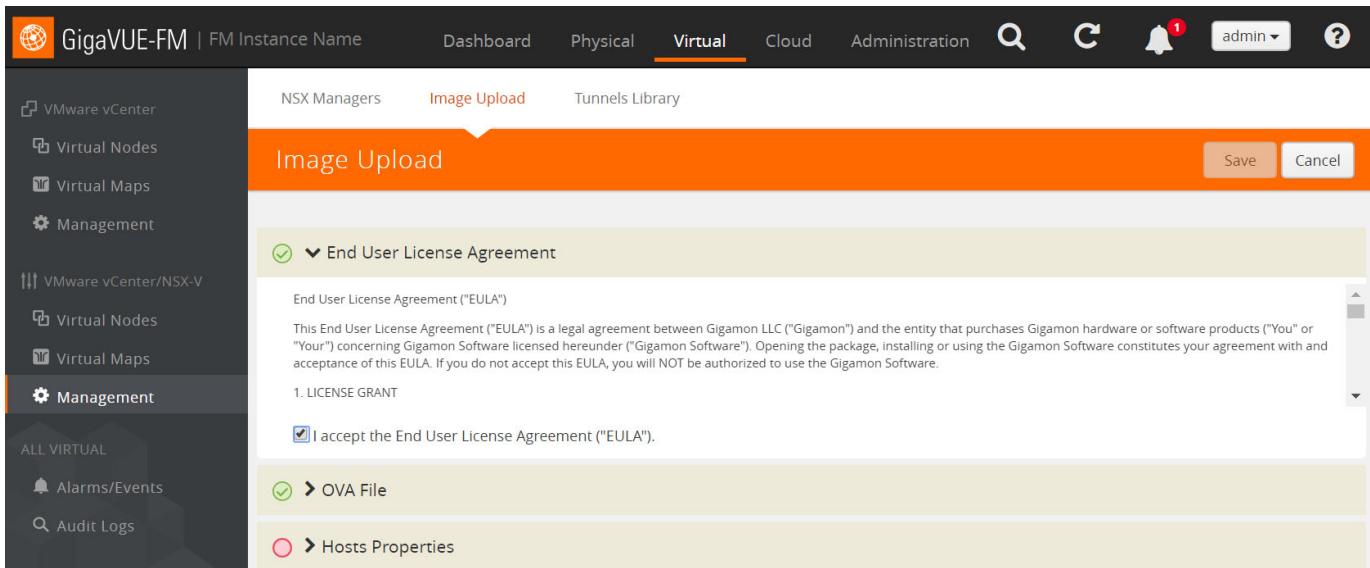
Figure 6-7: VMware vCenter Management Page

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**. Refer to Figure 6-8 on page 67.
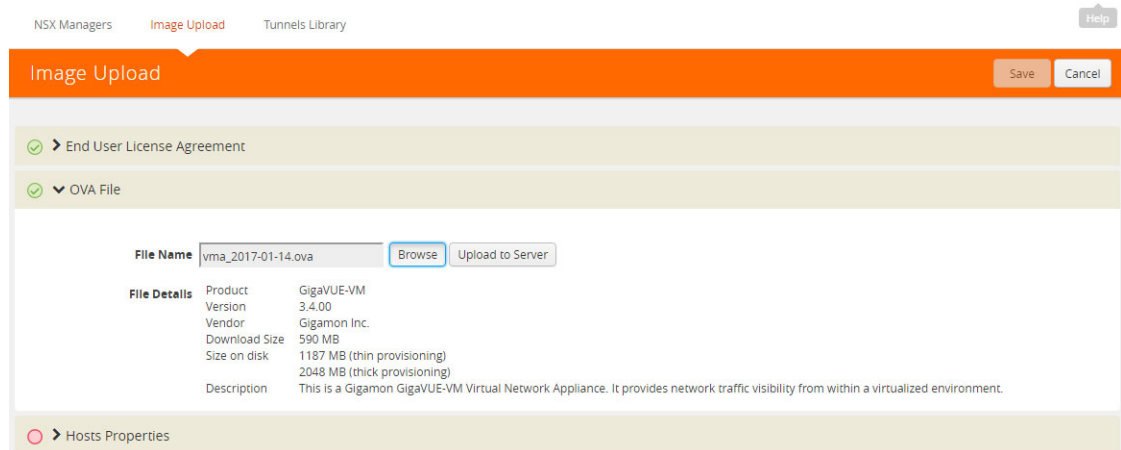
Figure 6-8: Browse the OVA File

Once the upload is complete, a confirmation message is displayed. Refer to Figure 6-9 on page 67.

Figure 6-9: Upload the OVA File to Server

5. Click the Hosts Properties link. Enter the password in the **Password** field. Re-enter the same password in the **Confirm Password** field. Refer to Figure 6-10 on page 68.

