GigaVUE Cloud Suite for OpenStack Configuration Guide

GigaVUE Cloud Suite

Product Version: 5.10

Document Version: 2.0

(See Change Notes for document updates.)

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
5.10.01	2.0	08/28/2020	Fixed formatting and cross-references issues, and streamlined instructions throughout the guide.
5.10.00	1.0	08/14/2020	Original release of this document with 5.10.00 GA.

Contents

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 Gigamon 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.

Topics:

- GigaVUE Cloud Suite Cloud Components
- Traffic Capturing Mechanism
- Configuring the Components in OpenStack
- Configuring Monitoring Sessions
- Compatibility Matrix
- Troubleshooting

GigaVUE Cloud Suite Cloud Components

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-premise or launched from an OpenStack image. GigaVUE-FM manages the configuration of the following visibility components in your OpenStack project:

- GigaVUE® V Series nodes
- GigaVUE® V Series Controllers
- G-vTAP Controllers (only if you are using G-vTAP agent as the traffic acquisition method)

- **G-vTAP Controller** manages multiple G-vTAP agents and orchestrates the flow of mirrored traffic to GigaVUE Cloud Suite 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 Cloud Suite V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Cloud Suite V Series Controllers to communicate with the GigaVUE Cloud Suite V Series nodes.
- **GigaVUE® V Series Node** is a visibility node that aggregates mirrored traffic from multiple G-vTAP agents. 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 GRE or VXLAN tunnels.

You can choose one of the following two options for configuring the components described above:

Table 1: Configuration options for Controllers and Nodes

Option 1: Standard Configuration	GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in all the projects
Option 2: Shared Controller Configuration	• GigaVUE V Series nodes are launched in all the projects • GigaVUE V Series controllers and G-vTAP controllers are launched in a shared project

Traffic Capturing Mechanism

GigaVUE Cloud Suite for OpenStack captures traffic in OpenStack cloud using G-vTAP agents, as described in this section.

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. Figure 1GigaVUE Cloud Suite Cloud Components for OpenStack using G-vTAP shows a high level architecture of Gigamon GigaVUE Cloud Suite for OpenStack using G-vTAP agents as the source for acquiring the traffic.

