



GigaVUE Cloud Suite for OpenStack– GigaVUE V Series 1 Guide

GigaVUE Cloud Suite

Product Version: 6.3

Document Version: 1.0

Last Updated: Friday, June 9, 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
6.3.00	1.0	06/02/2023	Original release of this document with 6.3.00 GA.

Contents

GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide	1
Change Notes	3
Contents	4
GigaVUE Cloud Suite for OpenStack	6
About GigaVUE Cloud Suite for OpenStack	7
Components of GigaVUE Cloud Suite for OpenStack	7
Architecture of GigaVUE Cloud Suite for OpenStack	8
G-vTAP Agent	8
Open vSwitch (OVS) Mirroring	9
Virtual Dashboard Widgets	12
Overview	12
V Series Alarms	12
Connection Status	13
Usage	13
Summary	13
Traffic Rate	13
Aggregate Summary	13
Get Started with GigaVUE Cloud Suite for OpenStack	
Deployment	14
Before You Begin	14
Supported Hypervisor	14
Minimum Compute Requirements	15
Network Requirements	16
Virtual Network Interface Cards (vNICs)	17
Key Pairs	17
Install and Upgrade GigaVUE-FM	18
Deploy GigaVUE Cloud Suite for OpenStack	19
Upload Fabric Images	19
Prepare G-vTAP Agent to Monitor Traffic	21
Linux G-vTAP Agent Installation	21
Windows G-vTAP Agent Installation	27
Install G-vTAP OVS Agent for OVS Mirroring	31
Pre-Configuration Checklist	34

Create Monitoring Domain	34
Configure GigaVUE Fabric Components	38
Configure G-vTAP Controller	39
Configure GigaVUE V Series Controller	42
Configure GigaVUE V Series Node	43
Configure Monitoring Session	46
Create a Monitoring Session	46
Prefiltering	48
Create Tunnel Endpoints	50
Create a Map	51
Agent Pre-filtering	54
Add Applications to Monitoring Session	55
Sampling	56
Slicing	57
Masking	58
NetFlow	59
Deploy the Monitoring Session	71
Add Header Transformations	73
Visualize the Network Topology	74
View Monitoring Session Statistics	75
Administer GigaVUE Cloud Suite for OpenStack	77
Configure the OpenStack Settings	77
Role Based Access Control	78
About Audit Logs	79
About Events	81
GigaVUE-FM Version Compatibility Matrix	82
Troubleshooting	84
OpenStack Connection Failed	84
Handshake Alert: unrecognized_name	84
GigaVUE V Series Node or G-vTAP Controller is Unreachable	85
Additional Sources of Information	86
Documentation	86
How to Download Software and Release Notes from My Gigamon	89
Documentation Feedback	89
Contact Technical Support	90
Contact Sales	91
Premium Support	91
The VUE Community	91
Glossary	92

GigaVUE Cloud Suite for OpenStack

This guide describes how to install, configure and deploy the GigaVUE Cloud solution on OpenStack. Use this document for instructions on configuring the GigaVUE Cloud components and setting up the traffic monitoring sessions for OpenStack.

Refer to the following sections for details:

- [About GigaVUE Cloud Suite for OpenStack](#)
- [Get Started with GigaVUE Cloud Suite for OpenStack Deployment](#)
- [Deploy GigaVUE Cloud Suite for OpenStack](#)
- [Configure Monitoring Session](#)
- [Administer GigaVUE Cloud Suite for OpenStack](#)
- [GigaVUE-FM Version Compatibility Matrix](#)
- [Troubleshooting](#)

About GigaVUE Cloud Suite for OpenStack

GigaVUE® Fabric Manager (GigaVUE-FM) is a web-based fabric management interface that provides a single-pane-of-glass visibility and management of both the physical and virtual traffic. GigaVUE-FM is a key component of the GigaVUE Cloud Suite for OpenStack.

The OpenStack software is designed for multi-tenancy (multiple projects), where a common set of physical compute and network resources are used to create project domains that provide isolation and security. Characteristics of a typical OpenStack deployment include the following:

- Projects are unaware of the physical hosts on which their instances are running.
- A project can have several virtual networks and may span across multiple hosts.

In a multi-project OpenStack cloud, where project isolation is critical, the GigaVUE solution extends visibility for the project's workloads without impacting others by doing the following:

- Support project-wide monitoring domains—a project may monitor any of its instances.
- Honor project isolation boundaries—no traffic leakage from one project to any other project during monitoring.
- Monitor traffic without needing cloud administration privileges. There is no requirement to create port mirror sessions and so on.
- Monitor traffic activity of one project without adversely affecting other projects.

Refer to the following sections for details:

- [Components of GigaVUE Cloud Suite for OpenStack](#)
- [Architecture of GigaVUE Cloud Suite for OpenStack](#)

Components of GigaVUE Cloud Suite for OpenStack

The GigaVUE Cloud Suite for OpenStack 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.

GigaVUE-FM can be installed on-premises or launched from an OpenStack image. GigaVUE-FM manages the configuration of the following visibility components in your OpenStack project:

- G-vTAP Controllers (only if you are using G-vTAP Agent as the traffic acquisition method)
- GigaVUE V Series 1 Configuration
 - GigaVUE® V Series Controllers
 - GigaVUE® V Series 1 nodes
- **G-vTAP Controller** manages multiple G-vTAP Agents and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more G-vTAP Controllers to communicate with the G-vTAP Agents. G-vTAP Controllers
- **GigaVUE® V Series Controller** manages multiple V Series nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Controllers to communicate with the GigaVUE V Series nodes.
- **GigaVUE® V Series Node** is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite Cloud using L2GRE, or ERSPAN, or VXLAN tunnels.

Architecture of GigaVUE Cloud Suite for OpenStack

GigaVUE Cloud Suite for OpenStack captures traffic in OpenStack cloud using G-vTAP Agents directly or through the hypervisor as described in this section.

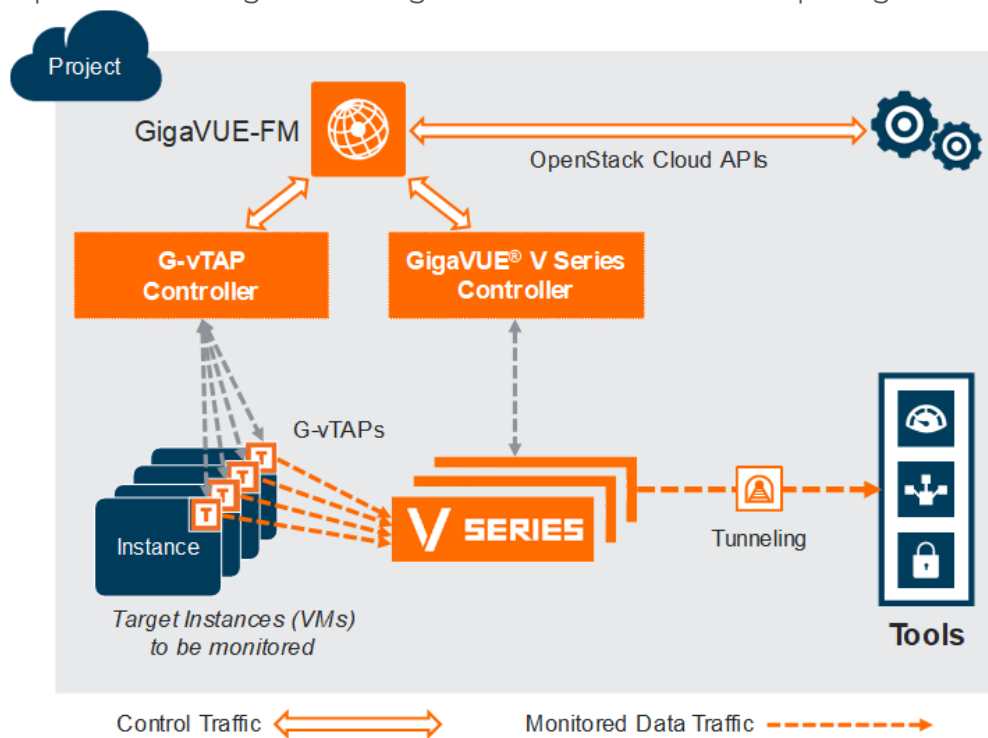
Refer to the following architectures for details:

- [G-vTAP Agent](#)
- [Open vSwitch \(OVS\) Mirroring](#)

G-vTAP Agent

A G-vTAP Agent is a tiny footprint user-space agent (G-vTAP) that is deployed in a project instance. This agent mirrors the traffic from a source interface to a destination mirror interface. The mirrored traffic is then sent to the GigaVUE Cloud Suite® V Series node. The

following figure shows a high-level architecture of Gigamon GigaVUE Cloud Suite for OpenStack using G-vTAP Agents as the source for acquiring the traffic.



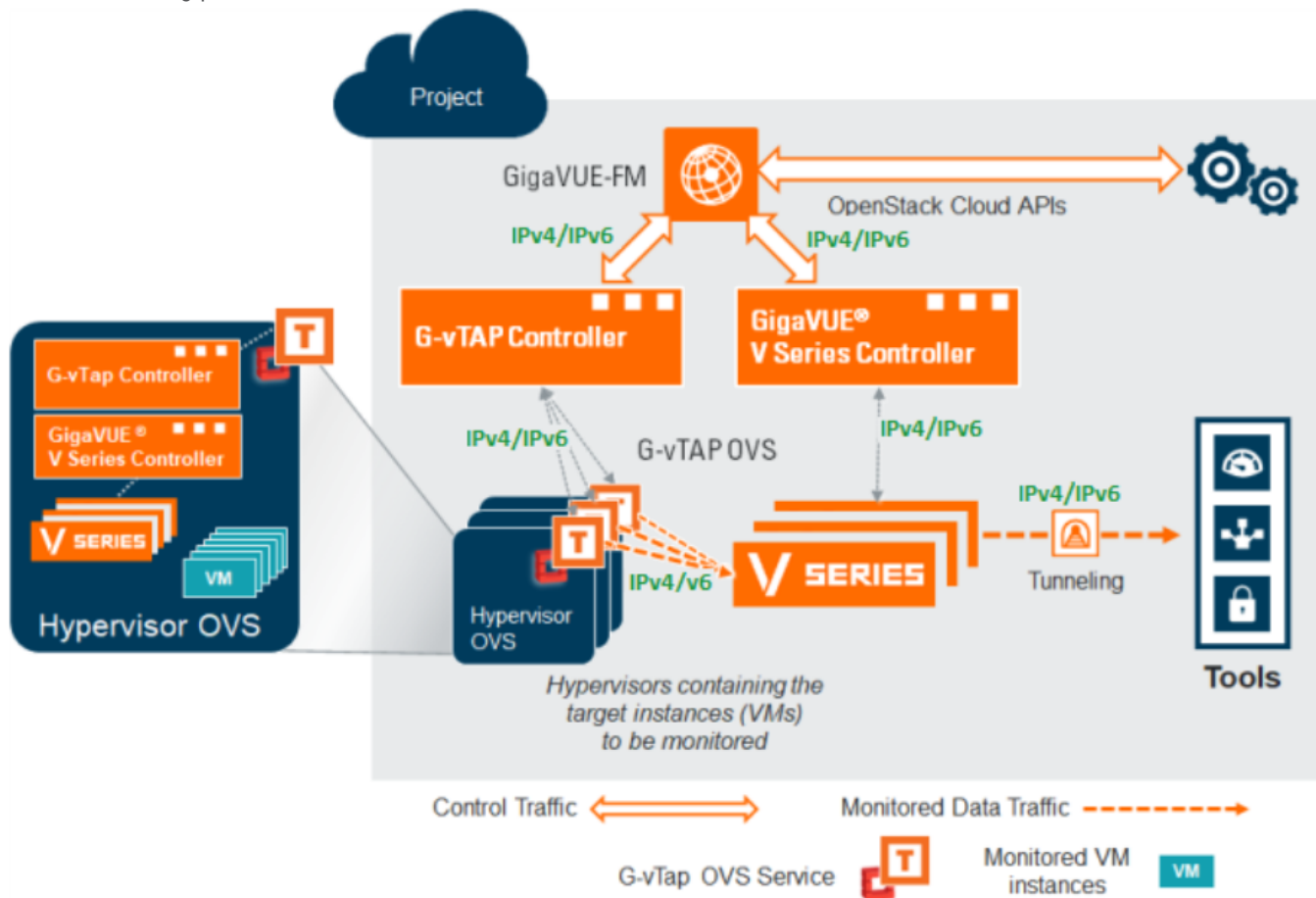
A G-vTAP Agent is deployed by installing the agent in the virtual instances. When a G-vTAP Agent is installed, a G-vTAP Controller must be configured in your environment. A G-vTAP Controller orchestrates the flow of mirrored traffic from G-vTAP Agents to the GigaVUE V Series nodes. A single G-vTAP Controller can manage up to 100 G-vTAP Agents deployed in the cloud.

By using G-vTAP Agents for mirroring traffic, the monitoring infrastructure is fully contained within the virtual machine being monitored. This agent is agnostic of the underlying virtual switch. Also, the cost of monitoring a virtual machine is borne by the same virtual machine.

Open vSwitch (OVS) Mirroring

When deploying Open vSwitch (OVS) Mirroring, a G-vTAP Agent is installed on the hypervisor where the VMs you wish to monitor are located. When a G-vTAP Agent is installed, a G-vTAP Controller must be configured in your environment. A G-vTAP Controller orchestrates the flow of mirrored traffic from G-vTAP Agents to the GigaVUE V Series nodes.

A single G-vTAP Controller can manage up to 100 G-vTAP Agents deployed in the cloud. By using OVS Mirroring or OVS Mirroring + DPDK, the mirroring infrastructure is fully contained within the hypervisors.



The G-vTAP Agents are deployed on the target hypervisors and the configuration file is to be modified based on the requirements and service. GigaVUE-FM connects to G-vTAP Controller and each G-vTAP Controller can talk to G-vTAP Agents. GigaVUE-FM receives the list of interfaces that can be used as the source or destination for the mirroring interface selected in GigaVUE-FM. GigaVUE-FM mirrors and forwards the traffic to the V Series nodes based on the deployed Monitoring Session.



- G-vTAP configures traffic mirroring in the OVS (with or without DPDK) and the management of the mirrored traffic is completely based on OVS architecture and the server.
- OVS Mirroring also supports Open vSwitch with DPDK. The configuration steps for OVS Mirroring and OVS Mirroring with DPDK are the same.

Prerequisites for OVS Mirroring

The following items are required to deploy a G-vTAP OVS agent:

- An existing OpenStack cloud environment should be available with admin project and login credentials to create a monitoring domain.
- A user with OVS access is required to enable OVS-Mirror. The user can be an admin or can be a user with a custom role that has the permissions and the ability to list projects.
- A working GigaVUE-FM with latest build.

