



GigaVUE Cloud Suite for Nutanix Guide— GigaVUE-VM Guide

GigaVUE Cloud Suite

Product Version: 6.4

Document Version: 1.0

Last Updated: Thursday, September 7, 2023

(See Change Notes for document updates.)

Copyright 2023 Gigamon Inc.. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.4.00	1.0	09/08/2023	The original release of this document with 6.4.00 GA.

Contents

GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite for Nutanix	5
Audience	5
About GigaVUE Cloud Suite for Nutanix	6
Components of GigaVUE Cloud Suite for Nutanix	6
Architecture of GigaVUE Cloud Suite for Nutanix	7
Role Based Access Control	7
Configure Components in Nutanix	9
Before You Begin	9
Prerequisites	9
Minimum Compute Requirements	10
Network Firewall Requirements	10
Upload Fabric Images	11
Install GigaVUE-FM on Nutanix	11
Deploy GigaVUE Cloud Suite for Nutanix	13
Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM	13
Nutanix Fabric Launch Configuration	13
Configuring Monitoring Domain	14
Nutanix Fabric Launch Configuration	16
Configure and Manage Resources	18
Visibility Components	18
Monitoring Session	19
Configure Nutanix Settings	26
Additional Sources of Information	27
Documentation	27
How to Download Software and Release Notes from My Gigamon	29
Documentation Feedback	30
Contact Technical Support	31
Contact Sales	31
Premium Support	32
The VUE Community	32

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 Suite Cloud components and setting up the traffic monitoring sessions for the Nutanix.

Topics:

- [About GigaVUE Cloud Suite for Nutanix](#)
- [Configure Components in Nutanix](#)
- [Deploy GigaVUE Cloud Suite for Nutanix](#)

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.

About 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:

- [Components of GigaVUE Cloud Suite for Nutanix](#)
- [Architecture of GigaVUE Cloud Suite for Nutanix](#)
- [Role Based Access Control](#)

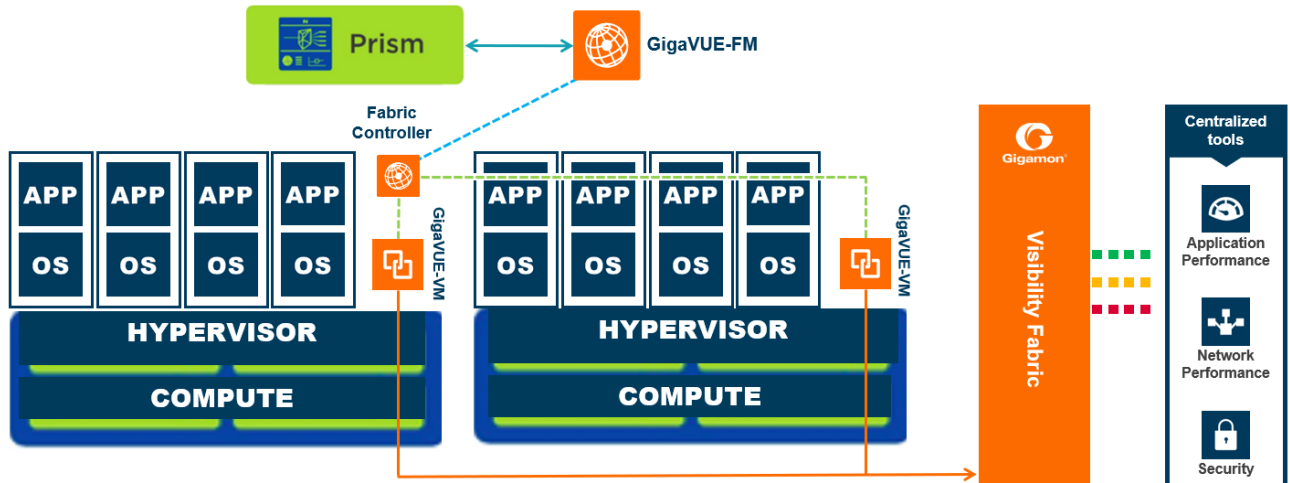
Components of GigaVUE Cloud Suite for Nutanix