Figure 6-10: Enter the Password

6. Click **Save**.

Upgrading the Gigamon Traffic Visibility in the VMware vCenter

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

1. Login to the VMware vCenter.

2. Select **Networking & Security** > **Installation** > **Service Deployment**. The Gigamon Traffic Visibility service shows as **Upgrade Available**. Refer to Figure 6-11 on page 68.
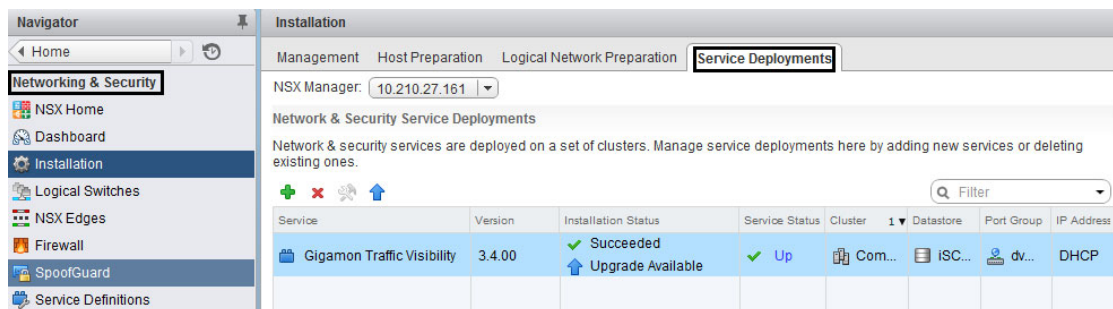
Figure 6-11: Service Deployment Page

3. Select the Gigamon Traffic Visibility service and click the **Upgrade** icon. Refer to .
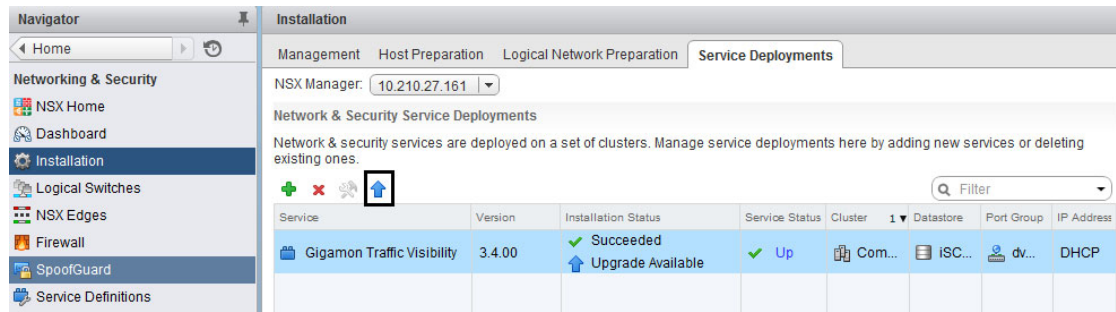
Figure 6-12: Upgrade the Gigamon Traffic Visibility Service

4. To upgrade the GigaVUE-VMs right away, select the **Upgrade now** radio button and click **OK**. Refer to .
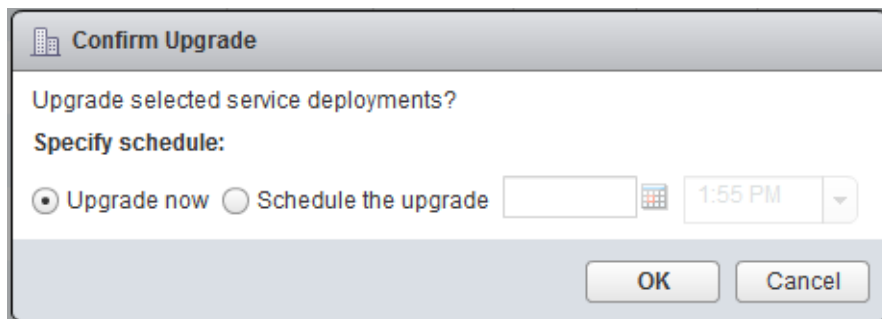
Figure 6-13: Confirm Upgrade Dialog Box

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

- Scheduled for upgrade
- Enabling
- Succeeded (refer to .)
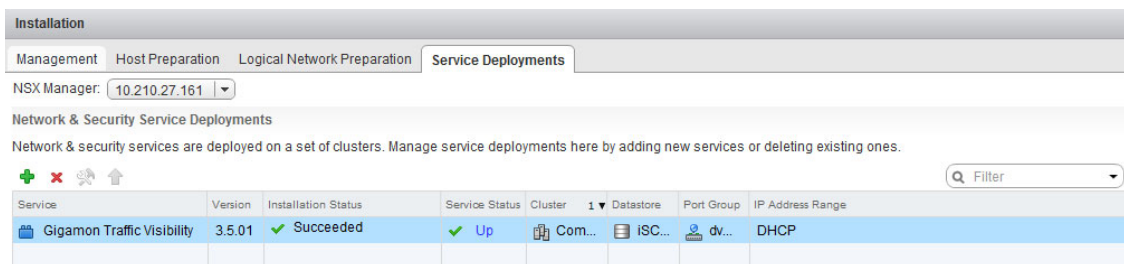
Figure 6-14: Update Succeeded
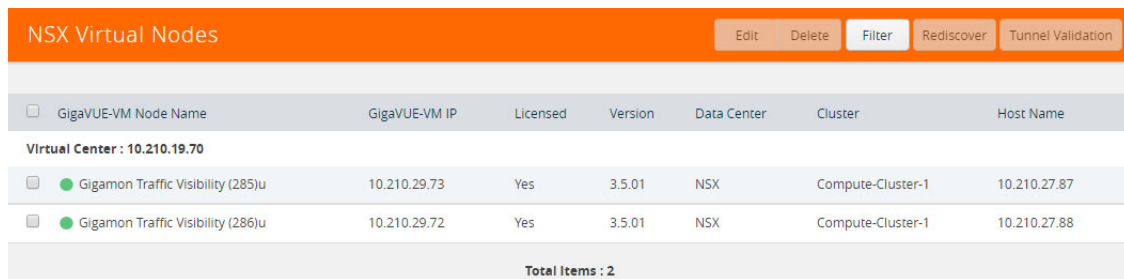
The GigaVUE-VM upgrade is completed when the Installation Status displays the status as Succeeded and the Service Status displays the status as Up.