OpenStack Cloud Environment Requirements

- ML2 mechanism driver: Open vSwitch.
- You must have the following role privileges to enable OVS mirroring.

OpenStack CLI command	Supported API/Action	Description
openstack hypervisor list	GET /os-hypervisors	Should list all hypervisors in the domain
openstack server list --all --host <hostname>	GET /servers	Should list all the servers on a specified host
openstack server list -all	GET /servers	Should list servers of all projects in the domain
openstack project list	GET /v3/projects	Should list all projects in the domain
openstack project list --user <user with custom role>	GET /v3/projects	Should list all projects that a specified user (user specified in FM config) is associated with
openstack user list	GET /v3/users	Should list all users in the domain
openstack subnet list	GET /subnets	Should list subnets for all projects in the domain
openstack network list	GET /network	Should list networks for all projects in the domain
openstack floating ip list	GET /floatingips	Should list floating ips for all projects in the domain
openstack floating ip set --port <portid> <floating ip>	PUT /floatingips/{floatingip_id}	Used to attach floating ip to fabric nodes
openstack security group list	GET /security-groups	Should list security groups for all projects in the domain
openstack security group show <security group id>	GET /security-groups/{security_group_id}	Should list details of specified security group
openstack port list	GET /ports	Should list ports for all projects in the domain
openstack port show <portid>	GET /ports/{portid}	Should list port details including bridge name



If the OpenStack CLI command `openstack hypervisor list` does not return a reachable IP for the hypervisors that are being monitored, you must manually enter a reachable IP for each hypervisor in OpenStack CLI using project properties. For each hypervisor you will need to add a key value pair property in the following format:

- key: value
- key: must be in the form `gigamon-hv-<hypervisorID>`



- value: reachable IP for hypervisor

For example: `openstack project set --property gigamon-hv-1=1.2.3.4 project-name`

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms, Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

Go to **Traffic > Virtual > Orchestrated Flows > Overview**. The Cloud Homepage appears.

Virtual Dashboard Widgets

This section describes the widgets that can be viewed on the overview page.

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Summary (Monitoring Session details)
- Traffic Rate
- Aggregate Summary

Overview

The overview dashboard displays the number of GigaVUE V Series Nodes active in GigaVUE-FM, number of Monitoring sessions and connections configured in all the platforms, and the number of alarms triggered in V Series Nodes.

V Series Alarms

The V Series Alarms widget presents a pie chart that helps you to quickly to view the V Series alarms generated. Each type of alarm triggered is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of V Series alarms triggered.

Connection Status

The connection status presents a pie chart that helps you to quickly to view the connection status of connections configured in the monitoring domain. Each type of connection status is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of connected.

Usage

The Usage widget displays the amount of traffic that flows through the GigaVUE V Series Nodes. Each bar in the graph indicates the volume usage on a particular day. Hovering the mouse over a bar in the graph displays the volume allowance and volume usage on that particular day.

Summary

This widget allows you to view the list of all the available monitoring session along with the respective monitoring domain, platform, connection, their health status, V Series Node health status and the deployment status of the connection. You can click on the monitoring session name to view the **Edit Monitoring session** page of the respective monitoring session.

Traffic Rate

The traffic rate widget displays the rate of traffic flowing through the GigaVUE V Series Nodes. Each line in the graph indicates the rate of traffic flow for transmitting, receiving, and their ratio which is specified by the legend.

Aggregate Summary

The aggregate summary displays the highest daily volume usage, average daily volume usage, highest daily volume over usage, average daily volume over usage, 95th percentile daily volume usage and the average daily volume allowance.

Get Started with GigaVUE Cloud Suite for OpenStack Deployment

This chapter describes how to configure GigaVUE® Fabric Manager (GigaVUE-FM), G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE V Series nodes in your OpenStack Cloud (Project). Refer to the following sections for details:

- [Before You Begin](#)
- [Install and Upgrade GigaVUE-FM](#)

Before You Begin

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

- [Supported Hypervisor](#)
- [Minimum Compute Requirements](#)
- [Network Requirements](#)
- [Virtual Network Interface Cards \(vNICs\)](#)
- [Security Group](#)
- [Key Pairs](#)

Supported Hypervisor

The following table lists the hypervisor with the supported versions for G-vTAP.

Hypervisor	Version
KVM	G-vTAP —Pike through Stein releases OVS Mirroring —Rocky and above

Minimum Compute Requirements

In OpenStack, flavors set the vCPU, memory, and storage requirements for an image. Gigamon recommends that you create a flavor that matches or exceeds the minimum recommended requirements listed in the following table.

Compute Instances	vCPU	Memory	Disk Space	Description
G-vTAP Agent	2 vCPU	4GB	N/A	Available as rpm or debian package. Instances can have a single vNIC or dual vNICs configured for monitoring the traffic.
G-vTAP OVS Agent	N/A	N/A	N/A	Available as rpm or debian package.
G-vTAP Controller	1 vCPU	4GB	8GB	Based on the number of agents being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE V Series Node	2 vCPU	3.75GB	20GB	NIC 1: Monitored Network IP; Can be used as Tunnel IP NIC 2: Tunnel IP (optional) NIC 3: Management IP
GigaVUE V Series Controller	1 vCPU	4GB	8GB	Based on the number of GigaVUE V Series nodes being monitored, multiple controllers will be required to scale out horizontally
GigaVUE-FM	2 vCPU	16GB	2x 40GB	GigaVUE-FM must be able to access the controller instance for relaying the commands. Use a flavor with a root disk and an ephemeral disk each of minimum 40GB.

Network Requirements

The following table lists the recommended requirements to setup the network topology.

Network	Purpose
Management	Identify the subnets that GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data	Identify the subnets that receives the mirrored tunnel traffic from the monitored instances. In data network, if a tool subnet is selected then the V Series node egress traffic on to the destinations or tools.

NOTE: If you are using IPv6 in the tenant network, then it is recommended to use SLAAC or stateless DHCPv6 for dynamic address assignment.

Virtual Network Interface Cards (vNICs)

OpenStack Cloud Instances with GvTAP Agents can be configured with one or more vNICs.

- **Single vNIC**—If there is only one interface configured on the instance with the G-vTAP Agent, the G-vTAP Agent sends the mirrored traffic out using the same interface.
- **Multiple vNICs**—If there are two or more interfaces configured on the instance with the G-vTAP Agent, the G-vTAP Agent monitors any number of interfaces. It provides an option to send the mirrored traffic out using any one of the interfaces or using a separate, non-monitored interface.

NOTE: vNICs are only applicable if the GvTap Agent is installed on the instances being monitored. It is not applicable for OVS Mirroring or OVS Mirroring +DPDK.

Key Pairs

A key pair consists of a public key and a private key. You must create a key pair and select the name of this key pair when you launch the G-vTAP Controllers, GigaVUE V Series nodes, and GigaVUE V Series Controllers from GigaVUE-FM. Then, you must provide the private key to connect to these instances. For information about creating a key pair, refer to OpenStack documentation.

Install and Upgrade GigaVUE-FM

You can install and upgrade the GigaVUE Cloud Suite® Fabric Manager (GigaVUE-FM) on cloud or on-premises. You can also upgrade GigaVUE-FM deployed in OpenStack environment.

- Cloud—To install GigaVUE-FM inside your OpenStack environment, you can simply launch the GigaVUE-FM instance in your Project. For installing the GigaVUE-FM instance, refer to [Install GigaVUE-FM on OpenStack](#)

NOTE: You cannot upgrade your 5.7.00 or lower versions of the GigaVUE-FM instance deployed in OpenStack environment to GigaVUE-FM 5.8.00 or higher versions. You must perform a fresh installation of GigaVUE-FM 5.8.00 or higher versions.

- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to *GigaVUE-FM Installation and Upgrade Guide* available in the [Gigamon Documentation Library](#).

Deploy GigaVUE Cloud Suite for OpenStack

This chapter describes how to connect, launch, and deploy fabric components of GigaVUE Cloud Suite for OpenStack in your OpenStack environment.

Refer to the following sections for details:

- [Upload Fabric Images](#)
- [Prepare G-vTAP Agent to Monitor Traffic](#)
- [Pre-Configuration Checklist](#)
- [Create Monitoring Domain](#)
- [Configure GigaVUE Fabric Components](#)

Upload Fabric Images

First, you must fetch the images from [Gigamon Customer Portal](#) using FTP, TFTP, SCP, or other desired method and copy it to your cloud controller. After fetching the images, you must source the credentials file and then upload the qcow2 images to Glance.

For example, you can source the credentials file with admin credentials using the following command:

```
$ source admin_openrc.sh
```

To upload the qcow2 images to Glance, use one of the following commands:

```
glance image-create --disk-format qcow2 --visibility public --container-format bare --progress -  
name gigamon-gigavue-vseries-cntlr-N -file gigamon-gigavue-cntlr-N.qcow2
```

Or

```
openstack image create --disk-format qcow2 --public --container-format bare --file gigamon-  
gigavue-vseries-cntlr-N gigamon-gigavue-vseries-cntlr-N.qcow2
```

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

- gigamon-gigavue-vseries-node-1.x.x
- gigamon-gigavue-vseries-cntlr-1.x.x
- gigamon-gigavue-gvtap-cntlr-1.x.x
- gigamon-gigavue-gvtap-ovs-cntlr-1.x.x

NOTE: After uploading the GigaVUE V Series 1 nodes, you must set the image properties.

openstack image set --property hw_vif_multiqueue_enabled=true \$IMAGE_ID

Prepare G-vTAP Agent to Monitor Traffic

G-vTAP Agent is a tiny footprint user-space agent (G-vTAP) that is deployed on each instance that you want to monitor. This agent mirrors the selected traffic from a source interface to a destination mirror interface. The mirrored traffic is encapsulated using GRE or VXLAN tunneling and then sent to the GigaVUE V Series node.

NOTE: The G-vTAP Agent installation is applicable only when the G-vTAP is your traffic acquisition method.

A source interface can be configured with one or more vNIC. While configuring a source interface, you can specify the direction of the traffic to be monitored in the instance. The direction of the traffic can be egress or ingress or both.

Refer to the following sections for more information:

- [Linux G-vTAP Agent Installation](#)
- [Windows G-vTAP Agent Installation](#)
- [Install G-vTAP OVS Agent for OVS Mirroring](#)

Linux G-vTAP Agent Installation

Refer to the following sections for Linux agent installation:

- [Single vNIC Configuration](#)
- [Multiple vNICs Configuration](#)
- [Install G-vTAP Agents](#)

Single vNIC Configuration

A single NIC/vNIC acts both as the source and the destination interface. A G-vTAP Agent with a single NIC/vNIC configuration lets you monitor the ingress or egress traffic from the NIC/vNIC. The monitored traffic is sent out using the same NIC/vNIC.

For example, assume that there is only one interface eth0 in the monitoring VM. In the G-vTAP configuration, you can configure eth0 as the source and the destination interface, and specify both egress and ingress traffic to be selected for monitoring purpose. The egress and ingress traffic from eth0 is mirrored and sent out using the same interface.

NOTE: Using a single NIC/vNIC as the source and the destination interface may cause increased latency in sending the traffic out from the VM.

Example of the G-vTAP config file for a single NIC/vNIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

Multiple vNICs Configuration

A G-vTAP Agent lets you configure multiple vNICs. One or many vNICs can be configured as the source interface. The monitored traffic can be sent out using any one of the vNICs or using a separate, non-monitored vNIC.

For example, assume that there is eth0 and eth1 in the monitoring instance. In the G-vTAP Agent configuration, eth0 can be configured as the source interface and egress traffic can be selected for monitoring purpose. The eth1 interface can be configured as the destination interface. So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series node.

Linux G-vTAP Agent Installation

Refer to the following sections for Linux agent installation:

- [Single vNIC Configuration](#)
- [Multiple vNICs Configuration](#)
- [Install G-vTAP Agents](#)

Single vNIC Configuration

A single NIC/vNIC acts both as the source and the destination interface. A G-vTAP Agent with a single NIC/vNIC configuration lets you monitor the ingress or egress traffic from the NIC/vNIC. The monitored traffic is sent out using the same NIC/vNIC.

For example, assume that there is only one interface eth0 in the monitoring VM. In the G-vTAP configuration, you can configure eth0 as the source and the destination interface, and specify both egress and ingress traffic to be selected for monitoring purpose. The egress and ingress traffic from eth0 is mirrored and sent out using the same interface.

NOTE: Using a single NIC/vNIC as the source and the destination interface may cause increased latency in sending the traffic out from the VM.

Example of the G-vTAP config file for a single NIC/vNIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

Multiple vNICs Configuration

A G-vTAP Agent lets you configure multiple vNICs. One or many vNICs can be configured as the source interface. The monitored traffic can be sent out using any one of the vNICs or using a separate, non-monitored vNIC.

For example, assume that there is eth0 and eth1 in the monitoring instance. In the G-vTAP Agent configuration, eth0 can be configured as the source interface and egress traffic can be selected for monitoring purpose. The eth1 interface can be configured as the destination interface. So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series node.

Install G-vTAP Agents

You must have sudo/root access to edit the G-vTAP Agent configuration file.

For dual or multiple NIC/ENI configuration, you may need to modify the network configuration files to make sure that the extra NIC/ENI will initialize at boot time.



Before installing G-vTAP Agent **.deb** or **.rpm** packages on your Linux VMs, you must install packages like Python3 and Python modules (netifaces, urllib3, and requests).

You can install the G-vTAP Agents either from Debian or RPM packages.

