GigaVUE Cloud Suite for Nutanix Configuration Guide

GigaVUE Cloud Suite

Product Version: 5.9.00

Document Version: 1.0

(See Change Notes for document updates.)

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
5.9.00	1.0	4/3/2020	Original release of this document with 5.9.00 GA.

Contents

GigaVUE Cloud Suite for Nutanix

This guide describes how to install, configure, and deploy the GigaVUE Cloud Suite for Nutanix in the Prism Central environment. Use this document for instructions on configuring the GigaVUE Cloud components and setting up the traffic monitoring sessions for the Nutanix.

Topics:

- Audience
- GigaVUE Cloud Suite for Nutanix
- Configure Components in Nutanix
- Configure Monitoring Sessions

Audience

This guide is intended for the users who have basic understanding of VMs and Nutanix Environment. This document expects the users to be familiar with the following terminologies that are used in this guide:

- **Cluster:** A group of nodes.
- **Node:** A node is a working machine in Nutanix cluster. Each node runs a standard hypervisor with processors, memories, and local storages.

GigaVUE Cloud Suite for Nutanix

This chapter introduces the GigaVUE Cloud Suite for Nutanix components and the supported architecture. Refer to the following sections for details:

- GigaVUE Cloud for Nutanix Components
- Supported Architecture

GigaVUE Cloud for Nutanix Components

The GigaVUE Cloud Suite for Nutanix includes the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud.
  You must have GigaVUE-FM installed either on-premises or launched from any of the supported cloud platforms. Refer to the "*GigaVUE-FM Installation and Upgrade Guide"* for details on installing and launching GigaVUE-FM.
- **GigaVUE Fabric Controller** manages multiple GVMs and orchestrates the flow of traffic from GVMs to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Fabric Controllers to communicate with the GVMs.
- **GigaVUE-VM (GVM)** is a visibility node that aggregates mirrored traffic from Nutanix hosts. It applies filters and distributes the optimized traffic to:
  - Cloud-based tools
  - On-premise tools, such as a GigaVUE H Series device

Supported Architecture

The design illustrates the Gigamon visibility in Nutanix and extend the same set of tools and policies used for the physical network to Nutanix deployed workloads.
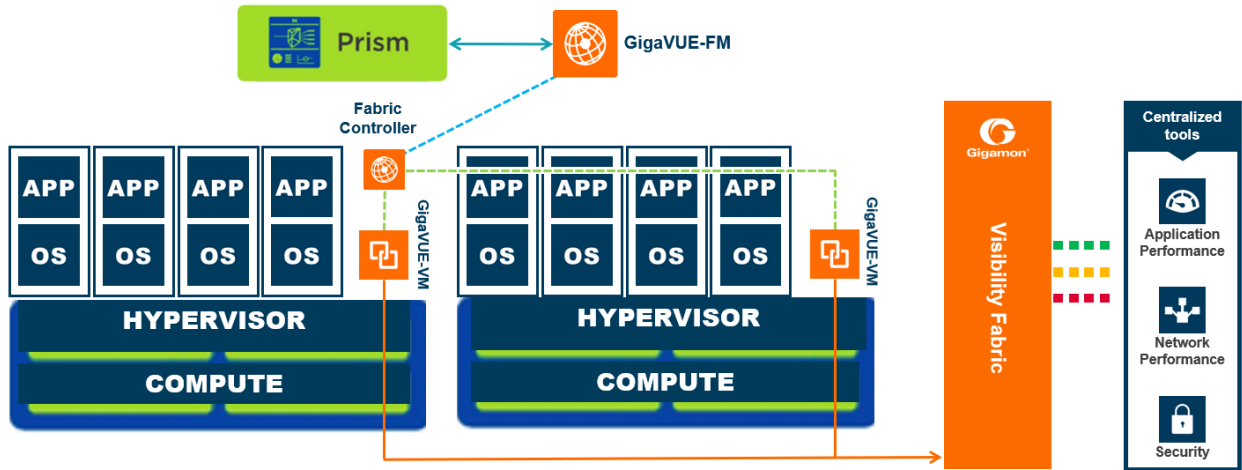
Role Based Access Control

Role Based Access Control (RBAC) controls the access privileges of users and restricts users from either modifying or viewing unauthorized data. Access privileges inGigaVUE Cloud Suite for Nutanix works on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depends on the following:

- **User role:** A user role defines permission for users to perform any task or operation
- **User group**: A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more groups.

To access the resources and to perform a specific operation in GigaVUE Cloud Suite for Nutanix you must be a user with **fm_super_admin** role or a user with write access to the following resource category depending on the task you need to perform.