Viewing the Upgraded GigaVUE-VM Nodes

To view the upgraded GigaVUE-VM Nodes:

1. Log back in to GigaVUE-FM.

2. Click Virtual on the top navigation link. On the left navigation pane, under VMware vCenter/NSX-V, select **Nodes**.

   The GigaVUE-VM node names now show 'u' for the upgraded virtual nodes. The version displays the new upgraded version. Refer to Figure 6-15 on page 70.

GigaVUE-VM Node Name	GigaVUE-VM IP	Licensed	Version	Data Center	Cluster	Host Name
NSX Virtual Nodes				Edit	Delete	Filter	Rediscover	Tunnel Validation
Virtual Center : 10.210.19.70						
● Gigamon Traffic Visibility (285)u	10.210.29.73	Yes	3.5.01	NSX	Compute-Cluster-1	10.210.27.87
● Gigamon Traffic Visibility (286)u	10.210.29.72	Yes	3.5.01	NSX	Compute-Cluster-1	10.210.27.88
			Total Items : 2			

Figure 6-15: Upgraded NSX Virtual Nodes

Removing the Gigamon Service from NSX and GigaVUE-FM

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

- *Step 1: Deleting the Network Introspection Services on page 70*
- *Step 2: Deleting the NSX Virtual Maps from GigaVUE-FM on page 71*
- *Step 3: Deleting the Traffic Visibility Service from NSX on page 72*
- *Step 4: Deleting the NSX Manager from GigaVUE-FM on page 72*
- *Step 5: Deleting the Virtual Center from GigaVUE-FM on page 73*

Step 1: Deleting the Network Introspection Services

To delete the network introspection services:

1. In vCenter, select **Networking & Security > Service Composer**.

2. Select the **Security Policies** tab.

3. Select the security policy from which you wish to delete the network introspection services.

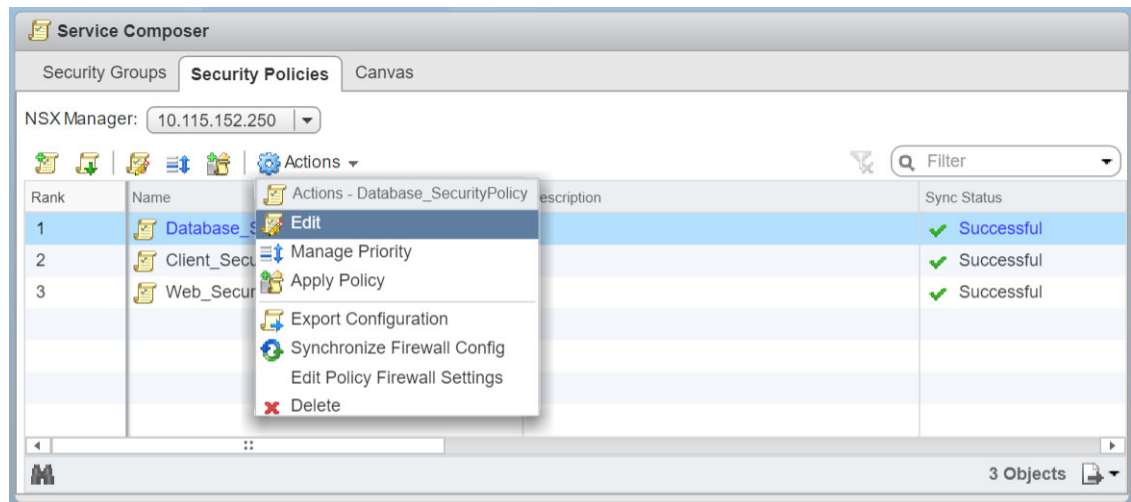**4.** Click **Actions** > **Edit**. The Edit Security Policy page is displayed.