Refer to the following topics for details:

- [Install G-vTAP from Ubuntu/Debian Package](#)
- [Install G-vTAP from RPM package](#)
- [Install G-vTAP from Red Hat Enterprise Linux and CentOS with Selinux Enabled](#)

Install G-vTAP from Ubuntu/Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent **6.3.00** Debian (.deb) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_6.3.00_amd64.deb
ubuntu@ip-10-0-0-246:~$ sudo dpkg -i gvtap-agent_6.3.00_amd64.deb
```

- Once the G-vTAP package is installed, modify the file **/etc/gvtap-agent/gvtap-agent.conf** to configure and register the source and destination interfaces. The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

NOTE: Any changes to the G-vTAP Agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the G-vTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0    mirror-src-ingress mirror-src-egress mirror-dst
```

Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0    mirror-src-ingress mirror-src-egress
# eth1    mirror-dst
```

Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0    mirror-src-ingress mirror-src-egress
# eth1    mirror-src-ingress mirror-src-egress mirror-dst
```

- Save the file.
- To enable the third-party orchestration, a configuration file **/etc/gigamon-cloud.conf** needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: orchestration
  password: orchestration123A!
  remoteIP: <controller list IP addresses separated by comma>
  remotePort: 8891
```

- Reboot the instance.

The G-vTAP Agent status will be displayed as running. Check the status using the following command:

```
ubuntu@ip-10-0-0-246:~$ sudo /etc/init.d/gvtap-agent status
```

Install G-vTAP from RPM package

To install from an RPM (.rpm) package on a Redhat, CentOS, or other RPM-based system:

1. Download the G-vTAP Agent **6.3.00** RPM (.rpm) package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Copy this package to your instance. Install the package with root privileges, for example:

```
[user@ip-10-0-0-214 ~]$ ls gvtap-agent_6.3.00_x86_64.rpm
[user@ip-10-0-0-214 ~]$ sudo rpm -i
gvtap-agent_6.3.00_x86_64.rpm
```

3. Modify the file **/etc/gvtap-agent/gvtap-agent.conf** to configure and register the source and destination interfaces. The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

NOTE: Any changes to the G-vTAP Agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the G-vTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0    mirror-src-ingress mirror-src-egress mirror-dst
```

Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0    mirror-src-ingress mirror-src-egress# eth1    mirror-dst
```

Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0    mirror-src-ingress mirror-src-egress# eth1    mirror-src-
ingress mirror-src-egress mirror-dst
```

4. Save the file.
5. To enable the third-party orchestration, a configuration file **/etc/gigamon-cloud.conf** needs to be created with the following contents:

```
Registration:
  groupName: <Monitoring Domain Name>
  subGroupName: <Connection Name>
  user: orchestration
  password: orchestration123A!
  remoteIP: <controller list IP addresses separated by comma>
  remotePort: 8891
```

6. Reboot the instance.

Check the status with the following command:

```
[user@ip-10-0-0-214 ~]$ sudo service gvtap-agent status G-vTAP Agent is running
```

Install G-vTAP from Red Hat Enterprise Linux and CentOS with Selinux Enabled

Prerequisite:

You must ensure that port 9901 is allowed in the Firewall. This port is required for the communication between G-vTAP and G-vTAP controller.

To install, follow these steps:

1. Launch the RHELPrerequisite:
2. You must ensure that port 9901 is allowed in the Firewall. This port is required for the communication between G-vTAP and G-vTAP controller.
3. To install, follow these steps:
4. /CentOS agent AML image.
5. Download the following packages from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
 - strongSwan TAR files
 - gvtap-agent_6.3.00_x86_64.rpm
 - gvtap.te files (type enforcement files)
6. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
7. Checkmodule -M -m -o gvtap.mod gvtap.te


```
semodule_package -o gvtap.pp -m gvtap.mod
sudo semodule -i gvtap.pp
```
8. Install G-vTAP Agent package:


```
sudo rpm -ivh gvtap-agent_6.3.00_x86_64.rpm
```
9. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

NOTE: Any changes to the GvTAP agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the GvTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
# sudo /etc/init.d/gvtap-agent restart
```

10. Install strongSwan:

```
tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
cd strongswan-5.7.1-1.el7.x86_64
sudo sh ./swan-install.sh
```

11. Reboot the instance.

Windows G-vTAP Agent Installation

Windows G-vTAP Agent allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This gives you more granular control over what traffic is monitored and mirrored.

VXLAN is the only supported tunnel type for Windows G-vTAP Agent.

Windows G-vTAP Agent Installation Using MSI Package

To install the Windows G-vTAP Agent using the MSI file:

1. Download the Windows G-vTAP Agent **6.3.00** MSI package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Install the downloaded MSI package as **Administrator** and the G-vTAP Agent service starts automatically.

- Once the G-vTAP package is installed, modify the file **C:\ProgramData\Gvtap-agent\gvtap-agent.conf** to configure and register the source and destination interfaces.

NOTE: Any changes to the GvTAP agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the GvTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.



Following are the rules to modify the G-vTAP configuration file:

- Interface is selected by matching its CIDR address with config entries.
- For the VMs with single interface:
 - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
 - mirror-dst is always granted implicitly to the interface.
- For the VMs with multiple interfaces:
 - mirror-dst needs to be granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
 - if none interfaces is granted any mirror-src permission, all interfaces will be granted mirror-src-ingress and mirror-src-egress.

Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

```
# 192.168.1.0/24 mirror-src-ingress mirror-src-egress mirror-dst
```

Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

```
# 192.168.1.0/24 mirror-src-ingress mirror-src-egress
# 192.168.2.0/24 mirror-dst
```

- Save the file.
- To enable the third-party orchestration, a configuration file **C:\ProgramData\Gvtap-agent\gigamon-cloud.conf** needs to be created with the following contents:

Registration:

```
groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: orchestration
password: orchestration123A!
remoteIP: <controller list IP addresses separated by comma>
remotePort: 8891
```

6. To restart the Windows G-vTAP Agent, perform one of the following actions:
 - Restart the VM.
 - Run 'sc stop gvtap' and 'sc start gvtap' from the command prompt.
 - Restart the G-vTAP Agent from the Windows Task Manager.

You can check the status of the G-vTAP Agent in the Service tab of the Windows Task Manager.

Windows G-vTAP Agent Installation Using ZIP Package

To install the Windows G-vTAP Agent using the ZIP package:

1. Download the Windows G-vTAP Agent **6.3.00** ZIP package from the [Gigamon Customer Portal](#). For assistance contact [Contact Technical Support](#).
2. Extract the contents of the .zip file into a convenient location.
3. Run 'install.bat' as an **Administrator** and the G-vTAP Agent service starts automatically.

4. Once the G-vTAP package is installed, modify the file **C:\ProgramData\Gvtap-agent\gvtap-agent.conf** to configure and register the source and destination interfaces.

NOTE: Any changes to the GvTAP agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the GvTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.



Following are the rules to modify the G-vTAP configuration file:

- Interface is selected by matching its CIDR address with config entries.
- For the VMs with single interface:
 - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
 - mirror-dst is always granted implicitly to the interface.
- For the VMs with multiple interfaces:
 - mirror-dst needs to be granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
 - if none interfaces is granted any mirror-src permission, all interfaces will be granted mirror-src-ingress and mirror-src-egress.

Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

```
# 192.168.1.0/24 mirror-src-ingress mirror-src-egress mirror-dst
```

Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

```
# 192.168.1.0/24 mirror-src-ingress mirror-src-egress
# 192.168.2.0/24 mirror-dst
```

5. Save the file.
6. To enable the third-party orchestration, a configuration file **C:\ProgramData\Gvtap-agent\gigamon-cloud.conf** needs to be created with the following contents:

Registration:

```
groupName: <Monitoring Domain Name>
subGroupName: <Connection Name>
user: orchestration
password: orchestration123A!
remoteIP: <controller list IP addresses separated by comma>
remotePort: 8891
```

7. To restart the Windows G-vTAP Agent, perform one of the following actions:
 - Restart the VM.
 - Run 'sc stop gvtap' and 'sc start gvtap' from the command prompt.
 - Restart the G-vTAP Agent from the Windows Task Manager.

You can check the status of the G-vTAP Agent in the Service tab of the Windows Task Manager.

NOTE: You must edit the Windows Firewall settings to grant access to the gvtap process. To do this, access the Windows Firewall settings and find “gvtapd” in the list of apps and features. Select it to grant access. Be sure to select both Private and Public check boxes. If “gvtapd” does not appear in the list, click **Add another app...** Browse your program files for the gvtap-agent application (gvtapd.exe) and then click **Add**. (**Disclaimer:** These are general guidelines for changing Windows Firewall settings. See Microsoft Windows help for official instructions on Windows functionality.)

Install G-vTAP OVS Agent for OVS Mirroring

This is applicable only if you are using G-vTAP OVS agent as the source of acquiring traffic. You must have sudo/root access to edit the G-vTAP OVS agent configuration file. Before installing the G-vTAP OVS agents, you must have launched the GigaVUE-FM instance.

NOTE: After rebooting your Ubuntu, you must redeploy the respective monitoring sessions to restore the mirror traffic on the respective Ubuntu VM interfaces.

You can install the G-vTAP OVS agents either from Debian or RPM packages as follows:

- [Install the G-vTAP OVS Agent from Ubuntu/Debian Package](#)
- [Install the G-vTAP OVS Agent from RPM package](#)

Install the G-vTAP OVS Agent from Ubuntu/Debian Package

To install from a Debian package:

1. Download the latest version of G-vTAP OVS Agent Debian (.deb) package from the [Gigamon Customer Portal](#).
2. Copy this package to OpenStack compute nodes. Install the package with root privileges, for example:

```
$ ls gvtap-ovs-agent_1.8-2_amd64.deb
$ sudo dpkg -i gvtap-ovs-agent_1.8-2_amd64.deb
```

3. Once the G-vTAP OVS agent package is installed, modify the file **/etc/gvtap-agent/gvtap-agent.conf** to configure and grant permission to monitor ingress and egress traffic and to transmit the mirrored packets.

NOTE: Any changes to the G-vTAP Agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the G-vTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

```
br-int mirror-dst
```

```
# Changes for OVS Mirroring
# This Value will be used as local Ip in OVS Mirror Config
tunnel-src 172.20.20.11
# This Value will be used as Next Hop for Tunneled Packets
tunnel-gw 172.20.20.1
# OVS Agent Mode, Values: auto|standard|dpdk|hw-offload
ovs-agent-mode auto
# VLAN Tag value (valid: 0-4094)
ovs-vlan-tag 2020
# Egress Interface for OVS Mirrored Traffic
ovs-egress-if vlan2020
```

4. After modifying the G-vTAP OVS config file, start the agent service.


```
$ sudo service gvtap-agent start
```
5. The G-vTAP OVS agent status will be displayed as running. Check the status using the following command:


```
$ sudo service gvtap-agent status
```

G-vTAP Agent is running

Install the G-vTAP OVS Agent from RPM package

To install from an RPM (.rpm) package on a Redhat, CentOS, or other RPM-based system:

1. Download the G-vTAP OVS Agent RPM (.rpm) package from the [Gigamon Customer Portal](#).
2. Copy this package to OpenStack compute nodes. Install the package with root privileges, for example:

```
$ ls gvtap-ovs-agent_1.8-2_x86_64.rpm
$ sudo rpm -ivh gvtap-ovs-agent_1.8-2_x86_64.rpm
```


3. Once the G-vTAP OVS agent package is installed, modify the file **/etc/gvtap-agent/gvtap-agent.conf** to configure and grant permission to monitor ingress and egress traffic and transmit the mirrored packets.

NOTE: Any changes to the GvTAP agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the GvTAP config file results in traffic loss until GigaVUE-FM does a periodic sync on its own every 15 minutes.

```
# br-int mirror-dst

# Changes for OVS Mirroring
# This Value will be used as local Ip in OVS Mirror Config
tunnel-src 172.20.20.11
# This Value will be used as Next Hop for Tunneled Packets
tunnel-gw 172.20.20.1
# OVS Agent Mode, Values: auto|standard|dpdk|hw-offload
ovs-agent-mode auto
# VLAN Tag value (valid: 0-4094)
ovs-vlan-tag 2020
# Egress Interface for OVS Mirrored Traffic
ovs-egress-if vlan2020
```

4. After modifying the G-vTAP OVS config file, start the agent service and verify its status.

```
$ systemctl start gvtap-agent.service
$ sudo service gvtap-agent status
G-vTAP Agent is running
```



When you are installing a self-signed RPM package, you must execute the following command to import the signing key into the RPM db.

```
sudo rpm --import /path/to/YOUR-RPM-GPG-KEY
```



To upgrade G-vTAP OVS agent:

- You must backup the **/etc/gvtap-agent/gvtap-agent.conf** configuration file before upgrading the G-vTAP OVS Agent and uninstall the old OVS agents.
- Follow the same installation procedure to upgrade the G-vTAP OVS agents.



- After upgrading the G-vTAP OVS Agent, copy and modify the **gvtap-agent.conf** file, stop the agent, and start the agent. Redeploy the Monitoring Session if required.