Resource Category	Cloud Configuration Task
Physical Device Infrastructure Management: This includes the following cloud infrastructure resources: - Cloud Connections - Cloud Proxy Server - Cloud Fabric Deployment - Cloud Configurations - Sys Dump - Syslog - Cloud licenses - Cloud Inventory	- Configure Components in Nutanix - Connect to Nutanix
Traffic Control Management: This includes the following traffic control resources: - Monitoring session - Stats - Map library - Tunnel library - Tools library - Inclusion/exclusion Maps	- Create, Clone, and Deploy Monitoring Session - Add Applications to Monitoring Session - Create Maps - View Statistics - Create Tunnel End Points

> **NOTE:** Cloud APIs are also RBAC enabled.

Refer to the GigaVUE Administration Guide for detailed information about Roles, Tags, User Groups.

Configure Components in Nutanix

This chapter describes how to configure GVMs, and GigaVUE® Fabric Controllers in your environment. Refer to the following sections for details:

- Before You Begin
- Launch GigaVUE-FM Instance
- Configure GigaVUE Cloud for Nutanix Components

Before You Begin

This section describes the requirements and prerequisites to configure the GigaVUE Cloud Suite for Nutanix. Refer to the following section for details.

- Prerequisites
- Minimum Compute Requirements
- Network Firewall Requirements

Prerequisites

The following are the prerequisites for configuring GigaVUE-FM and fabric images in Nutanix.

- If the Gigamon fabric VMs (Fabric Controller and GigaVUE-VM) are deployed on multiple clusters, the management network selected during configuration must have the same name on all clusters.
- You must upload the GigaVUE-FM image and fabric image (Fabric Controller and GVM) files in the Prism Central repository. Do not use the Prism Element to upload the GigaVUE-FM image and fabric image files.
- Assigning a Static IP on Gigamon Fabric Nodes is not supported and the management subnet selection must be DHCP enabled.
- Only one GVM can be deployed per Nutanix Node.

- A Fabric Controller can be shared among GVMs on multiple clusters as long as there is network connectivity

- The GVM does not support any GigaSMART applications in Nutanix for GigaVUE-FM version 5.8.

- For GigaVUE FM to orchestrate the solution, the minimum requirement that the Nutanix admin account must be a **Prism Central Admin** on Prism Central and a **Cluster Admin** on individual clusters. The password must set to be the same across the environment if they are locally managed. Alternatively, if the Nutanix Prism Central is configured with external authentication like AD/LDAP then you can avoid replicating the manual password creation across the environment.
- While uploading the fabric images in Nutanix, ensure that the file names of the Fabric images have,
  - "gigamon-fabric-cntlr-1.7-1" as the Fabric Controller filename.
  - "gigamon-gvm-nutanix-1.7-1" as the GVM filename.

Minimum Compute Requirements

The minimum recommended computing requirements are listed in the following table.

Compute Instances	vCPU	Memory	Disk Space	Description
GigaVUE-VM	2 vCPU	4GB	1 x 12GB	NIC 1: Management IP + vTAP interfaces
GigaVUE® Fabric Controller	1 vCPU	1GB	1 x 10GB	Based on the number of GVMs being monitored, multiple fabric controllers are required to scale out horizontally
GigaVUE-FM	2 vCPU	16GB	2 x 40GB	GigaVUE-FM must be able to access the controller instance for relaying the commands.

Network Firewall Requirements

Following are the Network Firewall Requirements for Gigamon fabrics for Nutanix deployments.

Table 1: Network Firewall Requirements

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM Inside Nutanix					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allows GVMs, GigaVUE Fabric Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM

Direction	Type	Protocol	Port	CIDR	Purpose
Inbound	SSH	TCP	22	Anywhere Any IP	Allows GVMs, GigaVUE Fabric Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP	9902	GigaVUE Fabric Controller IP	Allows GigaVUE-FM to communicate with GigaVUE Fabric Controllers
GigaVUE Fabric Controller					
Inbound	Custom TCP Rule	TCP	9902	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE Fabric Controllers
GVM					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE Fabric Controller IP	Allows GigaVUE Fabric Controllers to communicate with GVMs

Upload Fabric Images

The recent GVM, and Fabric Controller qcow2 image files can be downloaded from Gigamon Customer Portal. After fetching the images, upload the fabric images to Prism Central. Select all the available clusters as placements while uploading fabric images.

While uploading images to Nutanix, the names of the image files should be of the following format:

- gigamon-fabric-cntlr-1.7-1
- gigamon-gvm-nutanix-1.7-1

Once the images are uploaded, you can view the images under **Virtual Infrastructure > Images** in the Nutanix console.