Figure 6-16: Edit Policy

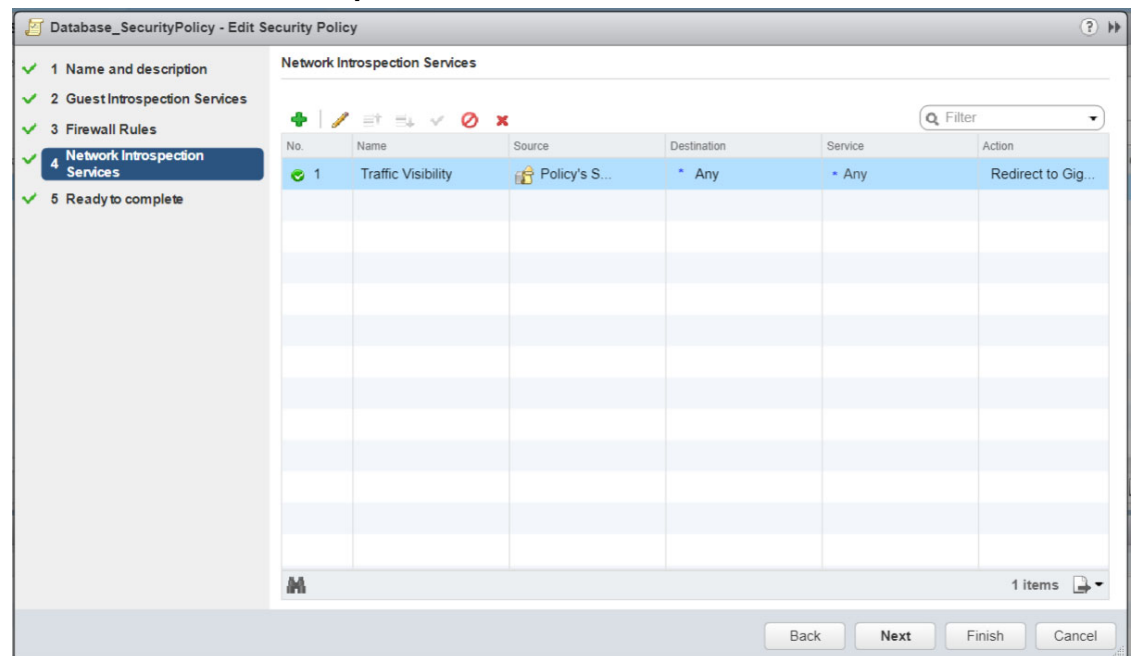**5.** Select **Network Introspection Services**.

Figure 6-17: Edit 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: Deleting the NSX Virtual Maps from GigaVUE-FM

To delete the NSX virtual maps from GigaVUE-FM:

1. In GigaVUE-FM, go to **Virtual** > **VMware vCenter/NSX-V** > **Virtual Maps**.
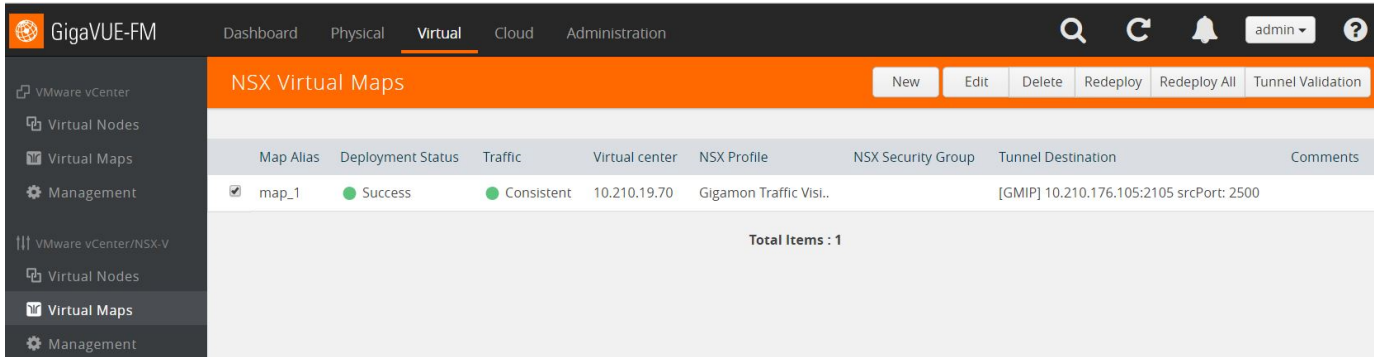
Figure 6-18: NSX Virtual Maps Delete

2. In the NSX Virtual Maps page, select the map and click **Delete**. The vendor template and the profile that corresponds to the map is deleted in NSX.

Step 3: Deleting the Traffic Visibility Service from NSX

To delete the Traffic Visibility Service from each cluster:

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

2. Select the **Service Deployments** tab.

3. From the table, select the service you wish to delete and click the red **X** (delete) icon. The selected service is deleted from all the hosts in the cluster.
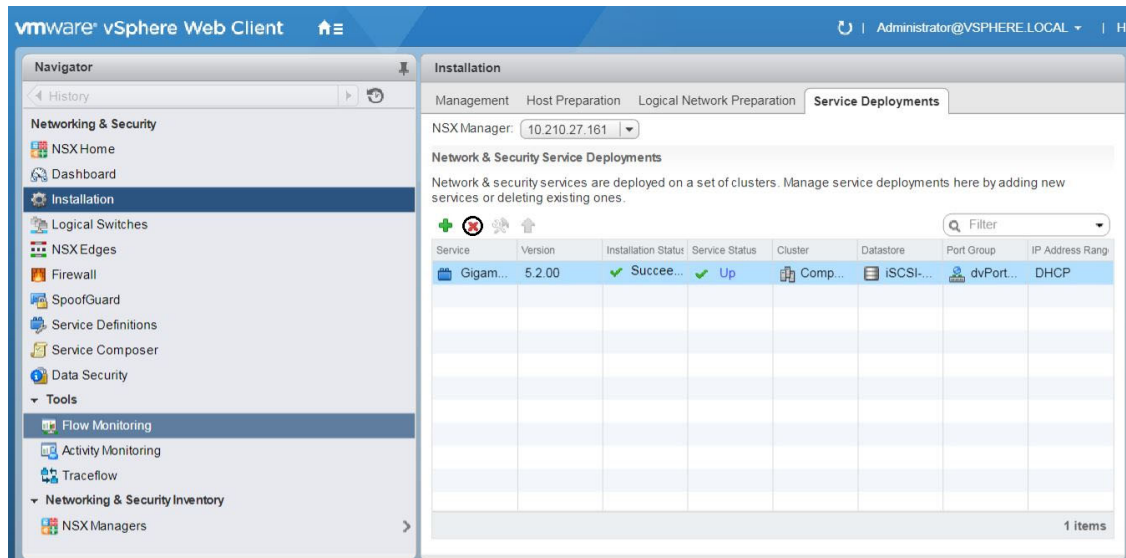
Figure 6-19: Delete the Selected Service