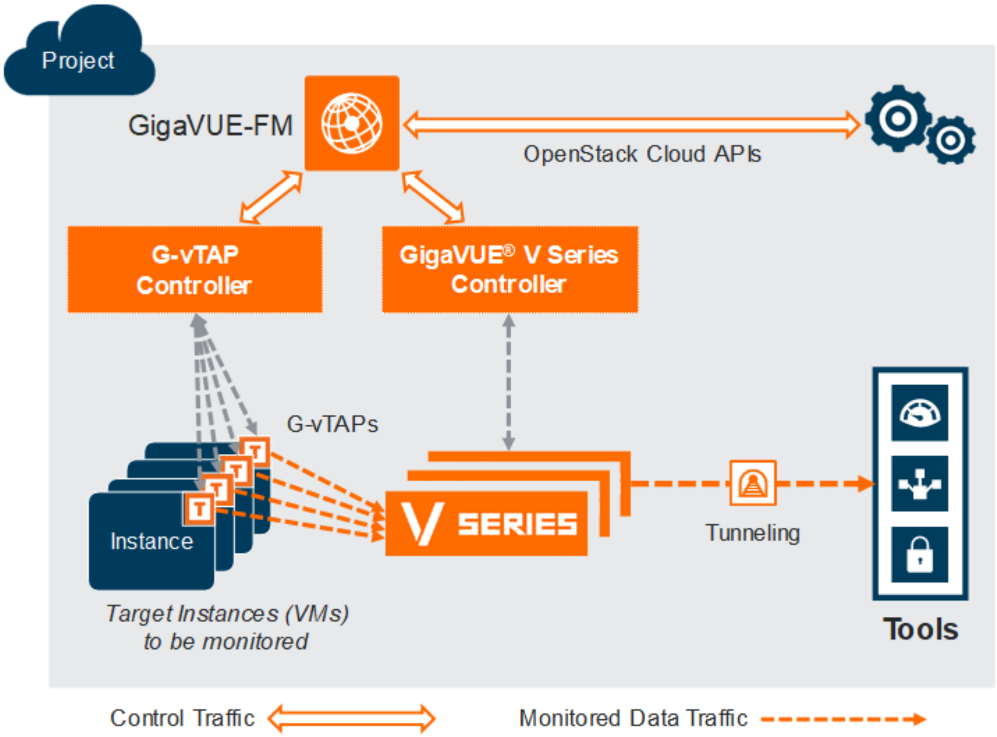


Figure 1 *GigaVUE Cloud Suite Cloud Components for OpenStack using G-vTAP*

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 Cloud Suite 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.

OpenVSwitch (OVS) Mirroring

When deploying OpenVSwitch (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 Cloud Suite 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. This G-vTAP agent must be on OpenVSwitch.

> **Note**: OVS Mirroring also supports OpenVSwitch with DPDK as a preview. The configuration steps for OVS Mirroring and OVS Mirroring with DPDK are the same.