```
service gvtap-agent stop
service gvtap-agent start
```

Pre-Configuration Checklist

The following table provides information that you would need while launching the visibility components using GigaVUE-FM. Obtaining this information will ensure a successful and efficient deployment of the GigaVUE Cloud Suite for OpenStack.

You can log in to GigaVUE-FM and use the CLI command: **ip host <controller-hostname> <ip-address of the controller>**. (For example: **ip host os-controller1 192.168.2.3**.) Then, add the connection to the OpenStack tenant.

In order for GigaVUE-FM to make a connection to an OpenStack tenant, GigaVUE-FM must be able to resolve the hostname of the OpenStack controller, even if using an IP address in the Identity URL. For example, if GigaVUE-FM is configured to use DNS, and that controller hostname is in the DNS, this will work, and no further configuration will be needed. If not, then you must add a host entry to GigaVUE-FM.

NOTE: If you are not using DNS, you must manually enter the host entry in `/etc/hosts` on GigaVUE-FM for the OpenStack Controller. On using DNS you can directly enter the host entry in GigaVUE-FM.

	Required Information
<input type="checkbox"/>	Authentication URL
<input type="checkbox"/>	Project Name
<input type="checkbox"/>	Floating IP
<input type="checkbox"/>	Region name for the Project
<input type="checkbox"/>	Domain
<input type="checkbox"/>	SSH Key Pair
<input type="checkbox"/>	Networks
<input type="checkbox"/>	Security groups

Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM:

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

OpenStack > Monitoring Domain

Monitoring Domain Configuration

Save Cancel

Use V Series 2 ☒ Yes

Monitoring Domain

Alias

URL

User Domain Name

Project Domain Name

Project Name

Region

Username

Password

Traffic Acquisition Method

Traffic Acquisition Tunnel MTU

Use FM to Launch Fabric ☒ Yes

FM Instance: GigaVUE-FM

3. Enter or select the appropriate information to configure Monitoring Domain for OpenStack. Refer to the following table for field-level details.

NOTE: For the URL, User Domain Name, Project Domain Name, and Region field values, refer to the RC file downloaded from your OpenStack dashboard.

Field	Description
Use V Series 2	Select No for V Series 1 configuration.
Monitoring Domain	A name for the monitoring domain.
Alias	An alias used to identify the monitoring domain.
URL	<p>The authentication URL is the Keystone URL of the OpenStack cloud. This IP address must be DNS resolvable.</p> <p>Refer to the OpenStack User Manual for more information on retrieving the authentication URL from the OpenStack.</p>
User Domain Name	<p>The domain name of your OpenStack authentication domain.</p> <div> <p>NOTE:</p> <ul style="list-style-type: none"> If you are using a separate domain for AUTH, enter that domain name as User Domain Name. If you are not using a separate domain, you can use the same domain for User and Project Domain Name. </div>
Project Domain Name	The domain name of your OpenStack project.
Project Name	The name of the project used for OpenStack authentication.
Region	<p>The region where the Project resides. You can find your region by running one of these commands, depending on your OpenStack version.</p> <p>keystone endpoint-list or openstack endpoint list or looking at the RC file in OpenStack to view your credentials.</p>
Username	<p>The username used to connect to your OpenStack cloud.</p> <div> <p>NOTE: If you are using OVS mirroring, you must belong to a role that meets the OpenStack minimum requirements for OVS Mirroring. Refer to OVS Mirroring Prerequisites for more information.</p> </div>
Password	The password of your OpenStack cloud.
Traffic Acquisition Method	<p>Select the type of agent used to capture traffic for monitoring:</p> <ul style="list-style-type: none"> TaaS: If you use select TaaS (Tunnel as a Source) as the tapping method, you can use the tunnel as a source option in the monitoring session, where the traffic is

Field	Description
	<p>directly tunneled to the GigaVUE V Series nodes without deploying G-vTAP Agents and G-vTAP Controllers. The user is responsible for creating this tunnel feed and pointing it to the GigaVUE V Series node(s).</p> <ul style="list-style-type: none"> ● G-vTAP: G-vTAP Agents are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to communicate to the G-vTAP Agents from GigaVUE-FM. ● OVS Mirroring: If you select the OVS Mirroring option, the mirrored traffic from the OpenStack connections is monitored directly using the GigaVUE V Series nodes, and you need not configure the G-vTAP Agents and G-vTAP Controllers. ● None: None is used if you are not using the connection for tapping and are only launching the V Series nodes for processing traffic from other connection, such as Kubernetes.
Projects to Monitor (Only for OVS Mirroring traffic acquisition method)	<p>This field only appears for OVS Mirroring traffic acquisition method.</p> <ul style="list-style-type: none"> ● Click the Get Project List to view the list of projects. <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>NOTE: The Get Project List button will only work if all the OpenStack credentials have been provided. Refer to OVS Mirroring Prerequisites.</p> </div> <ul style="list-style-type: none"> ● Select projects that you want to monitor from the list. ● You can click Select None to clear existing selections or Select All to add all available projects to the connection configuration.
Secure Mirror Traffic	<p>Check box to establish secure tunnel between G-vTAP Agents and GigaVUE V Series nodes (especially in a shared controller and GigaVUE V Series node configuration)</p>

4. Click **Save**. The **OpenStack Fabric Launch Configuration** page appears. Refer to [Configure GigaVUE Cloud Suite for OpenStack Components](#) for detailed information.

NOTE: If GigaVUE-FM fails to connect to OpenStack, an error message is displayed specifying the cause of failure. The connection status is also displayed in Audit Logs, refer to [About Audit Logs](#) for more information.

Configure GigaVUE Fabric Components

After configuring the Monitoring Domain, you will be navigated to the OpenStack Fabric Launch Configuration page. In the same **OpenStack Fabric Launch Configuration** page, you can configure the following fabric components:

- [Configure G-vTAP Controller](#)
- [Configure GigaVUE V Series Controller](#)
- [Configure GigaVUE V Series Node](#)

In the **OpenStack Fabric Launch Configuration** page, enter or select the required information as described in the following table.

Fields	Description
SSH Key Pair	The SSH key pair for the G-vTAP Controller. For more information about SSH key pair, refer to Key Pairs .
Availability Zone	The distinct locations (zones) of the OpenStack region.
Security Groups	The security group created for the G-vTAP Controller. For more information, refer to Security Group .

Select **Yes** to configure a GigaVUE V Series Controller.

SSH Key Pair	<input type="text" value="Select SSH Key Pair..."/>
Availability Zone	<input type="text" value="Select Availability Zone..."/>
Security Groups	<input type="text" value="Select management subnet security group..."/>
Configure a V Series Proxy	<input type="checkbox"/> No

Configure G-vTAP Controller

A G-vTAP Controller manages multiple G-vTAP Agents and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. While configuring the G-vTAP Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the G-vTAP Agents to the GigaVUE V Series nodes.

G-vTAP Controller

Controller Version(s)	<div>Add</div> <div> <div>Image</div> <div>Select image...</div> </div> <div> <div>Flavor</div> <div>Select flavor...</div> </div> <div> <div>Number of Instances</div> <div>1</div> </div>
Management Network	<div> <div>IP Address Type</div> <div> <input checked="" type="radio"/> Private <input type="radio"/> Floating </div> </div> <div> <div>Network</div> <div>Select management network...</div> </div> <div> <div>Port</div> <div>Select Port</div> </div>
Additional Network(s)	<div>Add</div>
Tags	<div>Add</div>
Cloud-Init User Data (Optional)	<div>Enter cloud-init user data in YAML cloud-config format</div>
Agent Tunnel Type	<div>VXLAN</div> <div> <input type="checkbox"/> Configuration Drive </div>
G-vTAP Controller Name ⓘ	<div>Gigamon-G-vTapController-</div> <div>+</div> <div>1</div> <div>Gigamon-G-vTapController-1</div>



- Only if G-vTAP Agents are used for capturing traffic, then the G-vTAP Controllers must be configured in the OpenStack cloud.
- A G-vTAP Controller can only manage G-vTAP Agents that have the same version.

Enter or select the required information in the G-vTAP Controller section as described in the following table.

Fields	Description
Controller Version(s)	<p>The G-vTAP Controller version that you configure must always have the same version number as the G-vTAP Agents deployed in the instances. For more detailed information refer GigaVUE-FM Version Compatibility Matrix.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>NOTE: If there is a version mismatch between the G-vTAP controllers and G-vTAP Agents, GigaVUE-FM cannot detect the agents in the instances.</p> </div> <p>To add G-vTAP Controllers:</p> <ol style="list-style-type: none"> a. Under Controller Versions, click Add. b. From the Image drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP Agents installed in the instances. c. From the Flavor drop-down list, select a size for the G-vTAP Controller. d. In Number of Instances, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.
Management Network	<p>This segment defines the management network that GigaVUE-FM uses to communicate with G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE V Series Nodes.</p> <p>Network - Select the management network ID.</p> <p>IP Address Type</p> <p>The type of IP address GigaVUE-FM needs to communicate with G-vTAP controllers:</p> <ul style="list-style-type: none"> o Private—A private IP can be used when GigaVUE-FM, the G-vTAP Controller, or the GigaVUE V Series Controller reside inside the same project. o Floating—A floating IP is needed only if GigaVUE-FM is not in the same project in the cloud or is outside the cloud. GigaVUE-FM needs a floating IP to communicate with the controllers from an external network.
Additional Network(s)	<p>(Optional) If there are G-vTAP Agents on networks that are not IP routable from the management network, additional networks or subnets must be specified so that the G-vTAP Controller can communicate with all the G-vTAP Agents.</p> <p>Click Add to specify additional networks (subnets), if needed. Also, make sure that you specify a list of security groups for each additional network.</p>

Fields	Description
Tag(s)	<p>(Optional) The key name and value that helps to identify the G-vTAP Controller instances in your environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-gvtap-controllers. There is a specific G-vTAP Controller Version for OVS Mirroring and OVS Mirroring + DPDK.</p> <p>To add a tag:</p> <ol style="list-style-type: none"> Click Add. In the Key field, enter the key. For example, enter Name. In the Value field, enter the key value. For example, us-west-2-gvtap-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Agent Tunnel Type	The type of tunnel used for sending the traffic from G-vTAP Agents to GigaVUE V Series nodes. The options are GRE or VXLAN tunnels.


Configure GigaVUE V Series Controller

The fields in the GigaVUE V Series Controller configuration section are the same as those on the G-vTAP Configuration page. Refer to [Configure G-vTAP Controller](#) for the field descriptions.

Configure GigaVUE V Series Node

NOTE: If you are using V Series 1.xx, GigaVUE V Series nodes can only be successfully launched after GigaVUE V Series Controller is fully initialized and the status is displayed as **OK**.

Creating a GigaVUE V Series node profile automatically launches the V Series node. Enter or select the required information in the V Series Node section as described in the following table.

Parameter	Description
Image	Select the GigaVUE V Series node image file.
Flavor	Select the form of the GigaVUE V Series node.
Management Network	<p>For the GigaVUE V Series Node, the Management Network is what is used by the GigaVUE V Series Controller to communicate with the GigaVUE V Series Nodes. Select the management network ID.</p> <p>NOTE: When both IPv4 and IPv6 addresses are available, IPv6 address is preferred, however if IPv6 address is not reachable then IPv4 address is used.</p>