Step 4: Deleting the NSX Manager from GigaVUE-FM

To delete the NSX Manager:

1. In GigaVUE-FM, go to **Virtual** > **VMware vCenter/NSX-V** > **Management**.

2. Under NSX Managers, select the IP address of the NSX Manager that you wish to delete and click **Delete**.
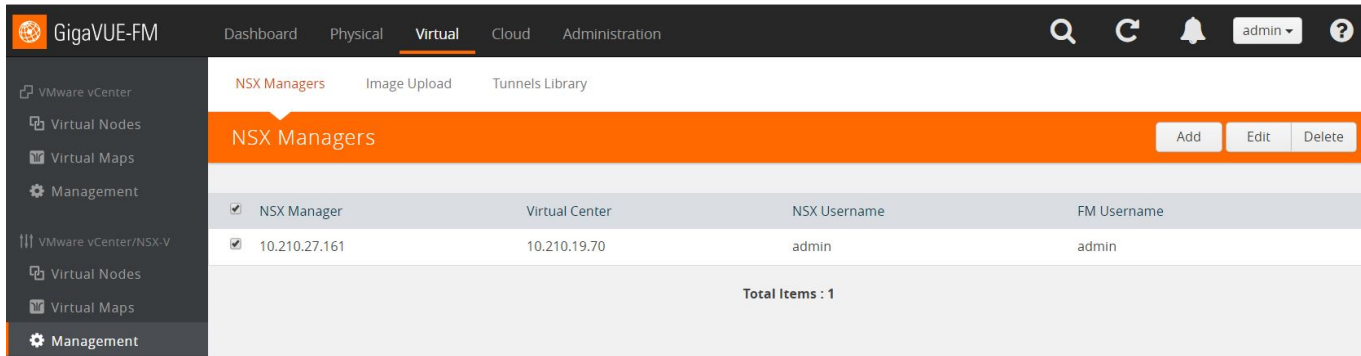
Figure 6-20: Delete the NSX Manager

Step 5: Deleting the Virtual Center from GigaVUE-FM

To delete the Virtual vCenter:

1. In GigaVUE-FM, go to **Virtual** > **VMware vCenter > Management.**

2. Under Virtual Centers, select the IP address of the virtual center you wish to delete and click **Delete**.
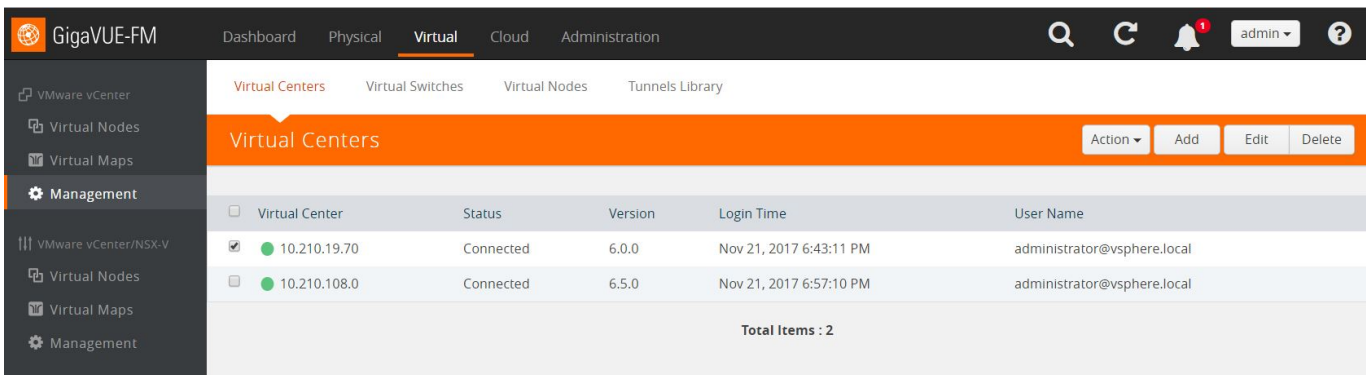

Figure 6-21: Delete the Virtual vCenter

7 Configuring the 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* on page 76
- *Creating a Tunnel Endpoint* on page 78
- *Tunnel Validation* on page 79
- *Configuring H Series IP Interfaces for the GigaVUE-VM Tunnel Library* on page 81

Tunnel Configuration Options

This section describes 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

  The GigaVUE 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 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
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: • **Tunnel Destination IP** — The IP address of the tunneled network port on the receiving end of the tunnel for both GMIP, ERSPAN, and L2GRE. (ERSPAN is only supported for VMware.) The IP address of the IP interface on the H Series device with GigaSMART. • **Tunnel Destination Port** — 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-VMs. • **Tunnel Source Port** — The port on the GigaVUE-VM from which mirrored traffic is originating. Enter 1 if this is not expected to be used.	The receiving end of the tunnel should be configured as follows: • 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. • Create a GigaSMART operation with a tunnel decapsulation component. The Decapsulation settings include the same listening UDP port you specified as the destination port at the sending end of the tunnel. • 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.