> **NOTE:** The GVM and Fabric Controller images are built with identical username (ubuntu) and password (ubuntu). You must change the password when you first login to the GVMs and Fabric controllers.
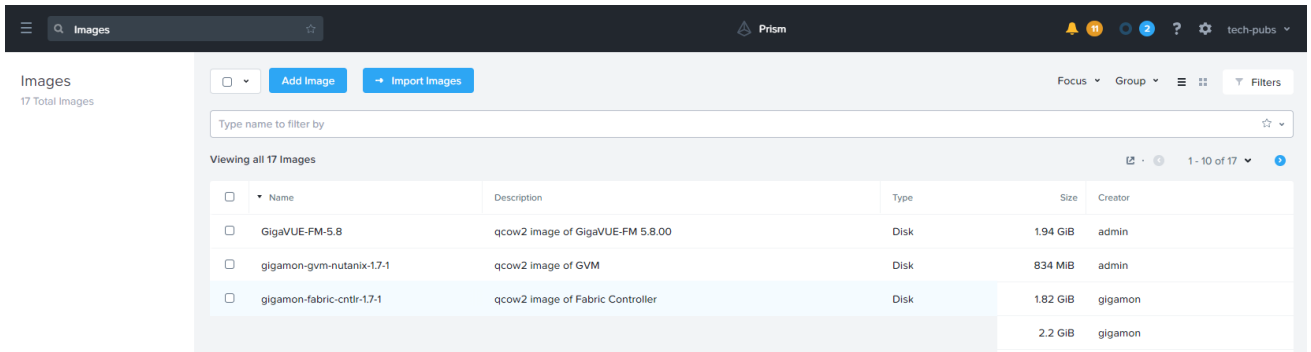
Figure 1: Upload Fabric Images in Prism Central

Launch GigaVUE-FM Instance

To launch the GigaVUE-FM instance from the Prism Central:

1. Log in to Prism Central.
2. In Prism Central, select **Dashboard > Virtual Infrastructure > VMs**. The VMs page appears.
3. On the VMs page, click **Create VM**. The **Create VM** window appears.

> **NOTE:** If the device has more than one cluster, select the required cluster in the **Cluster Selection** window.

4. Enter or select the values as described in the following table.

Field	Description
General Configuration	• **Name**—name for the VM. • **Description**—description for the VM. • **Timezone**—time zone from the drop-down list.
Compute Details	• **vCPU(s)**—number of vCPUs required. • **Number Of Cores Per vCPU**—number of cores per vCPU. • **Memory**—memory size of the vCPU(s). Minimum value is 8GiB.
Disks	Add, edit or delete the disks. Add the GigaVUE-FM qcow2 disk image and a Container (second disk), minimum of 40GB for the VM. You must select the fabric image as Boot Device.
Network Adapters (NIC)	Add, edit or delete the NIC.
VM Host Affinity	Set Affinity by choosing the required nodes to run GigaVUE-FM or a particular VM.

5. Click **Save** and the new VM appears in the VMs list with the **Power State** as **Off**.

6. Select the new VM and then select **Actions > Power On**. The new VM is now Active.
7. Select the new VM and then select **Actions > Launch console**. The GigaVUE-FM console appears.
8. Log in to the GigaVUE-FM console as admin with the default password admin123A! and you are requested to change the password.

Configure GigaVUE Cloud for Nutanix Components

You must establish a connection between GigaVUE-FM and your Prism environment before you can perform the configuration steps for GVM and Fabric Controller. After a connection is established, you can use GigaVUE-FM to specify a launch configuration for the GVMs, and GigaVUE Fabric Controllers.

Refer to the following sections for details:
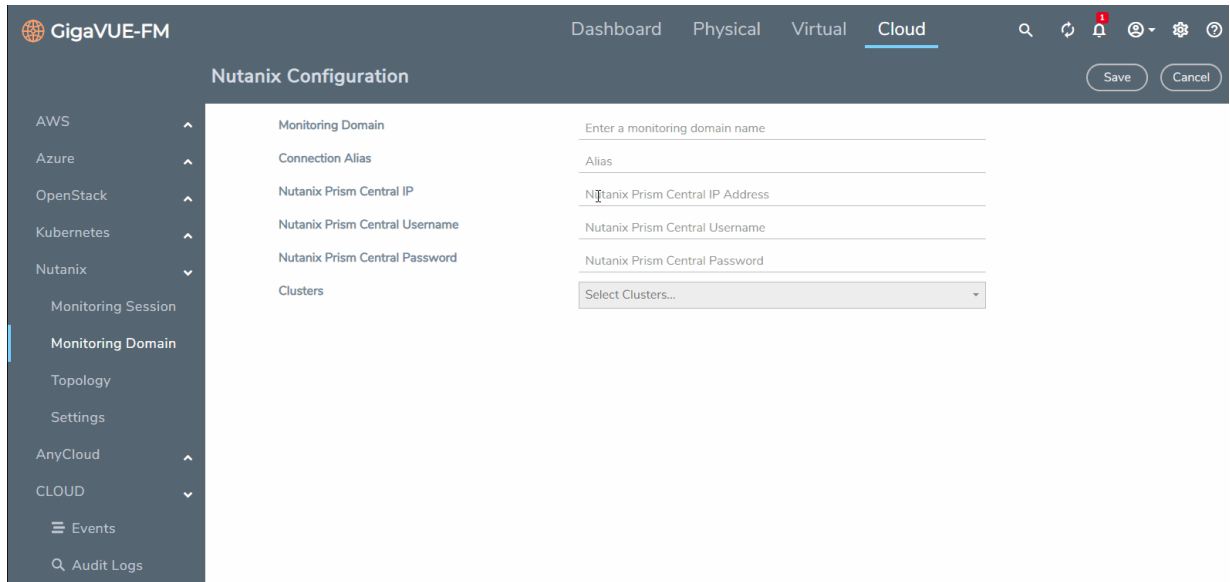
- Connect to Nutanix
- Nutanix Fabric Launch Configuration