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

Architecture of GigaVUE Cloud Suite for Nutanix

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

The Role Based Access Control (RBAC) feature controls the access privileges of users and restricts users from either modifying or viewing unauthorized data. Access privileges in GigaVUE Cloud Suite 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 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
<p>Physical Device Infrastructure Management: This includes the following cloud infrastructure resources:</p> <ul style="list-style-type: none"> • Cloud Connections • Cloud Fabric Deployment • Cloud Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory 	<ul style="list-style-type: none"> • Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric
<p>Traffic Control Management: This includes the following traffic control resources:</p> <ul style="list-style-type: none"> • Monitoring session • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps 	<ul style="list-style-type: none"> • 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 GigaVUE V Series Node and GigaVUE V Series Proxy in your environment. Refer to the following sections for details:

- [Before You Begin](#)
- [Upload Fabric Images](#)
- [Install GigaVUE-FM on Nutanix](#)
- [Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM](#)

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.

- You must upload the GigaVUE-FM image and fabric image (GigaVUE® V Series Node) 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 for GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller is not supported. DHCP must be enabled for the management subnet and tunnel subnet.
- Only one GigaVUE® V Series Node can be deployed per Nutanix Node.
- For GigaVUE Cloud Suite-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.
- Ensure that appropriate Nutanix fabric images are uploaded.
- You must create a subnet and security group. For more information on creating a subnet, see [Configuring Network Connections](#).

Default Login Credentials

You can login to the GigaVUE V Series Node, GigaVUE V Series proxy, and UCT-V Controller by using the default credentials.

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!
GigaVUE V Series proxy	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!
UCT-V Controller	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: gigamon Password: Gigamon123!

Minimum Compute Requirements

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

Compute Instances	vCPU	Memory	Disk Space	Description
GigaVUE-FM	2 vCPU	16GB	2 x 40GB	GigaVUE-FM must be able to access the V Series Nodes directly or a GigaVUE V Series Proxy that will relay the commands to the GigaVUE V Series Nodes.

Network Firewall Requirements

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

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM Inside Nutanix					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allow GVMs, GigaVUE Cloud Suite fabric controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allow GVMs, GigaVUE Cloud Suite fabric controllers, and

Direction	Type	Protocol	Port	CIDR	Purpose
					GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP	9902	GigaVUE Cloud Suite Fabric Controller IP	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite Fabric Controllers IP.
GigaVUE Cloud Suite Fabric Controller					
Inbound	Custom TCP Rule	TCP	9902	GigaVUE-FM IP	Allows GVM to communicate with GigaVUE Cloud Suite Fabric Controllers.
Outbound	Custom TCP Rule	TCP	9903	GVM IP Subnet	Allows GigaVUE Cloud Suite Fabric Controller to communicate with GVMs.
GVM					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE Cloud Suite Fabric Controller IP	Allows GigaVUE Cloud Suite Fabric Controller IP to communicate with GVMs.
Outbound	Custom UDP Rule	UDP	<ul style="list-style-type: none"> VXLAN (default 4789) L2GRE (IP 47) 	Tool IP	Allows GVM to communicate and tunnel traffic to the tool
Outbound	Custom ICMP Rule	ICMP	-	Tool IP	Allows GVM to health check the tool traffic.

Upload Fabric Images

The recent GigaVUE V Series Node and GigaVUE-FM image file 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.

Upload the appropriate Nutanix image file.

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

Install GigaVUE-FM on Nutanix

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

1. Log in to the [Gigamon Customer Portal](#) and click on Software and Release Notes.
2. Then, search **qcow2** in the search file field.
3. Use the **Filter by** option to filter your search by Product, Release, Release Type and Release date. Select GigaVUE-FM as the product, and then enter the release version in the release field.
4. The QCOW2 file appears in the list view. Click on the latest QCOW2 file to download it.
5. Log in to Prism Central.
6. In Prism Central, select **Dashboard > Virtual Infrastructure > VMs**. The VMs page appears.