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 7-1.

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

Table 7-1: 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. This is illustrated in Figure 7-1.
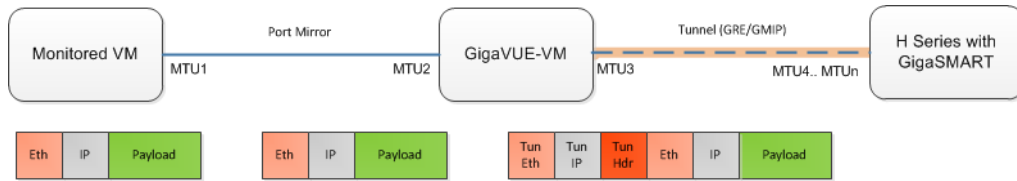
Figure 7-1: Fragmentation on GigaVUE-FM Tunnels in VMware Environments

Creating a 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. Navigate to the **Tunnels Library** page.

   Select the environment that you want to work with under Virtual in the Navigation pane, and then select **Management > Tunnels Library**.

2. Click **Add**.

3. The GigaVUE tunnels discovered should be displayed on the Add Tunnels Endpoint page as shown in Figure 7-2. If it is displayed, do the following:

   a. Select the tunnel that is configured to receive traffic from the GigaVUE-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* on page 76.

   c. Click **OK**.

Figure 7-2: Adding a Tunnel Endpoint

If the desired GigaVUE 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 *Configuring H Series IP Interfaces for the GigaVUE-VM Tunnel Library* on page 81.

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

a. Select **Other**.

b. For **Type**, select **GMIP**, **L2GRE,** or **ERSPAN**

    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* on page 76.

d. (Optional) Select the **DSCP** value. For a description of DSCP, refer to *DSCP* on page 76.

e. (Optional) Enable **Fragmentation** to allow GigaVUE-VM to fragment large packets. For a description of fragmentation, refer to *Tunnel Configuration Options* on page 76.

Figure 7-3 shows an example of a manually configured tunnel endpoint.

Figure 7-3: Adding a non-GigaVUE Tunnel Endpoint

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 can 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.
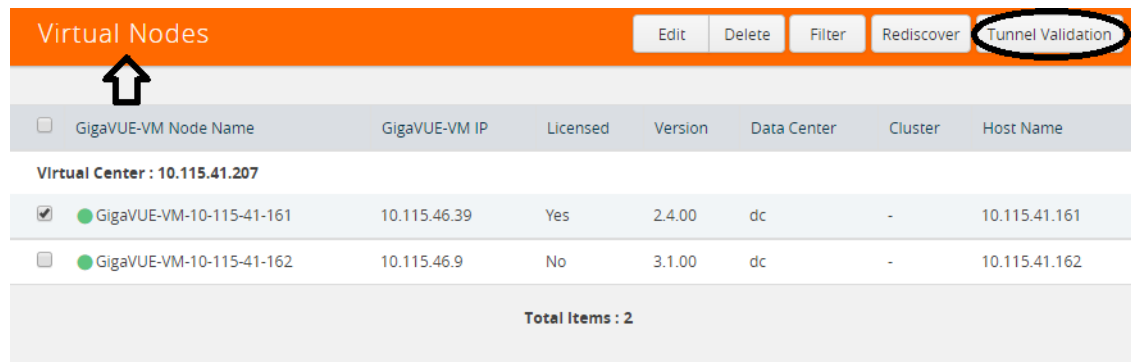
Figure 7-4: Tunnel Validation Selection From Virtual Nodes Page
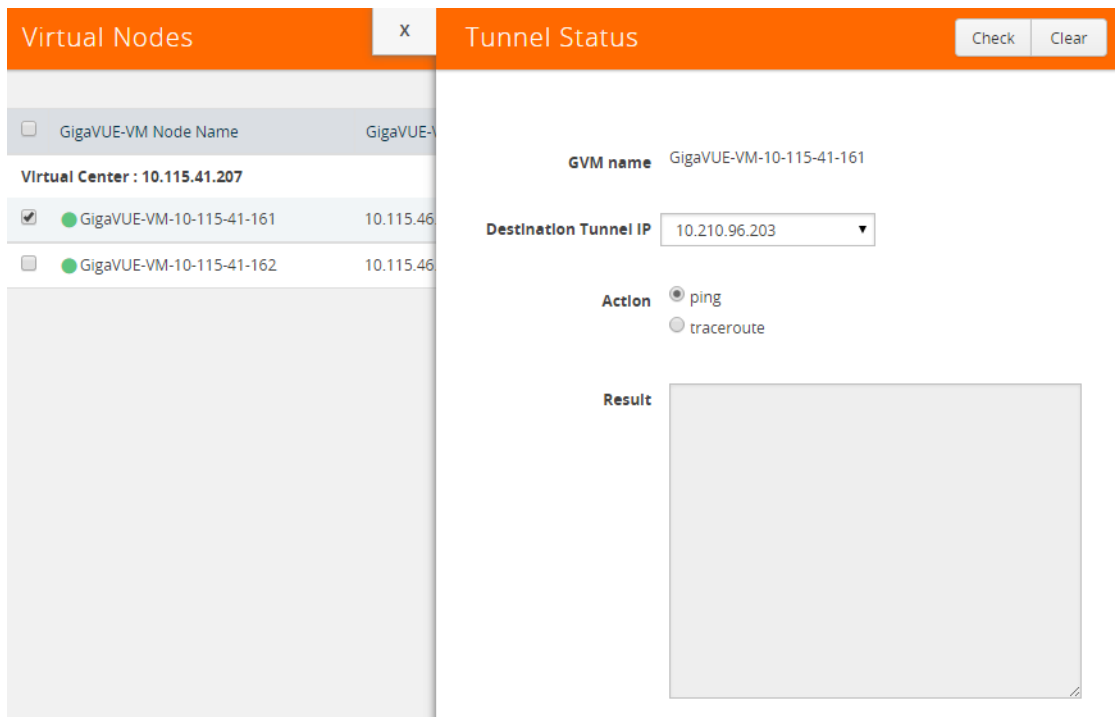
Figure 7-5: Tunnel Validation Status From Virtual Nodes Page