Connect to Nutanix

To configure Nutanix in GigaVUE-FM:

1. In GigaVUE-FM, on the top navigation bar, select **Cloud**.
2. On the left navigation pane, select **Nutanix > Monitoring Domain**. The Monitoring Domain page appears.
3. On the Monitoring Domain page, click **New**. The Nutanix Configuration page appears.

4. In the Nutanix Configuration page, enter or select the following details:

Field	Description
Monitoring Domain	Name of the monitoring domain.
Connection Alias	Name of the connection.
Nutanix Prism Central IP	IP address of the Prism Central.
Nutanix Prism Central Username	Username of the Prism Central User with admin role privilege.
Nutanix Prism Central Password	Prism Central Password used to connect to the Nutanix.
Cluster	Clusters that need to be monitored

5. Click **Save**. The Nutanix Fabric Launch Configuration page appears.

Nutanix Fabric Launch Configuration

The fabric images (Fabric controller and GVM) are launched by GigaVUE-FM based on the configuration made in Nutanix Fabric Launch Configuration page.

GigaVUE Fabric Controller manages multiple GVMs and orchestrates the flow of traffic from GVMs to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Fabric Controllers to communicate with the GVMs.

To configure the Nutanix Fabric Images in GigaVUE-FM, do the following:

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

2. On the Nutanix Fabric Launch Configuration page, enter or select the following information.

Field	Description
Cluster	Select the cluster where the Fabric controller and GVM are to be deployed.
Fabric Controller	**Version**—Select a Fabric Controller image file (gigamon-fabric-cntlr-1.7-1). Refer to Upload Fabric Images for more information. **Manangement Subnet**—The subnets registered in Prism Central are listed. Select a management subnet as specified in the Prerequisites. **Cloud-init User Data (Optional)**—Enter cloud-init user data (YAML, JSON, or Shell script) A Fabric Controller can be shared among GVMs on multiple clusters as long as there is network connectivity. Minimum one Fabric Controller must be configured in a cluster.
GVM	**Hosts**—Select a node or multiple nodes from the selected Cluster. **Version**—Select a GVM image file (gigamon-gvm-nutanix-1.7-1). Refer to Upload Fabric Images for more information. **Manangement Subnet**—The subnets registered in Prism Central are listed. Select a management subnet as specified in the Prerequisites. **Data Subnets**—Select the subnet(s) based on the required VMs and vNICs. Click **Add Subnet** to add additional Subnets. **Memory Size (GB)**—Enter the memory size of the vCPU(s) **Disk Size (GB)**—Enter the image size of the GVM. **Number of vCPUs**—Enter the number of vCPUs required. **Tunnel MTU**—Enter the Tunnel MTU size. **Cloud-init User Data (Optional)**—Enter cloud-init user data (YAML, JSON, or Shell script)

3. Click **Save & Configure Next Cluster** to configure next Cluster,
Or
Click **Save & Exit** to initiate the deployment of the selected fabric images. You can view the status of the deployment on the Tasks page of Prism Central.

Configure Monitoring Sessions

This chapter describes how to setup tunnel endpoints in a monitoring session to receive and send traffic to the GVM. It also describes how to filter and send the traffic from the GVM to the various monitoring tools.

Refer to the following sections for details:

- Overview of Visibility Components
- Create Tunnel Endpoints
- Create Monitoring Session
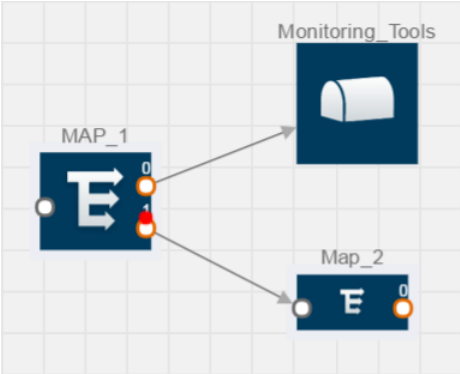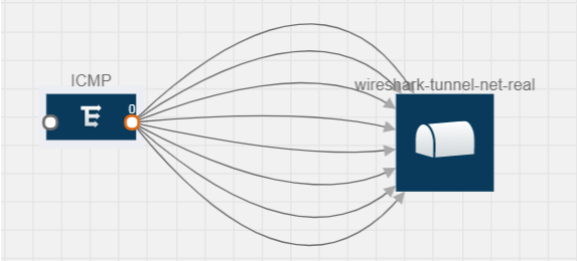- Configure Nutanix Settings

Overview of Visibility Components

The GVM aggregates the traffic from Nutanix platform and filters it using maps.