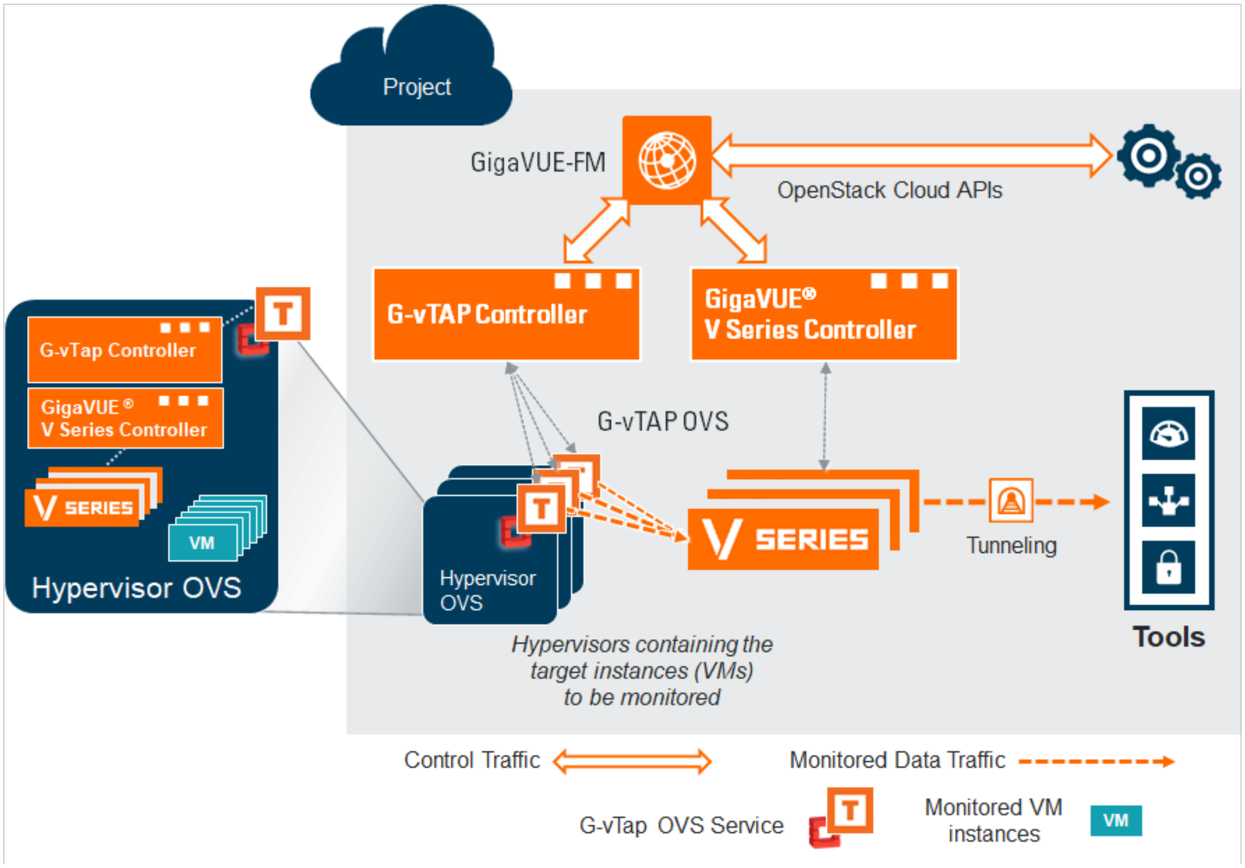


Figure 2 *GigaVUE Cloud Suite Cloud Components for OpenStack using OVS Mirroring or OVS Mirroring + DPDK*

OVS Mirroring Prerequisites

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

- An existing OpenStack cloud environment should be available with admin login credentials
- 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. Refer to OpenStack Role Privileges Required to Enable OVS Mirroring for the elevated privileges required.
- A working GigaVUE-FM with latest build.
- OpenStack Cloud Environment Requirements:
    - OpenStack Version: Rocky and above.
    - Ubuntu Version 16.04 and above or RedHat version 7.6 and above.
    - ML2 mechanism driver: OpenVSwitch

Tip: If the OpenStack CLI 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 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: gigamon-hv-1 : 10.120.10.2

OpenStack Role Privileges Required 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

OpenVSwitch (OVS) Mirroring + DPDK

Note: OVS Mirroring also supports OpenVSwitch with DPDK as a preview. The configuration steps for OVS Mirroring and OVS Mirroring with DPDK are the same. See instructions for OVS Mirroring throughout this guide when testing OVS Mirroring + DPDK.

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 Configuring the Components in 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 Customer Portal.

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 for OpenStack works on the same principles of access privileges in GigaVUE-FM in which the access rights of a user depends on the following:

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

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

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

NOTE: Cloud APIs are also RBAC enabled.

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

Configuring the Components in OpenStack

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
- Uploading the Images
- Launching the GigaVUE-FM Instance
- Installing the G-vTAP Agents
- Configuring the GigaVUE Cloud Suite Cloud in OpenStack

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
- Network Requirements
- Virtual Network Interface Cards (vNICs)
- Security Group
- Key Pairs

Supported Hypervisor

Table 1: Hypervisor for OpenStack lists the hypervisor with the supported versions for G-vTAP.

Table 1: Hypervisor for OpenStack

Hypervisor	Version
KVM	**G-vTAP**cPike, Queens, Ocata, Newton, Mitaka, and Liberty **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.

Table 2: Minimum Compute Requirement

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.
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
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

Table 3: Types of Networks lists the recommended requirements to setup the network topology.

Table 3: Types of Networks

Network	Purpose
Management	Identify the Network Interface Card (NIC) that GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data	Identify the Network Interface Card (NIC) that receives the mirrored GRE tunnel traffic from the monitored instances. This is applicable only for G-vTAP agents.

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.

Security Group

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE Cloud Suite V Series Controllers, GigaVUE Cloud Suite V Series nodes, and G-vTAP Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

It is recommended to create a separate security group for each component using the rules and port numbers listed in the Security Group Rules table.

The Security Group Rules table lists the rules and port numbers for each component.

Table 4: Security Group Rules

Direction	Ether Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	HTTPS	TCP	443	Any IP address	Allows G-vTAP Controllers, GigaVUE Cloud Suite V Series Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	IPv4	UDP	68	Any IP address	Allows GigaVUE-FM to communicate with DHCP server for assigning IP addresses and other related configuration information such as the subnet mask and default gateway
Inbound	IPv4	UDP	53	Any IP address	Allows GigaVUE-FM to communicate with DNS server for resolving the host name of the cloud controller for OpenStack
G-vTAP Controller					
Inbound	IPv4	TCP	9900	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with G-vTAP Controllers
G-vTAP Agent					
Inbound	IPv4	TCP	9901	G-vTAP Controller IP address	Allows G-vTAP Controllers to communicate with G-vTAP agents
Inbound	IPv4	TCP	9902	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite V Series Controllers
Inbound	Custom TCP Rule	TCP(6)	9903	GigaVUE Cloud Suite V Series Controller IP address	Allows GigaVUE Cloud Suite V Series Controllers to communicate with GigaVUE Cloud Suite V Series nodes
GRE Traffic					