NOTE: You can view the uploaded images under **Virtual Infrastructure > Images**. For more detailed information on how to upload fabric images refer Upload Fabric Images topic in the *GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide*.

7. 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.

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

Field	Description
General Configuration	<ul style="list-style-type: none"> • Name—Enter a name for the VM. • Description—Enter description for the VM. (optional) • Timezone—Select the time zone from the drop-down list.
Compute Details	<ul style="list-style-type: none"> • vCPU(s)—number of vCPUs required. Minimum value is 2vCPUs. However, the recommended value is 4vCPUs. • Number Of Cores Per vCPU—number of cores per vCPU. • Memory—memory size of the vCPU(s). Minimum value is 16GB.
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. Select the primary image (GigaVUE-FM qcow2) as Boot Device.
Network Adapters (NIC)	Add a minimum of 1 vNIC for traffic management.
VM Host Affinity (Optional)	Set Affinity by choosing the required nodes to run GigaVUE-FM or a particular VM.

9. Click **Save** and the new VM appears on the VMs list with the **Power State** as **Off**.
10. Select the new VM and then select **Actions > Power On**. The new VM is now Active.
11. Select the new VM and then select **Actions > Launch console**. The GigaVUE-FM console appears.
12. Log in to the GigaVUE-FM console as admin with the user name as admin and default password admin123A!! and you are requested to change the password.

NOTE: You can also choose to perform the IP Networking and NTP configurations by running the **fmctl jump-start** command after you power on the GigaVUE-FM instance. Refer to Perform Network Configurations topic in the *GigaVUE-FM Installation and Upgrade Guide* for more details on how to use **fmctl jump-start** to perform the initial network configuration.

You can also log in to GigaVUE-FM by logging in to WebUI using the configured IP address using the default user name **admin** and the default password **admin123A!!**.

Deploy GigaVUE Cloud Suite for Nutanix

This section describes how to connect, launch, and deploy fabric components of GigaVUE Cloud Suite for Nutanix.

Refer to the following sections for details:

- [Install GigaVUE-FM on Nutanix](#)
- [Create a Monitoring Domain](#)
- [Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM](#)
- [Configure Monitoring Sessions](#)

Configure GigaVUE Cloud Suite Fabric Components in GigaVUE-FM

You must establish a connection between GigaVUE-FM and your Prism environment before you can perform the configuration steps for GigaVUE® V Series Node and GigaVUE V Series Proxy. After a connection is established, you can use GigaVUE-FM to specify a launch configuration for the GigaVUE® V Series Nodes.

Nutanix Fabric Launch Configuration

The fabric images (GigaVUE V Series Proxy and GigaVUE® V Series Node) are launched by GigaVUE-FM based on the configuration made in Nutanix Fabric Launch Configuration page.

GigaVUE V Series Proxy manages multiple GigaVUE® V Series Node and orchestrates the flow of traffic from GigaVUE® V Series Nodes to the monitoring tools.

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 GigaVUE V Series Proxy and GigaVUE® V Series Node are to be deployed.
Enable Custom Certificates	<p>Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and an handshake error occurs.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE: If the certificate expires after the successful deployment of the fabric components, then the fabric components moves to failed state.</p> </div>
Certificate	Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate .
Configure a V Series Proxy (Optional)	Select this option to configure a V Series Proxy.
GigaVUE® V Series Node	<ul style="list-style-type: none"> • Hosts—Select a node or multiple nodes from the selected Cluster. • Version—Select a GigaVUE® V Series Node image file. Refer to Upload Fabric Images for more information. • Management 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 GigaVUE® V Series Node. • Number of vCPUs—Enter the number of vCPUs required. • Cloud-init User Data (Optional)—Enter cloud-init user data (YAML, JSON, or Shell script)

NOTE: Assigning a Static IP for GigaVUE V Series Nodes is not supported. DHCP must be enabled for the management subnet and tunnel subnet.