The following table lists the components of the monitoring session:

Table 1: Components of Traffic Visibility Sessions

Parameter	Description
Map	A map (M) is used to filter the traffic flowing through the GVM. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.
Rule	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic. A rule is also associated with priority and action set.
Priority	A priority determines the order in which the rules are executed. The greater the value, the higher the priority. The priority value can range from 0 to 99.
Action Set	An Action Set is an exit point in a map that you can drag and create links to the other maps and monitoring tools. A single map can have multiple action sets. A single action set can have multiple links connecting to maps. You can create an Action Set when you create a rule for a map. In the following example, Map 1 has two action sets: Action Set 0 and Action Set 1. The packets that match the rules in Action Set 0 are forwarded to monitoring tools. The packets that match the rules in Action Set 1 are forwarded to Map 2.

Parameter	Description
	 Figure 1: Action Set A single action set can have up to 8 links connecting the same destination point. The same packets from the map are replicated in 8 different links. *Figure 2: Action Set with Multiple Links*
Link	A link directs the packets to flow from a map to the destination. The destination could be the other maps and the monitoring tools.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Target	A target determines the instances that are to be monitored. Targets are determined based on the following formula:
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the maps, inclusion maps, and exclusion maps in the monitoring session.
Tunnel	A tunnel lists the monitoring tools to which the traffic matching the filtered criteria is routed.

Create Tunnel Endpoints

Traffic from the GVM is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE or VXLAN tunnel.

To create a tunnel endpoint:

1. In GigaVUE-FM, on the top navigation bar, select **Cloud**.
2. On the left navigation pane, select **Nutanix > Settings.**
3. Select the **Tunnel Spec Library** tab. The **Tunnel Library** page appears.
4. On the Tunnel Library page, click **New**. The **Add Tunnel Spec** page appears.
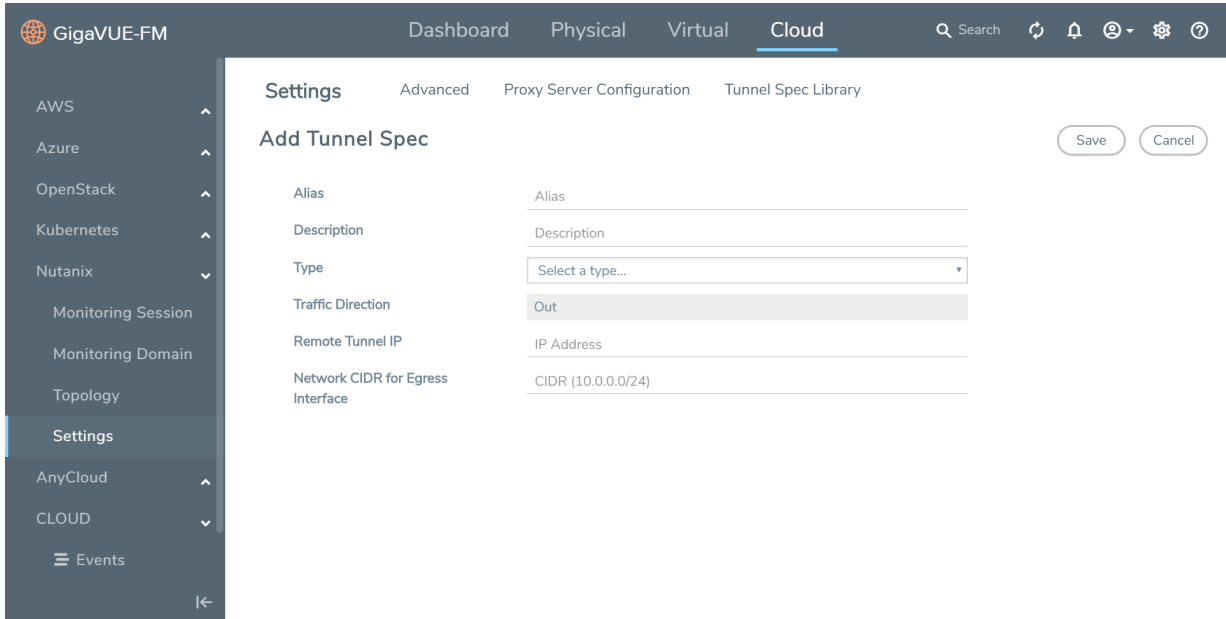
5. On the Add Tunnel Spec page, select or enter the required information as described in the following table.