Data Network	<p>Click Add to add additional networks. This is the network that the GigaVUE V Series node uses to communicate with the monitoring tools. Multiple networks are supported.</p> <ul style="list-style-type: none"> • Tool Subnet—Select a tool subnet, this is the default subnet that the GigaVUE-FM use to egress traffic to your tools. This subnet must have proper connectivity to your endpoint. • IP Address Type <ul style="list-style-type: none"> ◦ Private—A private IP can be used when GigaVUE-FM, the G-vTAP Controller, or the GigaVUE V Series Controller, or the V Series node 2 reside inside the same project. ◦ Floating—A floating IP address specified here will be where GigaVUE V Series node 1 can be managed by GigaVUE-FM and controllers. • Network 1—Select a network type. <p> For OVS Mirroring or OVS Mirroring + DPDK deployments, must select Floating in the Data Network section and then specify the IPs in the Floating IPs field. You can have multiple Floating IPs.</p> <p>A network provider that is able to receive the monitored traffic may also be used here for OVS Mirroring and OVS Mirroring + DPDK. In this case, you would not need to provide a floating IP; but could select "private" and choose the provider network.</p>
Tag(s)	(Optional) The key name and value that helps to identify the G-vTAP Controller instances in your environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-gvtap-controllers.

Parameter	Description
	<p>To add a tag:</p> <ol style="list-style-type: none"> Click Add. In the Key field, enter the key. For example, enter Name. In the Value field, enter the key value. For example, us-west-2-gvtap-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Min Instances	<p>The minimum number of GigaVUE V Series nodes to be launched in OpenStack. The minimum number can be 1.</p> <ul style="list-style-type: none"> When you deploy an OVS Mirroring or OVS Mirroring + DPDK monitoring session, the V Series nodes will automatically be deployed based on the # of hypervisors being monitored. When you deploy a G-vTAP based monitoring session, the V Series nodes will automatically be deployed based on the # of VMs being monitored and the instance per V Series node ratio defined in the OpenStack Settings page. <p>NOTE: GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.</p>
Max Instances	<p>The maximum number of GigaVUE V Series nodes that can be launched in OpenStack.</p> <p>NOTE: Max Instances is applicable only for V Series node 1 works with G-vTAP connections and OVS mirroring.</p>
Tunnel MTU (Maximum Transmission Unit)	<p>The Maximum Transmission Unit (MTU) is applied on the outgoing tunnel endpoints of the GigaVUE-FM V Series node when a monitoring session is deployed. The default value is 1450. The value must be 42 bytes less than the default MTU for GRE tunneling, or 50 bytes less than default MTU for VXLAN tunnels.</p>

Click **Save** to save the OpenStack Fabric Launch Configuration.

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

To view the G-vTAP Agents of the selected monitoring domain, click on the **G-vTAP Agents** button. The G-vTAP Agents page appears. The IP address, Registration time, and Status of the G-vTAP Agents are displayed on this page.

OpenStack Monitoring Domain

🔍 ↺ 🔔 ⚙️

New Actions **G-vTAP Agents** Refresh Inventory

🏠

Monitoring Domain

Connection

Name

Management IP

Type

Version

Status

✓ md1

conn1

Gigamon-G-vTapControll... 10.210.221.131 G-vTap Controller 1.8 ✓ Ok

Gigamon-VSeriesNode-1 10.210.221.77 V Series Node 2.1.0 ✓ Ok

🕒 ⚙️

FM Instance: GigaVUE-FM

Configure Monitoring Session

This chapter describes how to setup tunnel endpoints in a monitoring session to receive and send traffic to the GigaVUE V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools or to a GigaVUE Cloud Suite H Series node.

Refer to the following sections for details:

- [Create a Monitoring Session](#)
- [Create Tunnel Endpoints](#)
- [Create a Map](#)
- [Add Applications to Monitoring Session](#)
- [Deploy the Monitoring Session](#)
- [Add Header Transformations](#)
- [Visualize the Network Topology](#)
- [View Monitoring Session Statistics](#)

Create a Monitoring Session

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

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

For the connections without G-vTAPs there is no targets that are automatically selected. You can use Customer Orchestrated Source in the monitoring session to accept a tunnel from anywhere.

You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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

Create A New Monitoring Session

3. Enter the appropriate information for the monitoring session as described in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain that you want to select.
Connection	The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.

4. Click **Create**. The **Edit Monitoring Session** page appears with the new canvas.

In the Edit Monitoring Session page, you can select [Prefiltering](#) if required. To apply Prefiltering policy template refer to [Applying Prefiltering policy template to Monitoring Session](#).

If multiple connections are selected, the **Topology** view displays all the instances and components of the selected connections.

Applying Prefiltering policy template to Monitoring Session

You can apply the prefiltering policy template to a monitoring session. To apply a monitoring session do the following:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.
3. Create a new monitoring session. To create a new monitoring session, refer to [Create a Monitoring Session](#).
4. In the Edit Monitoring Session page, expand **Prefiltering**.
5. Select the required Prefiltering template from the **Template** drop-down list. The rules and filters configured in the template appear. You can also change the values as per the requirement. By default, the changes are not saved in the template. You can save the changes as a new template by clicking **Save as Template**.
6. Click **Next**. The topology view appears.

Prefiltering

Prefiltering allows you to filter the traffic at G-vTAP Agents before sending it to the GigaVUE V Series Nodes. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the policy template can be applied to a monitoring session.

You can define a policy template with rules and filter values. A policy template once created can be applied to multiple monitoring sessions. However a monitoring session can use only one template.

Each monitoring session can have a maximum of 16 rules.

You can also edit a specific policy template with required rules and filter values for a particular monitoring session while editing a monitoring session. However, the customized changes are not saved in the template.

Some of the points that must be remembered for prefiltering in Next Generation G-vTAP Agents are:

- Prefiltering is supported only in Next Generation G-vTAP Agents. It is not supported for classic mirroring mechanism.
- Prefiltering is supported for both Linux and Windows G-vTAP Agents .
- For single monitoring session only one prefiltering policy is applicable. All the agents in that monitoring sessions are configured with respective prefiltering policy .
- For multiple monitoring session, if the same agent is selected by two or more monitoring sessions then prefiltering policy cannot be applied. It is default to PassAll.

Creating Prefiltering policy template

GigaVUE-FM allows you to create a prefiltering policy template with a single rule or multiple rules. You can configure a rule with a single filter or multiple filters. Each monitoring session can have a maximum of 16 rules.

To create a prefiltering policy template do the following steps:

1. Go to **Resources > Prefiltering**, and then click **G-vTAP**.
2. Click **New**.
3. Enter the name of the template in the **Template Name** field.
4. Enter the name of a rule in the **Rule Name** field.
5. Click any one of the following options:
 - Pass — Passes the traffic.
 - Drop — Drops the traffic.
6. Click any one of the following options as per the requirement:
 - Bi-Directional — Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
 - Ingress — Filters the traffic that flows in.
 - Egress — Filters the traffic that flows out.
7. Select the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 to 8 where 8 can be used for setting a rule with least priority. Drop rules are added based on the priority and then pass rules are added.
8. Select the **Filter Type** from anyone of the following options:
 - L3
 - L4
9. Select the **Filter Name** from any one of the following options:
 - ip4Src
 - ip4Dst
 - ip6Src
 - ip6Dst
 - Proto - It is common for both ipv4, ipv6.
10. Select the **Filter Relation** from any one of the following options:
 - Not Equal to
 - Equal to
11. Enter the value for the given filter.
12. Click **Save**.

NOTE: Click + to add more rules or filters. Click - to remove a rule or a filter.

Create Tunnel Endpoints

Traffic from the V Series node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2 Generic Routing Encapsulation (GRE) tunnel, or a ERSPAN, or a Virtual Extensible LAN (VXLAN) tunnel.

To create a new tunnel:

- 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.

X

Add Tunnel Spec

Save

Add To Library

Alias

Alias *

Description

Description (optional)

Type

Select a type...

▼

Select a type...

ERSPAN

L2GRE

VXLAN

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

Field	Description
Alias	The name of the tunnel endpoint. NOTE: Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN to create a tunnel.
Traffic Direction	The direction of the traffic flowing through the V Series node. Choose Out for creating a tunnel from the V Series node to the destination endpoint. NOTE: Traffic Direction In is not supported for V Series 1 nodes.
Remote Tunnel IP	The IP address of the tunnel destination endpoint. NOTE: You cannot create two tunnels from a V Series node to the same IP address.

4. Click **Save**.

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

Create a 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.

Conditions	Description
L2, L3, and L4 Filters	
EtherType	The packets are filtered based on the selected ethertype. The following conditions are displayed: <ul style="list-style-type: none"> ● IPv4 ● IPv6 ● ARP ● RARP ● Other L3 Filters

Conditions	Description
	<p>If you choose IPv4 or IPv6, 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 <p>L4 Filters</p> <p>If you select TCP or UDP protocol, the following L4 filter conditions are displayed:</p> <ul style="list-style-type: none"> ● Port Source ● Port Destination
MAC Source	The egress traffic from the instances or ENIs matching the specified source MAC address is selected.
MAC Destination	The ingress traffic from the instances or ENIs 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 instances are passed through the filter. When Pass All is selected, the L3 and L4 filters are disabled.

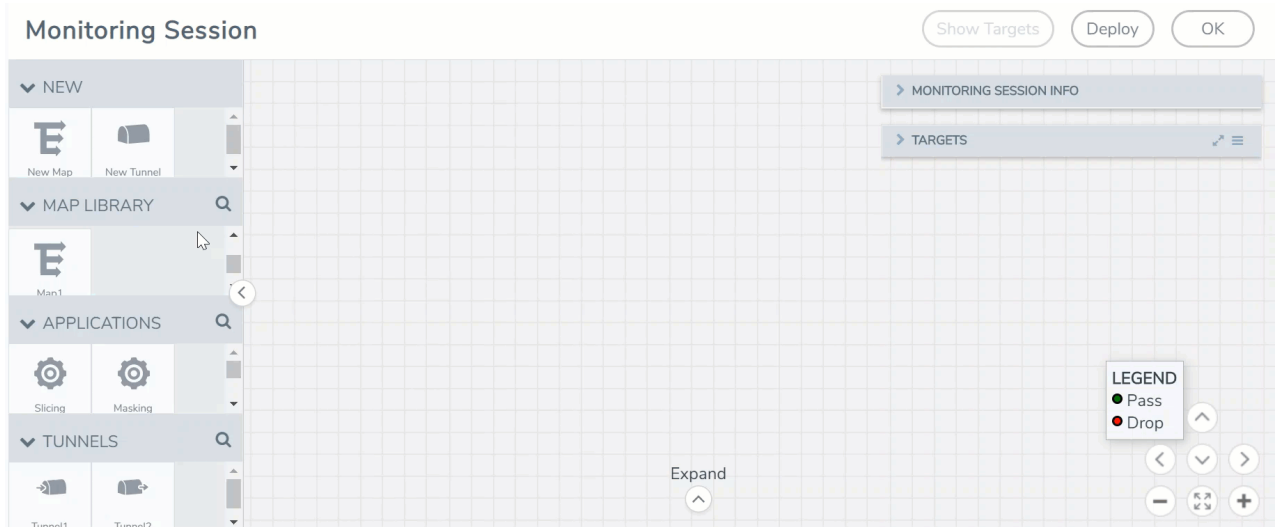
When you select a condition without source or destination specified, then both egress and ingress traffic is selected for tapping the traffic. For example, if you select EtherType as IPv4, TCP as the protocol, and do not specify IPv4 source or destination, then both egress and ingress traffic is selected 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. After creating a new monitoring session, or click **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.
2. In the canvas, select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.



3. Enter the appropriate information for creating a new map as shown in the following table.

Parameter	Description
Alias	The name of the new map. NOTE: The name can contain alphanumeric characters with no spaces.
Comments	The description of the map.
Map Rules	The rules for filtering the traffic in the map. To add a map rule: <ol style="list-style-type: none"> Click Add a Rule. 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. Select a condition from the Search L3 Conditions drop-down list and specify a value. (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.
Map Rules	<ol style="list-style-type: none"> (Optional) In the Priority and Action Set box, assign a priority and action set. (Optional) In the Rule Comment box, enter a comment for the rule. NOTE: Repeat steps b through f to add more conditions. NOTE: Repeat steps a through f to add nested rules.

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

4. 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, or create a **New Group** with a name.
 - Enter a description in the **Description** field, and click **Save**.
5. Click **Save**.

To edit a map, click the map and select **Details**, or click **Delete** to delete the map.

Agent Pre-filtering

The G-vTAP Agent pre-filtering option filters traffic before mirroring it from G-vTAP Agent to the V Series Nodes.

Agent pre-filtering is performed directly at the packet capturing point. By filtering at this point, unnecessary traffic is prevented from reaching the fabric nodes that perform filtering and manipulation functions. Preventing this traffic reduces the load on the V Series nodes and the underlying network.

NOTE: Agent pre-filtering is not supported for OVS Mirroring and OVS Mirroring + DPDK.