GigaVUE-VM User's Guide

Figure 7-6: Tunnel Validation Selection From Virtual Maps Page

Configuring 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 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 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 node to GigaVUE-FM, refer to *Adding a New Physical Node or Cluster to GigaVUE-FM* on page 206

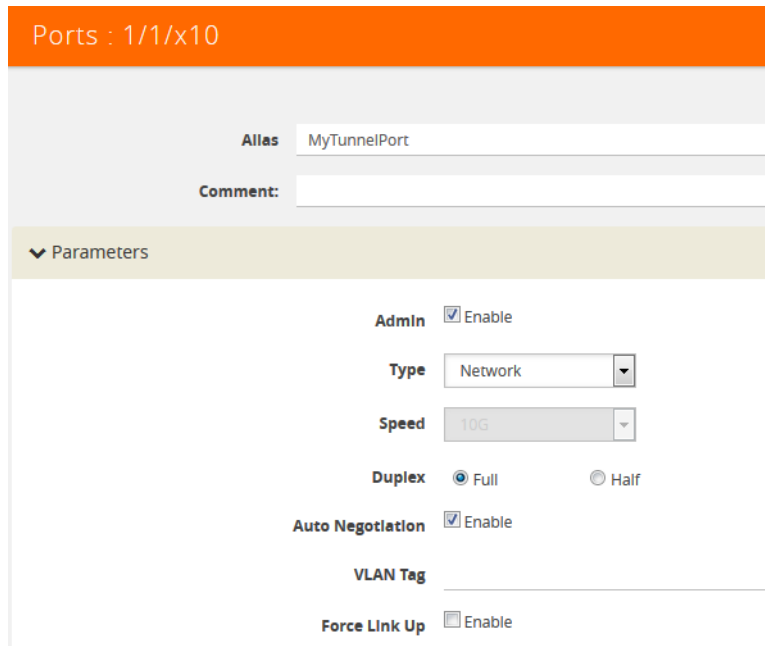   If you want to use the port on an physical node already added to GigaVUE-FM, do the following:

   a. Select **Physical Nodes** from the Navigation pane.

   b. Select the 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 Navigation pane, select **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**.

Figure 7-7 shows an example of a network port configuration.

Figure 7-7: Network Port Configuration

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**.