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.

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

Configuring Monitoring Domain

To configure Nutanix in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Nutanix**, and then click **Monitoring Domain**. The Nutanix Configuration page appears.
2. On the **Nutanix Configuration** page, click **New**. The Nutanix Configuration page appears.

Monitoring Domain	<input type="text" value="Enter a monitoring domain name"/>
Connection Alias	<input type="text" value="Alias"/>
Nutanix Prism Central IP	<input type="text" value="Nutanix Prism Central IP Address"/>
Nutanix Prism Central Username	<input type="text" value="Nutanix Prism Central Username"/>
Nutanix Prism Central Password	<input type="password" value="Nutanix Prism Central Password"/>
Clusters	<input type="button" value="Select Clusters..."/>

3. 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

4. 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 Cloud Suite Fabric Controller manages multiple GVMs and orchestrates the flow of traffic from GVMs to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Cloud Suite 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.

The screenshot displays the 'Nutanix Fabric Launch Configuration' page in the GigaVUE-FM interface. The page is divided into two main sections: 'Fabric Controller' and 'GVMs'. The 'Fabric Controller' section includes a dropdown for 'Cluster-A' and three input fields: 'Version' (with a 'Select image...' dropdown), 'Management Subnet' (with a 'Select management subnet...' dropdown), and 'Cloud-Init User Data (Optional)' (with a text area for YAML, JSON, or Shell script). The 'GVMs' section includes a 'Hosts' dropdown (with 'Select All' and 'Select None' buttons), a 'Version' dropdown (with a 'Select image...' dropdown), a 'Management Subnet' dropdown (with a 'Select management subnet...' dropdown), an 'Add Subnet' button, and several numeric input fields: 'Memory Size (GB)' (4), 'Disk Size (GB)' (12), 'Number of VCPUs' (2), and 'Tunnel MTU' (9001). A 'Cloud-Init User Data (Optional)' text area is also present. At the bottom, there is a 'Save & Configure Next Cluster' button. The interface includes a sidebar with navigation options like 'AWS', 'Azure', 'OpenStack', 'Kubernetes', 'Nutanix', 'Monitoring Session', 'Monitoring Domain', 'Topology', 'Settings', 'AnyCloud', 'CLOUD', 'Events', and 'Audit Logs'. The top navigation bar shows 'Dashboard', 'Physical', 'Virtual', and 'Cloud' (selected).

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	<ul style="list-style-type: none"> • Version—Select a Fabric Controller image file (gigamon-fabric-cntrl-1.7-1). Refer to Upload Fabric Images for more information. • Management 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	<ul style="list-style-type: none"> • 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. • Management 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.

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

Configure and Manage Resources

This section 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:

- [Visibility Components](#)
- [Monitoring Session](#)
- [Configure Nutanix Settings](#)

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:

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. 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.
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.

Parameter	Description
Target	A target determines the instances that are to be monitored. Targets are determined based on the following formula: $\text{Target} = (\text{Maps} \cap \text{Inclusion map}) - \text{Exclusion map}$
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.

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 a new Monitoring Session](#)
- [Create Tunnel Endpoints](#)
- [Create Map](#)
- [Deploy Monitoring Session](#)
- [View Statistics](#)
- [View Topology](#)

Create a new Monitoring Session

You can create multiple monitoring sessions within a single connection.

To create a new monitoring session:

1. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > Nutanix**. The Monitoring Session page appears.
2. Click **New**. The **Create a New Monitoring Session** dialog box appears.

Create A New Monitoring Session

Alias

Monitoring Domain

3. 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.

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

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. After creating a new monitoring session, or click **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.

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

Field	Description
Alias	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.