Agent Pre-filtering Guidelines

In cloud environments, there will be limits on how much traffic could be sent out per instance/single or double network interface.

Traffic will be passed if a network packet matches one or more of these rules:

- Only filters from traffic maps will be considered for G-vTAP filters. Inclusion and exclusion maps are purely for ATS (automatic target selection); not for G-vTAP.
- Filters from the first-level maps of the monitoring session will only be used to create G-vTAP maps.
- User-entered L2-L4 filters in the monitoring-session maps must be in the format that V Series Node currently accepts. Non L2-L4 filters are used purely by ATS to select the targets; not for G-vTAP.
- Both egress and ingress maps with filters are supported on G-vTAP.
- Both single and dual network interfaces for G-vTAP Agent VMs are supported.

Agent Pre-filtering Rules and Notes

G-vTAP Agent pre-filtering has the following capabilities and benefits:

- The agent pre-filtering option can be enabled or disabled at the monitoring-session level and is enabled by default.
- When enabled, traffic is filtered at the G-vTAP Agent-level, before mirroring to the V Series Nodes. Consequently, traffic flow to the V Series Nodes is reduced, which reduces the load/cost on the Cloud networks.
- Only rules from first-level maps are pushed to the agents.
- Pass rules are supported 100%.
- Drop rules are supported for only simple cases or single-drop rules with a pass all case.
- Rules that span all monitoring sessions will be merged for an G-vTAP Agent, if applicable
- If the max-rule limit of 16 is reached, then all the traffic is passed to the V Series node; no filtering will be performed.

Add Applications to Monitoring Session

GigaVUE Cloud Suite with V Series 1 node supports the following GigaSMART applications:

- [Sampling](#)
- [Slicing](#)
- [Masking](#)
- [NetFlow](#)

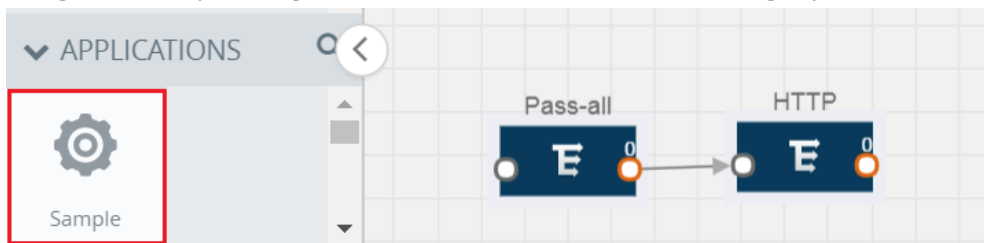
You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools.

Sampling

Sampling lets you sample the packets randomly based on the configured sampling rate and then forwards the sampled packets to the monitoring tools.

To add a sampling application:

1. Drag and drop **Sample** from **APPLICATIONS** to the graphical workspace.



2. Click **Sample** and select **Details**.



3. In the **Alias** field, enter a name for the sample.
4. For State, select the **On** check box to determine that the application is sampling packets randomly. Select the **Off** check box to determine that the application is not currently sampling the packets. The state can be changed at anytime whenever required.
5. From the Sampling Type drop-down list, select the type of sampling:
 - **Random Simple** — The first packet is selected randomly. The subsequent packets are also selected randomly based on the rate specified in the **Sampling Rate** field. For example, if the first packet selected is 5 and the sampling rate is 1:10, after the 5th packet a random 10 packets are selected for sampling.

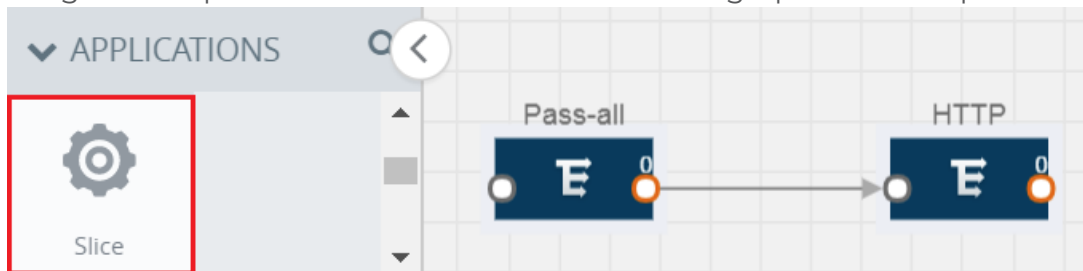
- **Random Systematic** —The first packet is selected randomly. Then, every nth packet is selected, where n is the value specified in the **Sampling Rate** field. For example, if the first packet selected is 5 and the sampling rate is 1:10, then every 10th packet is selected for sampling: 15, 25, 35, and so on.
6. In the **Sampling Rate** field, enter the ratio of packets to be selected. The default ratio is 1:1.
 7. Click **Save**.

Slicing

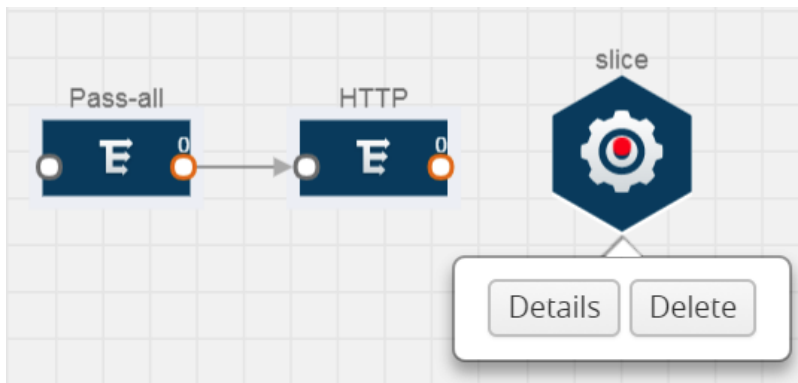
Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes.

To add a slicing application:

1. Drag and drop **Slice** from **APPLICATIONS** to the graphical workspace.



2. Click the Slice application and select **Details**.



3. In the **Alias** field, enter a name for the slice.
4. For State, select **On** or **Off** check box to enable or disable slicing. The state can be changed at a later time whenever required.
5. In the Slice Length field, specify the length of the packet that must be sliced.

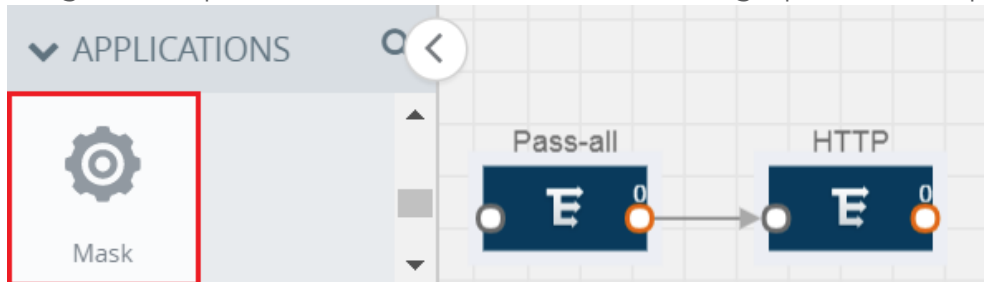
6. From the Protocol drop-down list, specify an optional parameter for slicing the specified length of the protocol. The options are as follows:
 - None
 - IPv4
 - IPv6
 - UDP
 - TCP
7. Click **Save**.

Masking

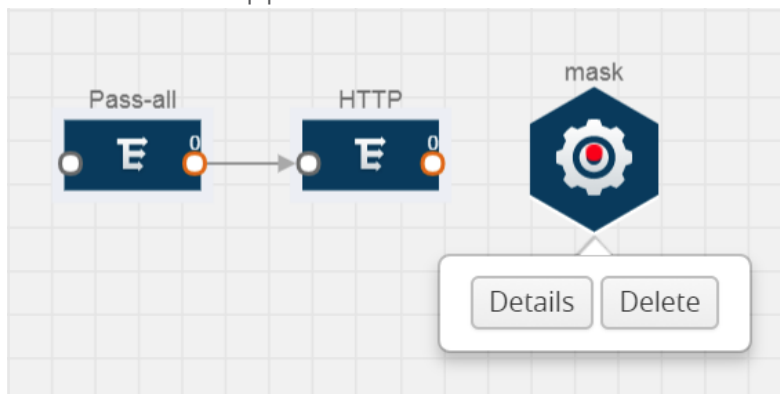
Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.

To add a masking application:

1. Drag and drop **Mask** from **APPLICATIONS** to the graphical workspace.



2. Click the Mask application and select **Details**.



3. In the **Alias** field, enter a name for the mask.
4. For State, select **On** or **Off** check box to enable or disable masking. The state can be changed at anytime whenever required.
5. In the Mask offset field, enter the offset from which the application should start masking data following the pattern specified in the Pattern field. The value can be specified in terms of either a static offset, that is, from the start of the packet or a relative offset, that is, from a particular protocol layer as specified in the Protocol field.

6. In the Mask length field, enter the length of the packet that must be masked.
7. In the Mask pattern field, enter the pattern for masking the packet. The value of the pattern is from 0 to 255.
8. From the Protocol drop-down list, specifies an optional parameter for masking packets on the data coming from the selected protocol.
9. Click **Save**.

NetFlow

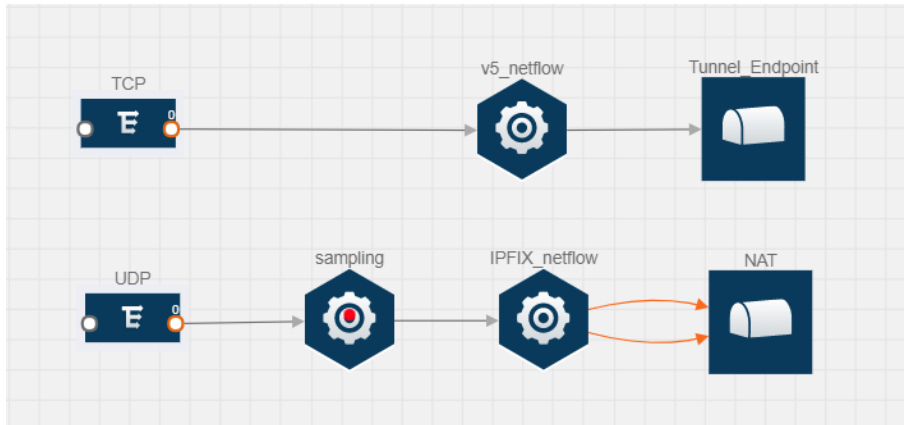
NetFlow collects IP network traffic on all interfaces where NetFlow monitoring is enabled. It gathers information about the traffic flows and exports the NetFlow records, which includes data and templates, to at least one NetFlow collector. The application that serves as a NetFlow collector receives the NetFlow data sent from exporters, processes the information, and provides data visualization and security analytics.

The following are the key benefits of NetFlow application:

- Compresses network information into a single flow record.
- Facilitates up to 99% reduction in data transferred.
- Accelerates the migration of mission-critical workloads to your cloud environment.
- Provides summarized information on traffic source and destination, congestion, and class of service.
- Identifies and classifies DDOS attacks, viruses, and worms in real-time.
- Secures network against internal and external threats.
- Identifies top consumers and analyzes their statistics.
- Reduces the cost of security monitoring.
- Analyzes the network flows based on algorithms and behavior rather than signature matching.
- Analyzes east-west traffic between flows within and across VPCs.

The NetFlow application contains key elements that specify what to match in the flow, such as all packets with the same source and destination port, or the packets that come in on a particular interface. For information about Match/Key fields, refer to [Match/Key Fields](#). A NetFlow record is the output generated by NetFlow. A flow record contains non-key elements that specify what information to collect for the flow, such as when the flow started or the number of bytes in the flow. For information about Match/Key fields, refer to [Collect/Non-Key Fields](#).

The following figure shows an example of a NetFlow application created on a GigaVUE V Series node in the monitoring session.



The NetFlow record generation is performed on GigaVUE V Series node running the NetFlow application. In [Add Applications to Monitoring Session](#), incoming packets from G-vTAP Agents are sent to the GigaVUE V Series node. In the GigaVUE V Series node, one map sends the TCP packet to the version 5 NetFlow application. Another map sends the UDP packet to a sampling application. The map rules and applications such as slice, mask, and sample can only be applied prior to sending the data to NetFlow.

A NetFlow application examines the incoming packets and creates a single or multiple flows from the packet attributes. These flows are cached and exported based on the active and inactive cache timeout specified in the Netflow application configuration.

The flow records can be sent to a tunnel for full packet inspection or to a NAT device for flow inspection. NAT allows the NetFlow records to be directly transmitted to a collector without a tunnel. For more information about NAT, refer to [Network Address Translation \(NAT\)](#).

The Netflow application exports the flows using the following export versions:

- version 5—The fields in the NetFlow record are fixed.
- version 9—The fields are configurable, thus a template is created. The template contains information on how the fields are organized and in what order. It is sent to the collector before the flow record, so the collector knows how to decode the flow record. The template is sent periodically based on the configuration.
- IPFIX—The extended version of version 9 supports variable length fields as well as enterprise-defined fields.

Match/Key Fields

NetFlow v9 and IPFIX records allow you to configure Match/Key elements.

The supported Match/Key elements are outlined in the following table:

	Description	Supported NetFlow Versions
Data Link		
Destination MAC	Configures the destination MAC address as a key field.	v9 and IPFIX
Egress Dest MAC	Configures the post Source MAC address as a key field.	IPFIX
Ingress Dest MAC	Configures the IEEE 802 destination MAC address as a key field.	IPFIX
Source MAC	Configures the IEEE 802 source MAC address as a key field.	v9 and IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP message as a key field.	v9 and IPFIX
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a key field.	IPFIX
IPv4 ICMP Type	Configures the type and code of the IPv4 ICMP message as a key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a key field.	IPFIX
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9 and IPFIX
IP DSCP	Configures the value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field as a key field.	IPFIX
IP Header Length	Configures the length of the IP header as a key field.	IPFIX
IP Precedence	Configures the value of the IP Precedence as a key field.	IPFIX
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9 and IPFIX
IP Total Length	Configures the total length of the IP packet as a key field.	IPFIX
IP TTL	For IPv4, configures the value of Time to Live (TTL) as a key field. For IPv6, configures the value of the Hop Limit	IPFIX

	Description	Supported NetFlow Versions
	field as a key field.	
IP Version	Configures the IP version field in the IP packet header as a key field.	v9 and IPFIX
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9 and IPFIX
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9 and IPFIX
IPv6 ICMP Code	Configures the code of the IPv6 ICMP message as a key field.	IPFIX
IPv6 ICMP Type	Configures the type of the IPv6 ICMP message as a key field.	IPFIX
IPv6 ICMP Type Code	Configures the type and code of the IPv6 ICMP message as a key field.	IPFIX
IPv6 Payload Length	Configures the value of the payload length field in the IPv6 header as a key field.	IPFIX
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9 and IPFIX
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport header as a key field.	v9 and IPFIX
TCP Ack Number	Configures the acknowledgment number in the TCP header as a key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP header as a key field.	IPFIX
TCP Src Port	Configures the source port identifier in the TCP header as a key field.	IPFIX
TCP Urgent	Configures the urgent pointer in the TCP header as a key field.	IPFIX

	Description	Supported NetFlow Versions
TCP Window Size	Configures the window field in the TCP header as a key field.	IPFIX
UDP Dest Port	Configures the destination port identifier in the UDP header as a key field.	IPFIX
UDP Src Port	Configures the source port identifier in the TCP header as a key field.	IPFIX

Collect/Non-Key Fields

NetFlow v9 and IPFIX records allow you to configure Collect/Non-Key elements.

The supported Collect/Non-Key elements are outlined in the following table:

	Description	Supported NetFlow Versions
Counter		
Byte Count	Configures the number of octets since the previous report in incoming packets for the current flow as a non-key field.	v9 and IPFIX
Packet Count	Configures the number of incoming packets since the previous report for this flow as a non-key field.	v9 and IPFIX
Data Link		
Destination MAC	Configures the destination MAC address as a non-key field.	v9 and IPFIX
Egress Des MAC	Configures the post source MAC address as a non-key field.	IPFIX
Ingress Des MAC	Configures the IEEE 802 destination MAC address as a non-key field.	IPFIX
Source MAC	Configures the IEEE 802 source MAC address as a non-key field.	v9 and IPFIX
Timestamp		
Flow End Millisec	Configures the absolute timestamp of the last packet of current flow in milliseconds as a non-key field.	IPFIX