Field	Description
Alias	Enter a name for the tunnel endpoint.
Description	Enter any required details or comments for the tunnel endpoint.
Type	Select the tunnel type (L2GRE or VXLAN).
Traffic Direction	The direction of the traffic flowing through the GVM. By default the value is set as **Out**.
Remote Tunnel IP	The IP address of the tunnel destination endpoint.
Network CIDR for Egress Interface	Specify the CIDR of the egress interface through which the mirrored traffic is exported (routed) to reach the tunnel endpoint.

6. Click **Save** and a new Tunnel Endpoint is created.
7. Select **Nutanix > Settings > Tunnel Spec Library** and verify that the tunnel endpoint is added to GigaVUE-FM.

Create Monitoring Session

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

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

To design your monitoring session, refer to the following sections:

- Create New Session
- Clone Monitoring Session
- Create Map
- Deploy Monitoring Session
- View Statistics
- View Topology

Create New Session

You can create multiple monitoring sessions within a single connection.

To create a new session:

1. In GigaVUE-FM, on the top navigation bar, select **Cloud**.
2. Select **Nutanix > Monitoring Session**. The Monitoring Sessions page appears.
3. Click **New**. The **Create a New Monitoring Session** dialog box appears.

4. In the Create a New Monitoring Session dialog box, enter the required information as described in the following table.

Field	Description
Alias	Enter a name for the monitoring session.
Monitoring Domain	Select an existing monitoring domain. The Connection field appears on selecting a monitoring domain.
Connection	Select the required connections.

5. Click **Create** and a new monitoring session is created.

Clone Monitoring Session

You can clone an existing monitoring session.

To clone a monitoring session:

1. In the **Monitoring Session** page, select the monitoring session that you need to clone.
2. Click **Clone**. The **Clone Monitoring Session** dialog box appears.
3. In the Clone Monitoring Session dialog box, enter the required information as described in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain.

4. Click **Create** to create the cloned monitoring session.
5. Once the monitoring session is created, click **Edit** to add connections to the cloned monitoring session.

Create Map

Each map can have up to 32 rules associated with it. The following table lists the various rule conditions that you can select for creating a map, inclusion map, and exclusion map.

Table 3: Conditions for the Rules

Conditions	Description
L2, L3, and L4 Filters	
Ether Type	The packets are filtered based on the selected ethertype. The following conditions are displayed: • IPv4 • ARP • RARP • Other **L3 Filters** If you choose IPv4, the following L3 filter conditions are displayed: • Protocol • IP Fragmentation • IP Time to live (TTL) • IP Type of Service (TOS) • IP Explicit Congestion Notification (ECN) • IP Source • IP Destination **L4 Filters** If you select TCP or UDP protocol, the following L4 filter conditions are displayed: • Port Source • Port Destination
MAC Source	The egress traffic matching the specified source MAC address is selected.
MAC Destination	The ingress traffic matching the specified destination MAC address is selected.
VLAN	All the traffic matching the specified IEEE 802.1q Virtual LAN tag is filtered. Specify a number from 0 to 4094.
VLAN Priority Code Point (PCP)	All the traffic matching the specified IEEE 802.1q Priority Code Point (PCP) is filtered. Specify a value between 0 to 7.
VLAN Tag Control Information (TCI)	All the traffic matching the specified VLAN TCI value is filtered. Specify the exact TCI value.
Pass All	All the packets coming from the monitored VMs are passed through the filter. When Pass All is selected, the L3 and L4 filters are disabled.

When you select a condition without source or destination specified, then both egress and ingress traffic is selected for tapping the traffic. For example, if you select Ether Type as IPv4, TCP as the protocol, and do not specify IPv4 source or destination, then both egress and ingress traffic is selected for monitoring purpose.

When you select a condition with either source or destination specified, it determines the direction based on the selection.

> **NOTE:** You can create Inclusion and Exclusion Maps using all default conditions except Ether Type and Pass All.

To create a new map:

1. Select **Nutanix > Monitoring Session**.
2. Click **New**. The Monitoring Sessions page appears.
3. Create a new session. Refer to Create Monitoring Session.
4. Select **New > New Map**, drag and drop a new map template to the workspace. The **New Map** quick view appears.

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

Parameter	Description
Alias	The name of the new map.
Comments	The description of the map.

Map Rules	The rules for filtering the traffic in the map.
	 To add a map rule:
	   a. Click **Add a Rule**.
	   b. Select a condition from the **Search L2 Conditions** drop-down list and specify a value. Based on this selection, the Search L3 Conditions drop-down list is automatically updated.
	   c. Select a condition from the **Search L3 Conditions** drop-down list and specify a value.
	   d. (Optional) If you have selected TCP or UDP as the protocol in the L3 conditions, then select Port Source or Port Destination from the Search L4 Conditions drop-down list and specify a value. If you have selected conditions other than TCP or UDP, then the Search L4 Conditions drop-down list is disabled.
	   e. (Optional) In the Priority and Action Set box, assign a priority and action set.
	   f. (Optional) In the Rule Comment box, enter a comment for the rule.
	