4. Click **Save**.

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

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 1: Conditions for the Rules

Conditions	Description
L2, L3, and L4 Filters	
EtherType	<p>The packets are filtered based on the selected ethertype. The following conditions are displayed:</p> <ul style="list-style-type: none"> ■ IPv4 ■ ARP ■ RARP ■ Other <p>L3 Filters</p> <p>If you choose IPv4, the following L3 filter conditions are displayed:</p> <ul style="list-style-type: none"> ■ Protocol ■ IP Fragmentation ■ IP Time to live (TTL) ■ IP Type of Service (TOS) ■ IP Explicit Congestion Notification (ECN) ■ IP Source ■ IP Destination

Conditions	Description
	L4 Filters If you select TCP or UDP protocol, the following L4 filter conditions are displayed: <ul style="list-style-type: none"> ■ 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 EtherType 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 EtherType and Pass All.

To create a new map:

1. In the Monitoring Session canvas, select **New > New Map**, drag and drop a new map template to the workspace. The **New Map** quick view appears.
2. 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	<p>The rules for filtering the traffic in the map.</p> <p>To add a map rule:</p> <ol style="list-style-type: none"> 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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>NOTE:</p> <ul style="list-style-type: none"> • Repeat steps b through f to add more conditions. • Repeat steps a through f to add nested rules. </div>



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

3. 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.

4. 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:

Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected monitoring session. NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again.
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. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > Nutanix**. The Monitoring Session page appears.
2. Click **Topology** tab, the Topology page appears.
3. Select a connection from the **Select connection...** drop-down list. The topology view of the subnets and instances are displayed.
4. (Optional) Select a monitoring session from the **Select monitoring session...** drop-down list. The monitored subnets and instances change to blue.
5. 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.
6. (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. Go to **Inventory > VIRTUAL > Nutanix** and then click **Settings**. The Settings page appears.
2. Click **Advanced** tab on 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.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.

Additional Sources of Information

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

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.4 Hardware and Software Guides
<p>DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p>Hardware</p> <p>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices</p>
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide

GigaVUE Cloud Suite 6.4 Hardware and Software Guides	
GigaVUE-OS Installation Guide for DELL S4112F-ON	
G-TAP A Series 2 Installation Guide	
GigaVUE M Series Hardware Installation Guide	
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW	
Software Installation and Upgrade Guides	
GigaVUE-FM Installation, Migration, and Upgrade Guide	
GigaVUE-OS Upgrade Guide	
GigaVUE V Series Migration Guide	
Fabric Management and Administration Guides	
GigaVUE Administration Guide	covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
*GigaVUE V Series Applications Guide	
GigaVUE V Series Quick Start Guide	
GigaVUE Cloud Suite Deployment Guide - AWS	
GigaVUE Cloud Suite Deployment Guide - Azure	
GigaVUE Cloud Suite Deployment Guide - OpenStack	
*GigaVUE Cloud Suite Deployment Guide - Nutanix	
GigaVUE Cloud Suite Deployment Guide - VMware	
*GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration	
GigaVUE Cloud Suite for AnyCloud Guide	
Universal Cloud Tap - Container Guide	
Gigamon Containerized Broker Deployment Guide	
GigaVUE Cloud Suite for AWS—GigaVUE V Series 1 Guide	
GigaVUE Cloud Suite for Azure—GigaVUE V Series 1 Guide	

GigaVUE Cloud Suite 6.4 Hardware and Software Guides	
GigaVUE Cloud Suite for OpenStack-GigaVUE V Series 1 Guide	
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide	
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
Reference Guides	
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices	
GigaVUE-OS Security Hardening Guide	
GigaVUE Firewall and Security Guide	
GigaVUE Licensing Guide	
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices	
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices	
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)	
Release Notes	
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release	
NOTE: Release Notes are not included in the online documentation.	
NOTE: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon . Refer to How to Download Software and Release Notes from My Gigamon .	
In-Product Help	
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.	

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	
For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

The **VÜE 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 VÜE 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.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)