Flow End Sec	Configures the flow start SysUp time as a non-key field.	IPFIX
Flow End Time	Configures the flow end SysUp time as a non-key field.	v9 and IPFIX
Flow Start Millisec	Configures the value of the IP Precedence as a non-key field.	IPFIX

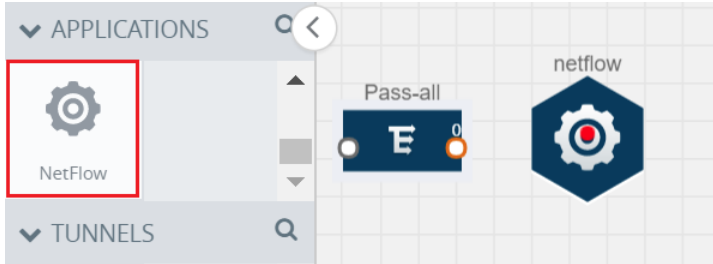
	Description	Supported NetFlow Versions
Flow Start Sec	Configures the absolute timestamp of the first packet of this flow as a non-key field.	IPFIX
Flow Startup Time	Configures the flow start SysUp time as a non-key field.	v9 and IPFIX
Flow		
Flow End Reason	Configures the reason for Flow termination as a non-key field.	IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP message as a non-key field.	v9 and IPFIX
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 ICMP Type	Configures the type of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a non-key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a non-key field.	IPFIX
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9
IP Version	Configures the IP version field in the IP packet header as a key field.	v9
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a non-key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport header as a non-key field.	v9 and IPFIX

	Description	Supported NetFlow Versions
TCP Ack Number	Configures the acknowledgment number in the TCP header as a non-key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a non-key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a non-key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a non-key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP header as a non-key field.	IPFIX
TCP Src Port	Configures the source port identifier in the TCP header as a non-key field.	IPFIX
TCP Urgent	Configures the urgent pointer in the TCP header as a non-key field.	IPFIX
TCP Window Size	Configures the window field in the TCP header as a non-key field.	IPFIX
UDP Dest Port	Configures the destination port identifier in the UDP header as a non-key field.	IPFIX
UDP Src Port	Configures the source port identifier in the UDP header as a non-key field.	IPFIX

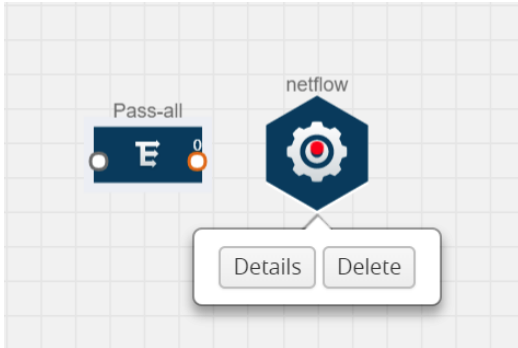
Add Version 5 NetFlow Application

To add a version 5 NetFlow application:

1. Drag and drop **NetFlow** from **APPLICATIONS** to the graphical workspace.



2. Click the NetFlow application and select **Details**. A quick view is displayed for configuring the NetFlow application.



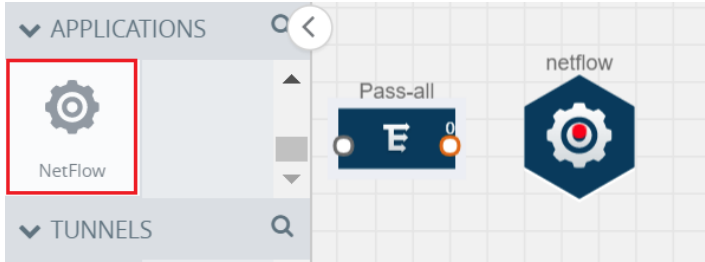
3. In the **Alias** field, enter a name for the v5 NetFlow application.
4. For State, select the **On** check box to determine that the application is currently running. Select the **Off** check box to determine that the application is currently not running. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select v5.
6. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.
7. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.
8. Click **Save**.

For more examples demonstrating the NetFlow application configuration in the GigaVUE V Series nodes, refer to [NetFlow Examples](#).

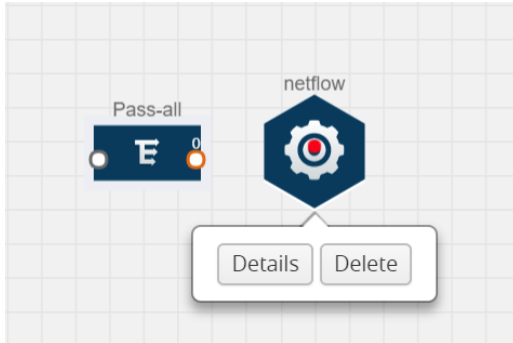
Add Version 9 and IPFIX NetFlow Application

To add a v9 and IPFIX NetFlow application:

1. Drag and drop **NetFlow** from **APPLICATIONS** to the graphical workspace.



2. Click the NetFlow application and select **Details**. A quick view is displayed for configuring the NetFlow application.



3. In the **Alias** field, enter a name for the NetFlow application.
4. For State, select the **On** check box to determine that the application is generating NetFlow records from the packets coming from the G-vTAP Agents. Select the **Off** check box to determine that the application is not currently generating NetFlow records. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select the version you want to use to generate the NetFlow records. The default version selected is v5.
6. In the **Source ID** field, enter the observation domain to isolate the traffic. The NetFlow application uses source ID to segregate the records into categories. For example, you can assign source ID 1 for traffic coming over TCP. This results in generating a separate NetFlow record for TCP data. Similarly, you can assign Source ID 2 for traffic coming over UDP. This results in generating a separate NetFlow record for UDP data.
7. From the **Match fields** drop-down list, select the parameters that identify what you want to collect from the incoming packets. The Match fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to [Match/Key Fields](#).
8. From the **Collect fields** drop-down list, select the parameters that identify what you want to collect from the NetFlow records. The Collect fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to [Collect/Non-Key Fields](#).
9. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.
10. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.

11. In **Template refresh interval**, enter the frequency at which the template must be sent to the tool. The default value is 1800 seconds.
12. Click **Save**.

For some examples demonstrating the NetFlow application configuration in the GigaVUE V Series nodes, refer to [NetFlow Examples](#).

Network Address Translation (NAT)

NAT allows the NetFlow records to be directly transmitted to a collector without a tunnel

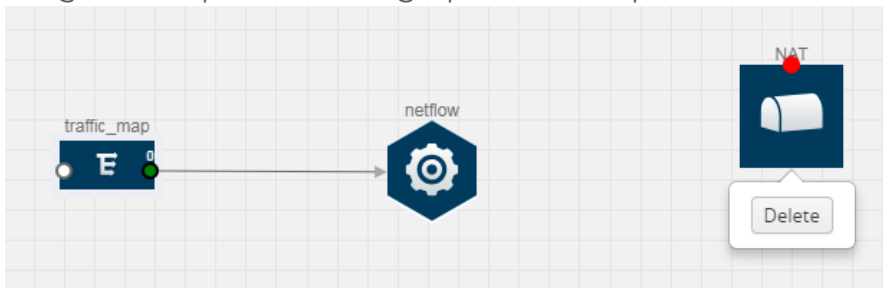
The NetFlow records are exported to the collector over UDP protocol with the configurable source IP and destination IP.

NOTE: Only one NAT can be added per monitoring session.

Add NAT and Link NetFlow Application to NAT

To add a NAT device and create a link from a NetFlow application to a NAT device:

1. Drag and drop **NAT** to the graphical workspace.



2. Drag and drop a link from the NetFlow application to a NAT device. A Link quick view is displayed. It is a header transformation operation that lets you configure the IPv4 destination IP of the NetFlow collector.

X
Link
Save

Alias:

Link_abc

Source type:

Application

Destination type:

Tunnel

Transformations:

Add a transformation

IPv4 Destination

10.2.2.23

X

Destination Port

0 to 65535

X

3. Creating a Link from NetFlow to NAT
4. In the **Alias** field, enter a name for the link.

5. From the **Transformations** drop-down list, select any one of the header transformations:
 - IPv4 Destination
 - ToS
 - Destination Port

NOTE: Only the above three header transformations are allowed on the link from the NetFlow application to a NAT device.

6. In **IPv4 Destination**, enter the IP address of the NetFlow collector.
7. (Optional) By default, the Destination Port is 2055. To change the destination port, enter a port number.
8. Click **Save**. The transformed link is displayed in Orange.
9. Repeat steps 7 to 10 to send additional NetFlow records to NAT.

NetFlow Examples

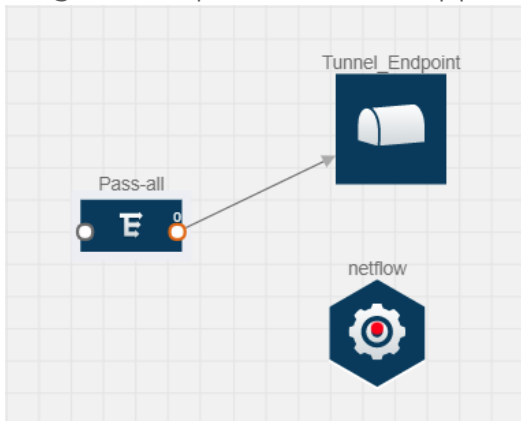
This section provides an example to demonstrate the NetFlow application configuration in the GigaVUE V Series nodes. Refer [Example 1](#) below.

Example 1

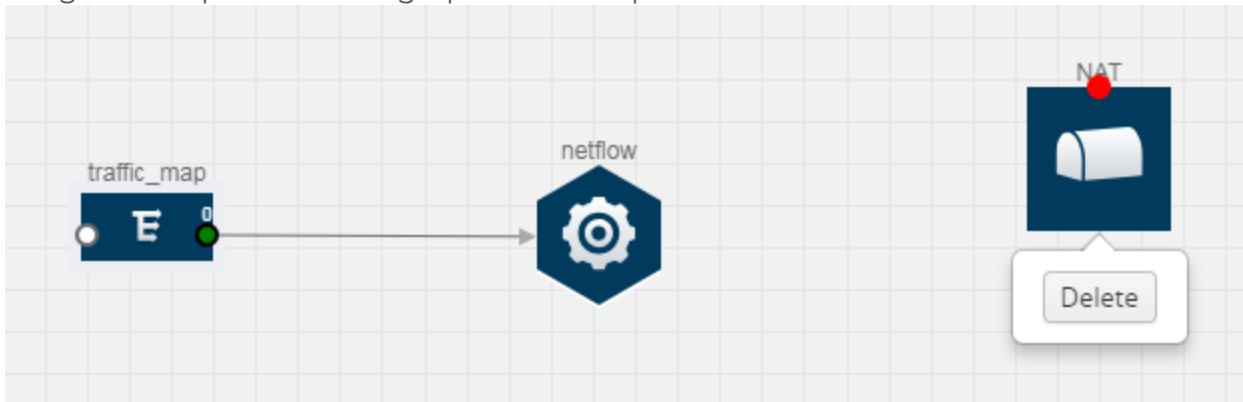
In this example, a pass all map is created and the entire traffic from a VPC is sent to a tool for full packet inspection. At the same time, a NetFlow application is added to generate flow records for flow inspection.

1. Create a monitoring session.
2. In the monitoring session, create a Pass all map. A pass all map sends all the traffic received from the G-vTAP Agents to the tunnel endpoint or NAT.
3. Drag and drop a tunnel from **Tunnels**. A tunnel encapsulates the flow records and then sends them to the tools for full packet inspection.
4. Create a link from the Pass-all map to the tunnel endpoint. The traffic from the Pass-all map is forwarded to the tunnel endpoint that is connected to a tool.

5. Drag and drop a v5 NetFlow application.



6. Click the NetFlow application and select **Details**. The Application quick view is displayed. For steps to configure the v5 NetFlow application, refer to [Add Version 5 NetFlow Application](#).
7. Create a link from the Pass all map to the v5 NetFlow application.
8. Drag and drop **NAT** to the graphical workspace.



9. Create a link from the v5 NetFlow application to NAT. The link must be configured with the destination IP address of the NetFlow collector and the GigaVUE V Series node interface. For steps to configure the link, refer to [Add Applications to Monitoring Session](#).
10. Click on the link created from the v5 NetFlow application to NAT. The information about the NetFlow collector destination IP and port is displayed.

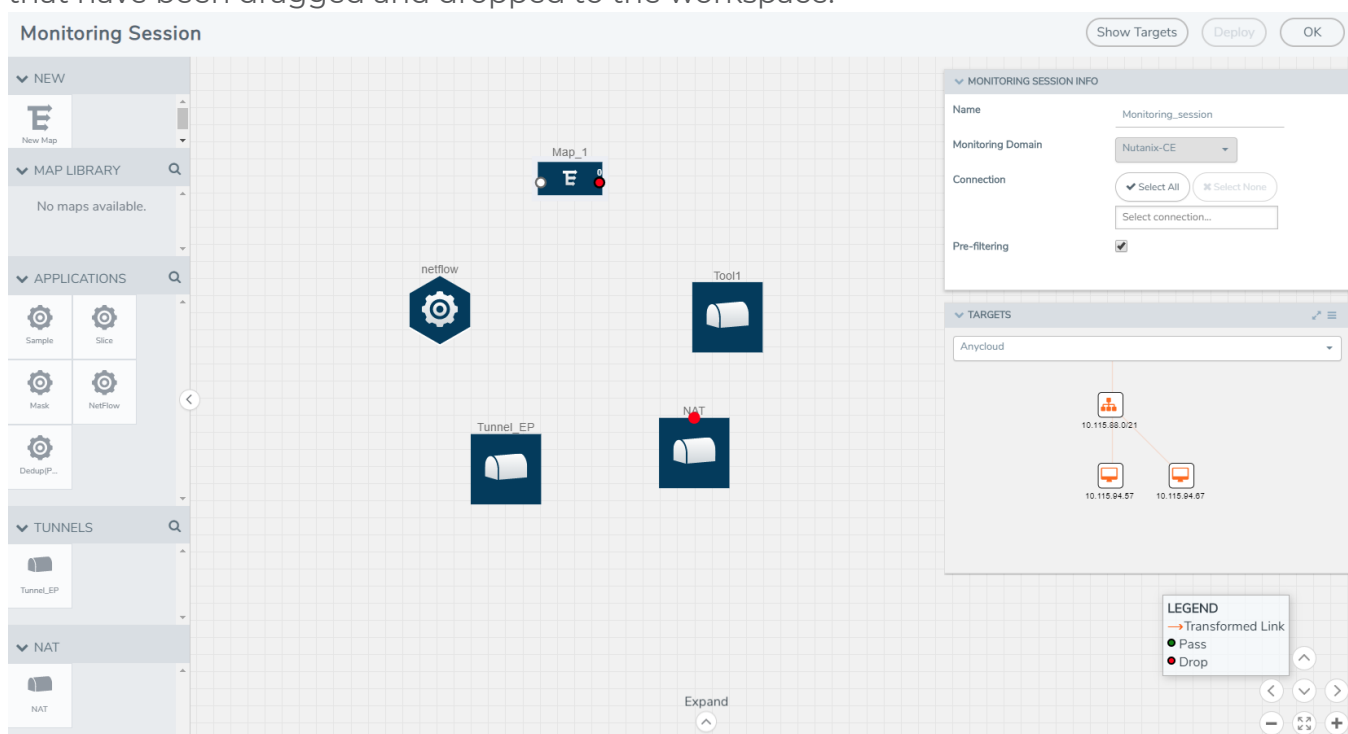
Deploy the Monitoring Session

To deploy the monitoring session:

1. Drag and drop one or more maps from the **MAP Library** to the workspace.
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. (Optional) Drag and drop one or more applications from the **APPLICATIONS** section to the workspace.

NOTE: For information about adding applications to the workspace, refer to [Adding Applications to the Monitoring Session](#).

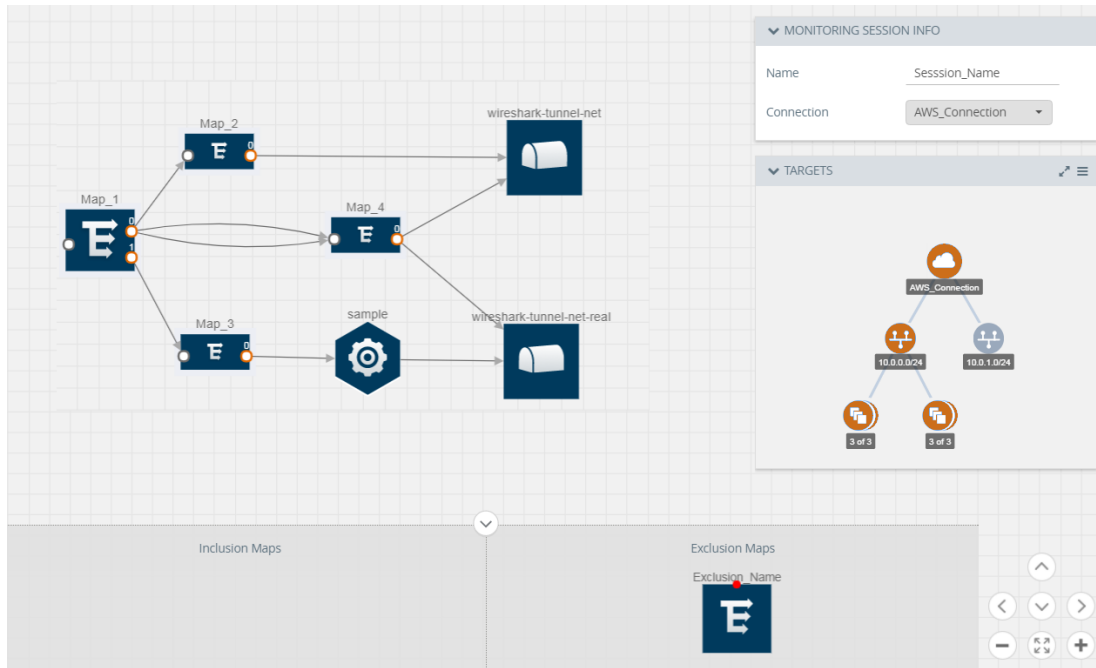
4. Drag and drop one or more tunnels from the **TUNNELS** section. The following figure illustrates three maps, one exclusion map, one application, and two tunnel endpoints that have been dragged and dropped to the workspace.



5. Hover your mouse on the map, click the red dot, and drag the link over to another map, application, or tunnel. You can drag more than one link from a map to the destination. On these links, you can apply link transformation to alter the packets. For information about adding link transformation, refer to [Add Header Transformations](#).
6. Hover your mouse on the map, click the red dot, and drag the arrow over to another map, application, or tunnel.

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

7. Hover your mouse on the application, click the red dot, and drag the arrow over to the tunnel endpoints. In the following figure, the traffic matching the rules in each action set is routed to maps, applications, or monitoring tools.



8. Click **Show Targets** to view details about the subnets and monitoring instances. The instances and the subnets that are being monitored are highlighted in blue.
9. 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 V Series nodes and G-vTAP Agents. 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 G-vTAP or V Series node failure.
- Failure—The session is not deployed on any of the V Series nodes and G-vTAP Agents.

If there was an error in deploying, the Monitoring Session Deployment Report will display the information about it.

NOTE: After rebooting your Ubuntu, you must redeploy the respective monitoring sessions to restore the mirror traffic on the respective Ubuntu VM interfaces.

The Monitoring Session page also has the following buttons:

- **Redeploy**—Redeploys the selected monitoring session.
- **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.
- **Apply Template**—Adds a Prefiltering template for the selected monitoring session.

Add Header Transformations

Header transformation is performed on a link in a monitoring session. You can select a link and modify the packet header before they are sent to the destination. The header transformation feature is supported only with GigaVUE V Series node version 1.3-1 and above.

Header transformations are used to perform many simple operations on the network packets. The source and destination MAC addresses, port numbers, and IP addresses can be masked to prevent the information from being exposed to the monitoring tools.

The monitoring tools cannot always distinguish the traffic coming from multiple VNets with the same subnet range. You can add VLAN ID, VLAN priority, and DSCP bits to the header for distinguishing the traffic coming from multiple VNets with the same subnet range.

In addition to header transformation, GigaVUE V Series node allows you to add multiple links to the same destination. Using multiple links, you can send duplicate packets or various transformed packets to the same destination. For example, you can add different L2GRE or VXLAN tunnel IDs to the packets and send them to different applications within the same tool.

The filtered packets from the ICMP map are sent to the same tunnel endpoint in four different links. In each link, you can apply one or more header transformations. A link with the header transformation applied is displayed in orange. When you mouse over the orange link, a detailed information about the alias and the type of transformation is displayed.

GigaVUE V Series node supports the following header transformations:

Option	Description
MAC Source	Modify the Ethernet source address.
MAC Destination	Modify the Ethernet destination address.

Option	Description
VLAN Id	Specify the VLAN ID.
VLAN PCP	Specify the VLAN priority.
Strip VLAN	Strip the VLAN tag.
IPv4 Source	Specify the IPv4 source address.