Figure 7-8 shows an example of a GigaSMART Group with the alias MyTunnelGSgrp and port 1/5/e1.
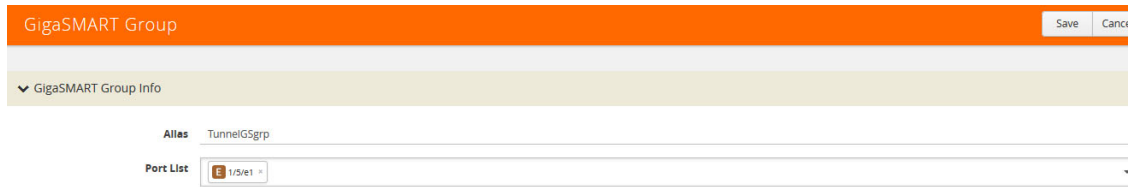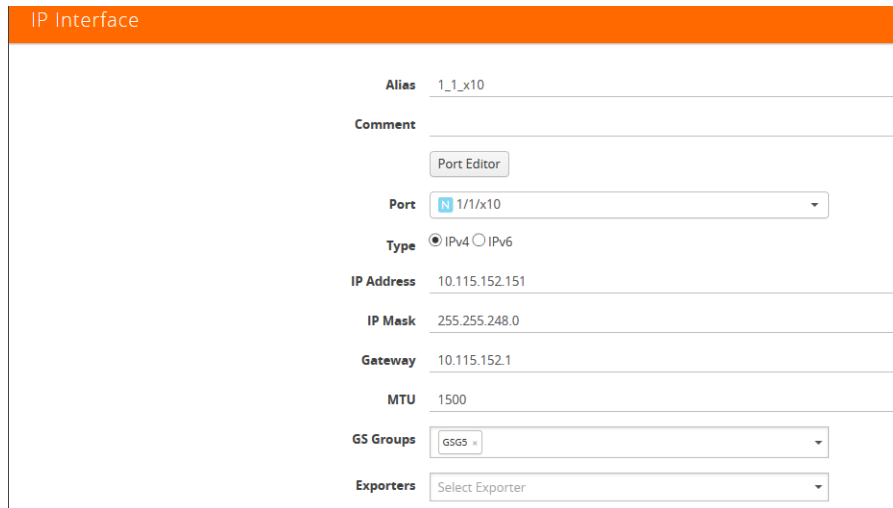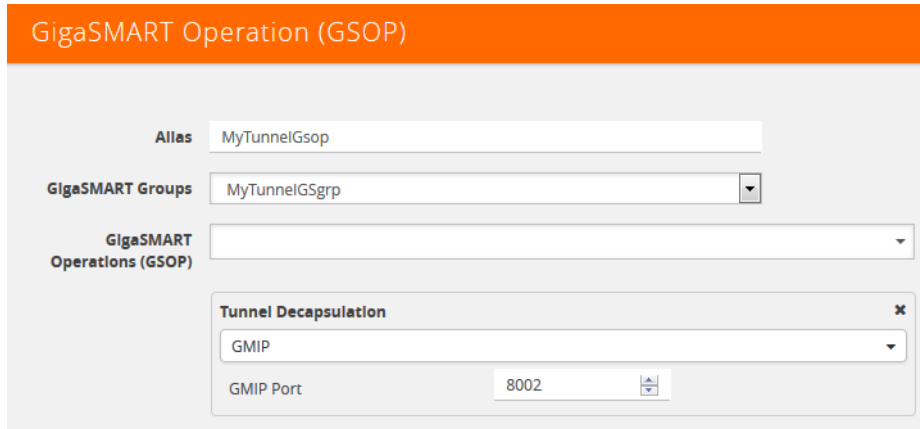

Figure 7-8: GigaSMART Group Configured

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.

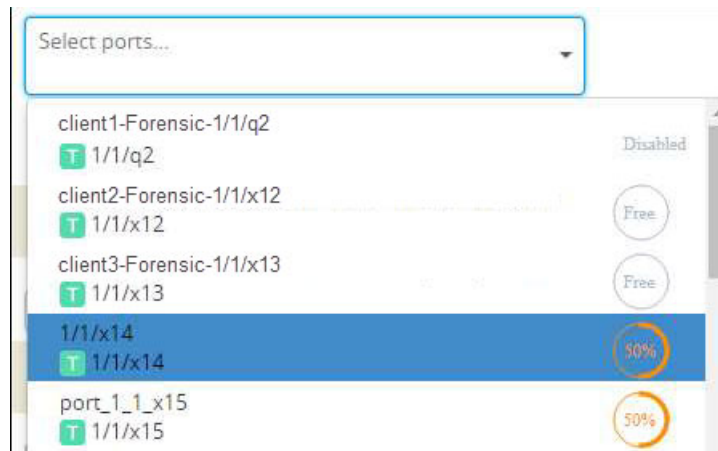**d.** Click **Save**.

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.

    a. Return to GigaVUE-FM.

    b. Under VMware vCenter, go to **Management > Tunnels Library**.

    c. Click **Add**.

    d. Select **GigaVUE**.

    e. Select the tunnel endpoint created in the previous steps and specify a **Tunnel Source Port**. Figure 7-9 shows the GigaVUE tunnel source port created in the previous steps.

Figure 7-9: Adding a Tunnel Endpoint

f. Click **OK**.

The tunnel end point is added to the Tunnels Library and can be used for the Virtual Maps. Figure 7-10shows the port in the previous step added to the Tunnels Library page.

	Destination Tunnel IP	Tunnel Source Port	Tunnel Destination Port	Tunnel Type	DSCP	Fragmentation	Physical Port	Physical Node	Physical Node Type
☐	10.115.152.151	888	8002	GMIP		disabled	1/1/x10	10.115.152.53	HC2
☐	10.115.152.150	80	8001	GMIP		disabled	1/1/x21	10.115.152.53	HC2

Total Items : 2

Figure 7-10: Tunnels Library

8 Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- *Documentation* on page 87
- *Documentation Feedback* on page 87
- *Contacting Technical Support* on page 88
- *Contacting Sales* on page 88
- *The Gigamon Community* on page 88

Documentation

Gigamon provides additional documentation for GigaVUE-VM on the Gigamon Customer Portal.

Document	Summary
GigaVUE-VM Release Notes	Summarizes new features and known issues in this release for GigaVUE-FM and GigaVUE-VM.
GigaVUE-FM User's Guide	Describes how to install, configure and operate GigaVUE-FM, the fabric management software

Documentation Feedback

To send feedback and report issues in our documentation, complete the short survey at the following link:

https://www.surveymonkey.com/r/gigamondocumentationfeedback

Contacting Technical Support

See https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information. You can also email Technical Support at support@gigamon.com.

Contacting Sales

Use the following information to contact sales:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Premium Support

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

The Gigamon Community

The Gigamon Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the Gigamon Community site to:

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

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

Register today at community.gigamon.com

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