	 NOTE:
	 • Repeat steps **b** through **f** to add more conditions.
	 • Repeat steps **a** through **f** to add nested rules.

NOTE: Do not create duplicate map rules with the same priority.

6. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
   - Select an existing group from the **Select Group** list and click **Save**.
   - Enter a name for the new group in the **New Group** field and click **Save**.

NOTE: The maps saved in the Map Library can be reused in any monitoring session created in the connection.

7. Click **Save**.

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

- Click a map and select **Details** to edit the map or select **Delete** to delete the map.
- Click the **Show Targets** button to view the monitoring targets highlighted in orange.
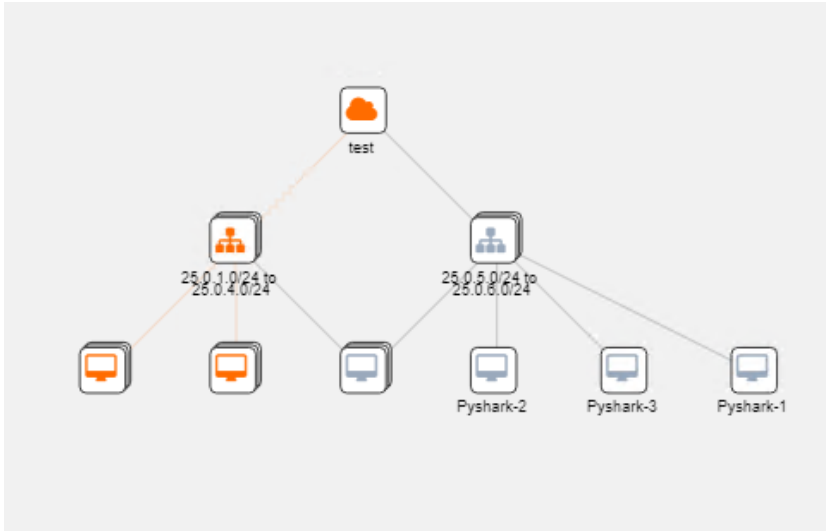
- Click to expand the **Targets** dialog box. Click to change the view from the Topology view to the targets view. To view details about a GVM, click the arrow next to the VM.
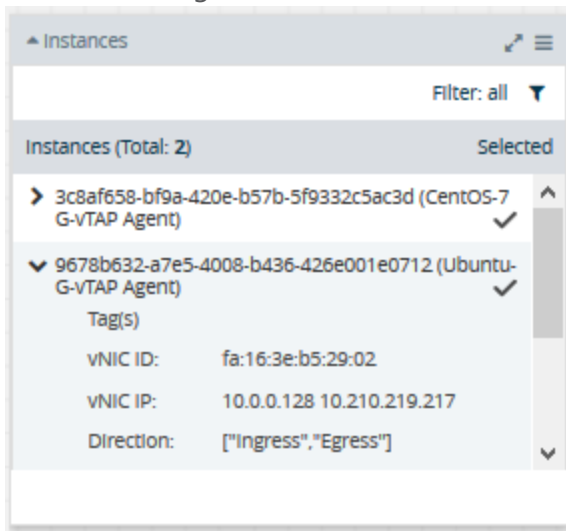
- In the Instances window, click

Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop one or more maps from the **MAP LIBRARY** section to the canvas.
2. (Optional) To add Inclusion and Exclusion maps, drag and drop the maps from the Map Library to their respective section at the bottom of the workspace.

3. Drag and drop one or more tunnels from the **TUNNELS** section to the canvas.
4. Hover your mouse on the map, click the red dot, and drag the arrow over to another map, or tunnel.

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

5. Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
6. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all GVMs. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Partial Success—The session is not deployed on one or more instances due to GVM failure.
   - Failure—The session is not deployed on any of the GVMs.

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

The Monitoring Session page also has the following buttons:

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

View Statistics

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

On the Monitoring Sessions page, click **View** in the Statistics column to view the Monitoring Session Statistics page.

The Monitoring Session Statistics page appears where you can analyze incoming and outgoing traffic.

Directly below the graph, you can click on **Incoming Maps**, **Outgoing Maps**, or **Ratio (Out/In)** to view the statistics individually.

At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.

On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a Quick View for that item to see more details about the incoming and outgoing traffic for that item.

You can also scroll down the Map Statistics Quick View to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the Quick View.

View Topology

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

To view the topology diagram:

1. Select **Nutanix > Topology**. The Topology page appears.
2. Select a connection from the **Select connection...** drop-down list. The topology view of the subnets and instances are displayed.
3. (Optional) Select a monitoring session from the **Select monitoring session...** drop-down list. The monitored subnets and instances change to blue.
4. Select one of the following check boxes:

   - **Fabric**—Displays the topology view of the Fabric VMs.