IPv4 Destination	Specify the IPv4 destination address.
ToS	Specify the DSCP bits in IPv4 traffic class.
Source Port	Specify the UDP, TCP, or SCTP source port.
Destination Port	Specify the UDP, TCP, or SCTP destination port.
Tunnel ID	Specify the tunnel ID. The tunnel ID header transformation can only be applied on the links with the tunnel endpoint destination. Using Tunnel ID header transformation, the filtered packets can be sent to different applications or programs within the same monitoring tool.

To add a header transformation:

1. On the Monitoring Session, click the link and select **Details**. The Link quick view is displayed.
2. From the **Transformations** drop-down list, select one or more header transformations.

NOTE: Do not apply VLAN Id and VLAN PCP transformation types with the Strip VLAN ID transformation type on the same link.

3. Click **Save**. The selected transformation is applied to the packets passing through the link.
4. Click **Deploy** to deploy the monitoring session.

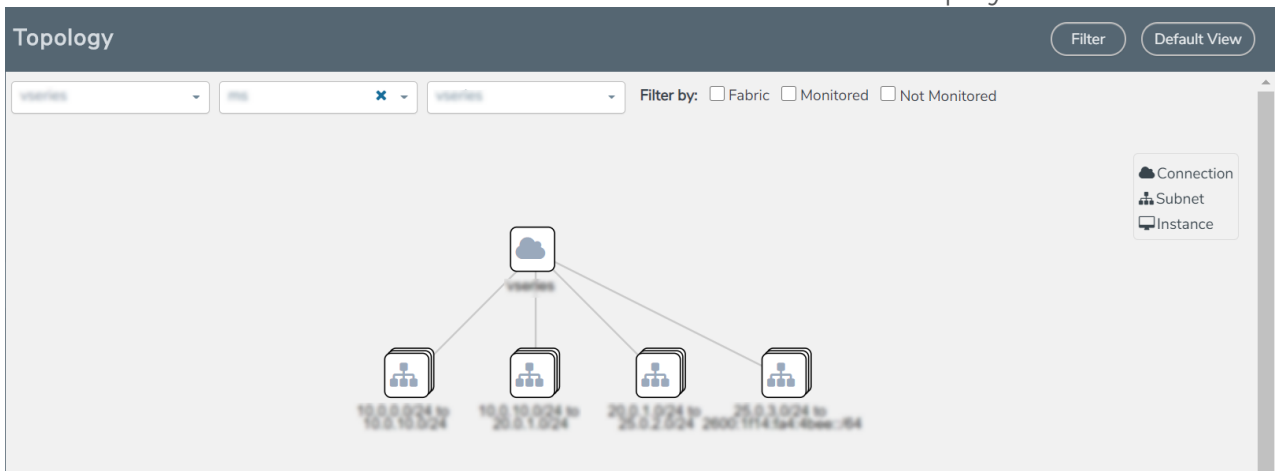
Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.

4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



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

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

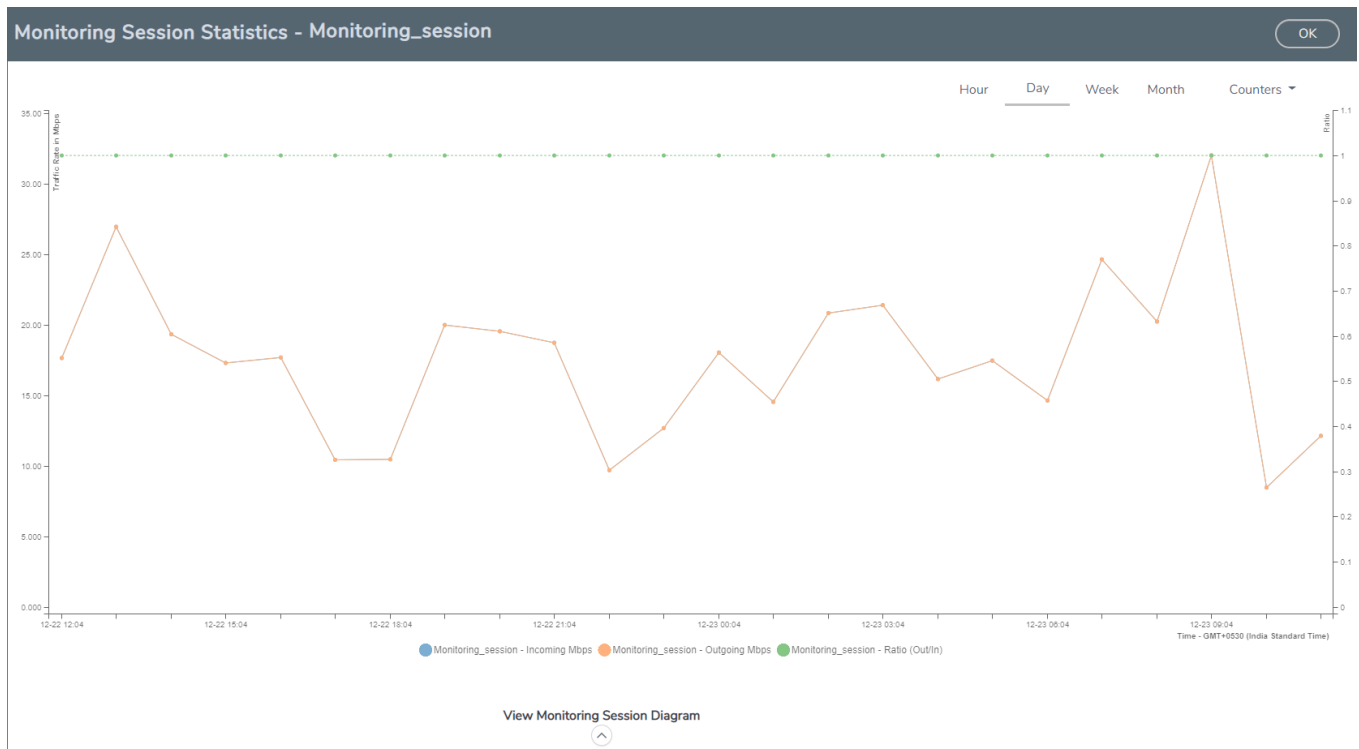
- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the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

View Monitoring Session Statistics

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

On the Monitoring Sessions page, click **View** in the Statistics column to view the Monitoring Session Statistics page. The **Monitoring Session Statistics** page appears where you can analyze incoming and outgoing traffic.

NOTE: If there are multiple monitoring sessions with different target selection, then the incoming maps will not show true statistics and it shows the aggregate traffic from all the targets.



You can also perform the following actions on the Monitoring Session Statistics page:

- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.
- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.
- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the V Series Node for which you want to view the statistics from the V Series Node drop-down menu on the top left-corner of the Monitoring Session Statistics page.
- Hover over the V Series Node drop-down to view the number of the applications, end points, and other application environments configured for a particular V Series Node. It also displays the error message related to configuration for the particular V Series Node.

Administer GigaVUE Cloud Suite for OpenStack

You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for OpenStack:

- [Configure the OpenStack Settings](#)
- [Role Based Access Control](#)
- [About Audit Logs](#)
- [About Events](#)

Configure the OpenStack Settings

To configure the OpenStack Settings:

1. Go to **Inventory > VIRTUAL > OpenStack**, and then click **Settings**.
2. Click **Settings** drop-down, and then select **Advanced Settings**.
3. Click **Edit** to edit the Advanced Settings fields.

Refresh interval for VM target selection inventory (secs)	120
Refresh interval for fabric deployment inventory (secs)	900
Number of G-vTap Agents per V Series Node	100
Number of hypervisors per V Series Node	5
Refresh interval for G-vTAP agent inventory (secs)	900
OVS Mirror tunnel range start	10000
OVS Mirror tunnel range end	30000

Refer to the following table for descriptions of the Settings fields.

Settings	Description
Refresh interval for VM target selection inventory (secs)	Specifies the frequency for updating the inventory of VMs in OpenStack.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the inventory of GigaVUE fabrics in OpenStack.
Number of G-vTAP Agents per V Series Node (applicable only for G-vTAP based connections)	Specifies the maximum number of instances that can be assigned to the V Series node.

Settings	Description
Number of hypervisors per V Series Node (applicable only for OVS mirroring)	Specifies the maximum number of hypervisors that can be assigned to the V Series node.
Refresh interval for G-vTAP Agent inventory (secs)	Specifies the frequency for discovering the G-vTAP Agents available in the project. This is applicable for G-vTAP Agents only.
OVS Mirror tunnel range start	Specifies the startup range value of the OVS mirror tunnel ID. This is applicable for G-vTAP OVS Agents only.
OVS Mirror tunnel range end	Specifies the closing range value of the OVS mirror tunnel ID. This is applicable for G-vTAP OVS Agents only.

NOTE: A maximum of 100 OpenStack connections are allowed for an OpenStack module.

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
Physical Device Infrastructure Management: This includes the following cloud infrastructure resources: <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
Traffic Control Management: This includes the following traffic control resources: <ul style="list-style-type: none"> • Monitoring session • Threshold Template • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps 	<ul style="list-style-type: none"> • Create, Clone, and Deploy Monitoring Session • Create and Apply Threshold Template • 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.

About Audit Logs

Audit logs track the changes and activities that occur in the virtual nodes due to user actions. The logs can be filtered to view specific information.

Navigate to **Dashboard > SYSTEM > Audit Logs**. The **All Audit Logs** page appears.

All Audit Logs Filter Manage

Filter : none

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

< < Go to page: 1 of 16 > > Total Records: 106

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: <ul style="list-style-type: none"> Log in and Log out based on users. Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

NOTE: Ensure that the GigaVUE-FM time is set correctly to ensure accuracy of the trending data that is captured.

Filtering the audit logs allows you to display specific type of logs. You can filter based on any of the following:

- **When:** display logs that occurred within a specified time range.
- **Who:** display logs related a specific user or users.
- **What:** display logs for one or more operations, such as Create, Read, Update, and so on.
- **Where:** display logs for GigaVUE-FM or devices.
- **Result:** display logs for success or failure.

To filter the audit logs, do the following:

1. Click **Filter**. The quick view for Audit Log Filters displays.
2. Specify any or all of the following:
 - **Start Date** and **End Date** to display logs within a specific time range.
 - **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
 - **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
 - **Where** narrows the logs to particular of system that the log is related to, either FM or device. Select **All Systems** apply both FM and device to the filter criteria.
 - **Result** narrows the logs related to failures or successes. Select All Results to apply both success and failure to the filter criteria.
3. Click **OK** to apply the selected filters to the Audit Logs page.

About Events

The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- Cloud provider License Expiry
- G-vTAP Agent Inventory Update Completed
- Cloud provider Connection 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. An example of alarm could be your cloud provider license expiry.

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

Navigate to **Dashboard > SYSTEM > Events**. The Event page appears.

Events
Filter
Manage

Events: 60 | Filter : none

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

<>
<
 Go to page: 1 of 9 >
>>
 Total Records: 60

The following table describes the parameters recording for each alarm or event. You can also use filters to narrow down the results.

Controls/ Parameters	Description
Source	The source from where the alarms and events are generated.
Time	<p>The timestamp when the event occurred.</p> <div> IMPORTANT: Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured timezone. </div>
Scope	The category to which the alarms or events belong. Alarms and events can belong to the following category: Virtual Fabric Node, VM Domain, VM Manager.
Event Type	The type of event that generated the alarms and events.
Severity	<p>The severity is one of Critical, Major, Minor, or Info.</p> <p>Info is informational messages. For example, when GigaVUE V Series nodes are installed, such a message is displayed as Info.</p>
Affected Entity Type	The resource type associated with the alarm or event.
Affected Entity	The resource ID of the affected entity type.
Description	The description of the event, which includes any of the possible notifications with additional identifying information where appropriate.
Device IP	The IP address of the device.
Host Name	The host name of the device.

To filter the alarms and event:

1. Click **Filter**. The Filter quick view is displayed.
2. Select the filtering criteria, then click **Apply Filter**. The results are displayed in the Events page.

GigaVUE-FM Version Compatibility Matrix

The following tables list the different versions of GigaVUE Cloud Suite Cloud solution components available with different versions of GigaVUE-FM.

NOTE: GigaVUE-FM version 6.3 supports the latest fabric components version as well as (n-2) versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

GigaVUE-FM	G-vTAP Agent	G-vTAP OVS Agent	G-vTAP Controller	GigaVUE V Series Controller	GigaVUE V Series 1 Nodes
6.3.00	v6.3.00	v6.3.00	v6.3.00	v1.7-4	v1.7-4
6.2.00	v6.2.00	v6.2.00	v6.2.00	v1.7-4	v1.7-4
6.1.00	v6.1.00	v6.1.00	v6.1.00	v1.7-4	v1.7-4
6.0.00	v1.8-7	v1	v1.8-7	v1.7-4	v1.7-4
5.16.00	v1.8-5	v1	v1.8-5	v1.7-3	v1.7-3
5.15.00	v1.8-5	v1	v1.8-5	v1.7-2	v1.7-2
5.14.00	v1.8-4	v1	v1.8-4	v1.7-1	v1.7-1
5.10.01, 5.11.00, 5.11.01, 5.12.00, 5.13.00, 5.13.01, 5.14.00	v1.7-1	v1	v1.7-1	v1.7-1	v1.7-1

Troubleshooting

This section provides the information needed to troubleshoot GigaVUE-FM integration with OpenStack.

OpenStack Connection Failed

The connFailed state indicates that the OpenStack connection has failed. Check the following troubleshoot tips to restore the connection:

- Verify if GigaVUE-FM is able to reach the OpenStack cloud controller.
- Check if the OpenStack cloud controller is DNS resolvable from GigaVUE-FM.
- Verify if the region name provided while launching the instance is accurate.
- Ensure that all the security group rules required for communication between GigaVUE-FM and OpenStack cloud controller OR GigaVUE-FM and DNS server are accurately setup.
- Check if the Compute Servers that the nova API returns are reachable from GigaVUE-FM. Refer to [Handshake Alert: unrecognized_name](#).

Handshake Alert: unrecognized_name

When setting up the OpenStack connection in GigaVUE-FM, the GigaVUE-FM logs might show a handshake alert: unrecognized_name error. This error is related to a Server Name Indication (SNI) error. Starting with Java 7, the JDK does not ignore the unrecognized name warning. To resolve this issue, perform either of the following:

- Fix the configuration on the server where the error is occurring.
- Ignore the warning on the client side (GigaVUE-FM server) by using the Java system property `--Djsse.enableSNIExtension=false` while launching GigaVUE-FM.

Contact support for information on how to use the Java system property. However, this is not recommended for security reasons.

GigaVUE V Series Node or G-vTAP Controller is Unreachable

If GigaVUE V Series node or G-vTAP controller is unreachable, verify the following:

- The correct version of the image is uploaded.
- The network is reachable.

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 6.3 Hardware and Software Guides	
DID YOU KNOW?	If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware	how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
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 Cloud Suite 6.3 Hardware and Software Guides	
GigaVUE-TA200 Hardware Installation Guide	
GigaVUE-TA200E Hardware Installation Guide	
GigaVUE-TA400 Hardware Installation Guide	
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 for AWS–GigaVUE V Series 2 Guide	
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide	
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide	
*GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide	
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide	
*GigaVUE Cloud Suite for Third Party Orchestration	
GigaVUE Cloud Suite for AnyCloud Guide	
Universal Container Tap Guide	

GigaVUE Cloud Suite 6.3 Hardware and Software Guides

Gigamon Containerized Broker Guide

GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide

GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide

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 for AWS Secret Regions Guide

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)