   - **Monitored**—Displays the topology view of the selected target interfaces that are being monitored.

   - **Not Monitored**—Displays the topology view of the interfaces that are not being monitored.

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

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

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

Configure Nutanix Settings

To configure the Nutanix Settings:

1. In GigaVUE-FM, on the top navigation bar, select **Cloud**.
2. On the left navigation pane, select **Nutanix > Settings > Advanced.**
3. In the **Advanced** tab of the Settings page, click **Edit** to edit the Settings fields. Refer to the following table for descriptions of the Settings fields:

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of connections you can establish in GigaVUE-FM.
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the state of target VMs in Nutanix.

Additional Sources of Information

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

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The Gigamon Community

Documentation

The following table provides a list of the additional documentation provided for GigaVUE H Series and TA Series nodes. "*" indicates new documents in this release. "**" indicates documents that are renamed in this release.

> **NOTE**: Release Notes are not included in the online documentation. Registered Customers can download the Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download PDFs from My Gigamon.

> **TIP**: If you keep all PDFs for a particular release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.

Table 1: Documentation Suite for Gigamon Products

Summary	Document
• complete doc set for the respective release, minus Release Notes, in a zip file	**All-Documents Zip**
• how to unpack, assemble, rack-mount, connect, and initially configure the respective GigaVUE devices • reference information and specifications for the respective GigaVUE devices	**GigaVUE-HC1 Hardware Installation Guide**
	GigaVUE-HC2 Hardware Installation Guide
	GigaVUE-HC3 Hardware Installation Guide
	GigaVUE TA Series Hardware Installation Guide
Software Installation and Upgrade Guides	
• how to install GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM • how to migrate GigaVUE-FM on VMware ESXi, Hardware Appliance, and AWS	****GigaVUE-FM Installation and Migration Guide**
• how to upgrade the embedded GigaVUE-OS on GigaVUE H Series and GigaVUE TA Series nodes	**GigaVUE-OS Upgrade Guide**
Administration Guide	
• how to administer the GigaVUE-OS and GigaVUE-FM software	**GigaVUE-OS and GigaVUE-FM Administration Guide**
Configuration and Monitoring Guides	
• how to install, deploy, and operate GigaVUE Cloud Suite • how to configure GigaSMART operations	**GigaVUE-FM User's Guide**
• how to deploy the GigaVUE Cloud Suite solution in any cloud platform	**GigaVUE Cloud Suite for AnyCloud Configuration Guide**

Summary	Document
• how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the respective cloud platform	**GigaVUE Cloud Suite for AWS Configuration Guide**
	GigaVUE Cloud Suite for AWS QuickStart Guide
	***GigaVUE Cloud Suite for AWS SecretRegions Configuration Guide**
	GigaVUE Cloud Suite for Azure Configuration Guide
	GigaVUE Cloud Suite for Kubernetes Configuration Guide
	***GigaVUE Cloud Suite for Nutanix Configuration Guide**
	GigaVUE Cloud Suite for OpenStack Configuration Guide
	GigaVUE Cloud Suite for VMware Configuration Guide
Reference Guides	
• library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices	**GigaVUE-OS-CLI Reference Guide**
• guidelines for the different types of cables used to connect Gigamon devices	**GigaVUE-OS Cabling Quick Reference Guide**
• compatibility information and interoperability requirements for Gigamon devices	**GigaVUE-OS Compatibility and Interoperability Matrix**
• samples uses of the GigaVUE-FM Application Program Interfaces (APIs) **NOTE:** Content will be merged into the GigaVUE-FM User's Guide in a future release.	**GigaVUE-FM REST API Getting Started Guide**
Release Notes	
• new features, resolved issues, and known issues in this release • important notes regarding installing and upgrading to this release **NOTE:** In 5.7.00, the Release Notes documents combines GigaVUE-OS, GigaVUE-FM, and GigaVUE Cloud Suite into one document.	**GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, and GigaVUE Cloud Suite Release Notes**

Summary	Document
In-Product Help	
• how to install, deploy, and operate GigaVUE Cloud Suite. Provided from the GigaVUE Cloud Suite interface.	**GigaVUE-FM Online Help**
• the web-based GUI for the GigaVUE-OS. Provided from the GigaVUE-OS H-VUE interface.	**GigaVUE-OS H-VUE Online Help**

> **NOTE:** Registered customers can log in to My Gigamon to download documentation for specific releases under Software & Documentation Downloads. Refer to How to Download PDFs from My Gigamon.

How to Download PDFs from My Gigamon

To download release-specific PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Documentation** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.7," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.7.xx.

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

Contact 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.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

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

Register today at community.gigamon.com

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