Direction	Ether Type	Protocol	Port	CIDR	Purpose
Inbound	Custom Protocol Rule	GRE (47)	47	Any IP address	Allows mirrored traffic from G-vTAP agents to be sent to GigaVUE Cloud Suite V Series nodes using the L2 GRE or VXLAN tunnel Allows monitored traffic from GigaVUE Cloud Suite V Series nodes to be sent to the monitoring tools using the L2 GRE or VXLAN tunnel
VXLAN Traffic					
Inbound	Custom UDPRule	UDP	4789	Any IP address	Allows mirrored traffic from G-vTAP agents to be sent to GigaVUE Cloud Suite V Series nodes using the VXLAN tunnel Allows monitored traffic from GigaVUE Cloud Suite V Series nodes to be sent to the monitoring tools using the VXLAN tunnel

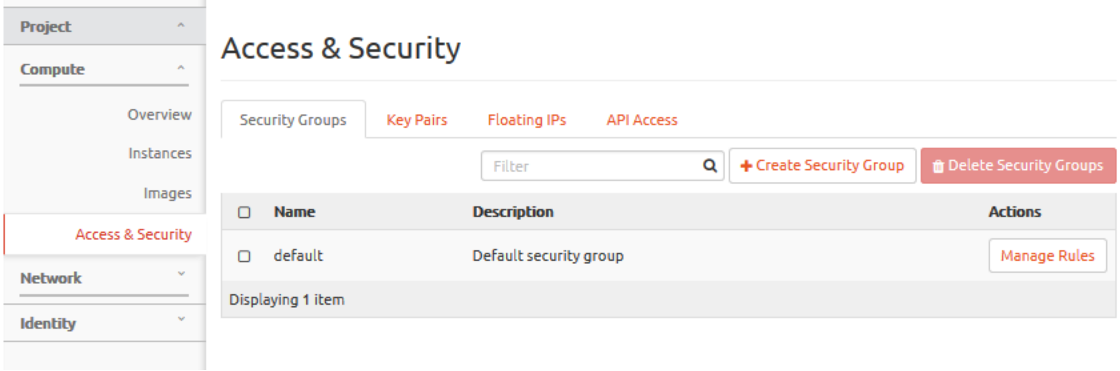
NOTE: The Security Group Rules table lists only the ingress rules. Make sure the egress ports are open for communication.

Along with the ports listed in the Security Group Rules table, make sure the suitable ports required to communicate with Service Endpoints such as Identity, Compute, and Cloud Metadata are also open.

Create a Security Group

To create an inbound security group for a component:

1. In OpenStack, click **Access & Security**.
2. Click the **Security Groups** tab.

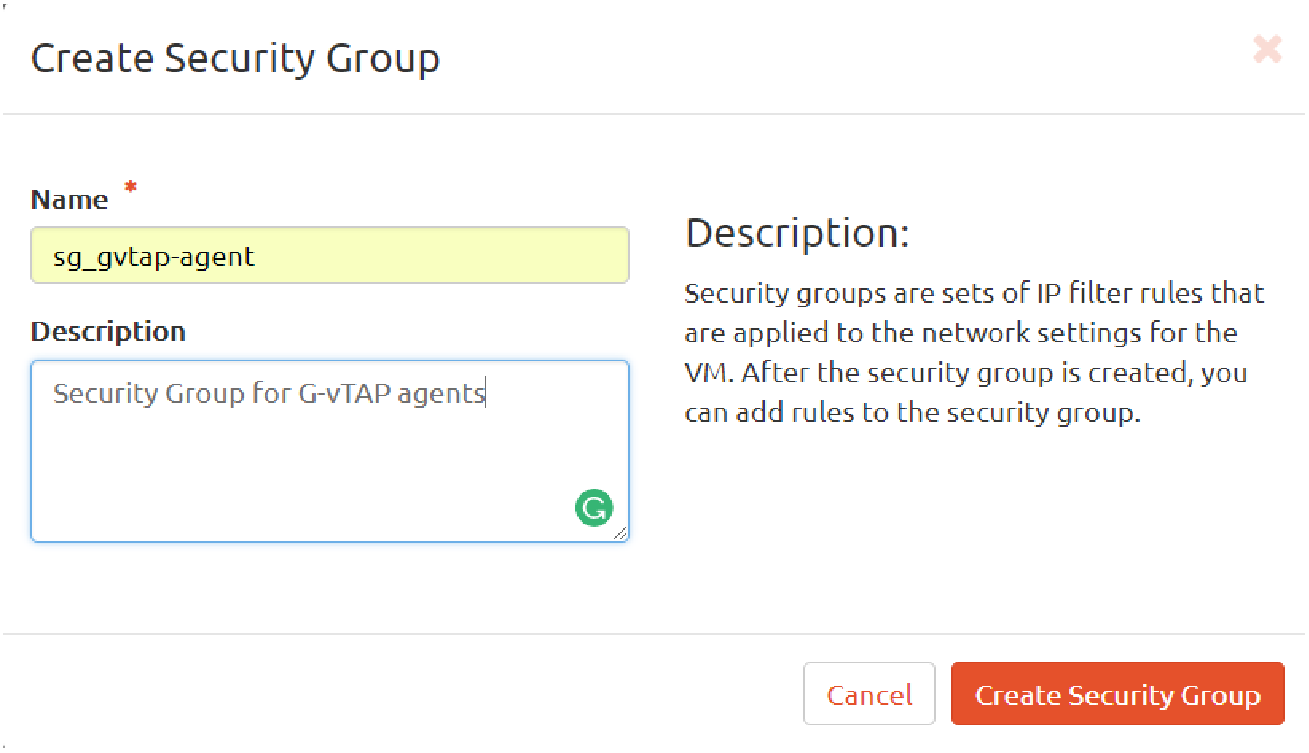


☐	Name	Description	Actions
☐	default	Default security group	Manage Rules

Displaying 1 item

3. Click **Create Security Group** .

4. Enter a name and description in the respective fields and click **Create Security Group**.



Create Security Group

Name *

sg_gvtap-agent

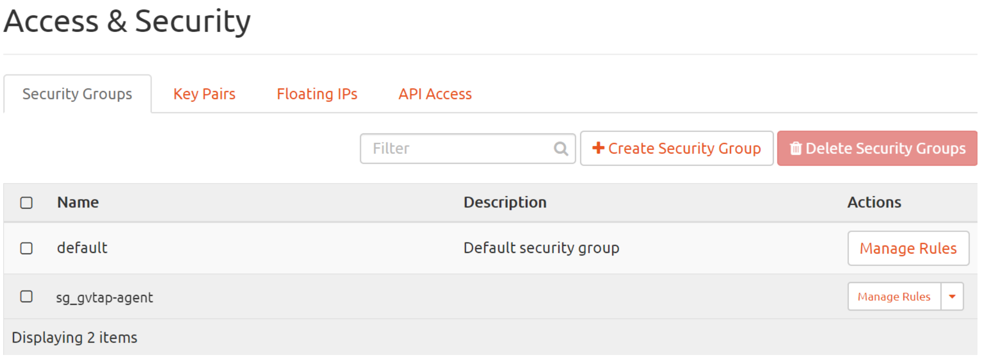
Description

Security Group for G-vTAP agents

Description:

Security groups are sets of IP filter rules that are applied to the network settings for the VM. After the security group is created, you can add rules to the security group.

The security group is created and added to the Access & Security page.

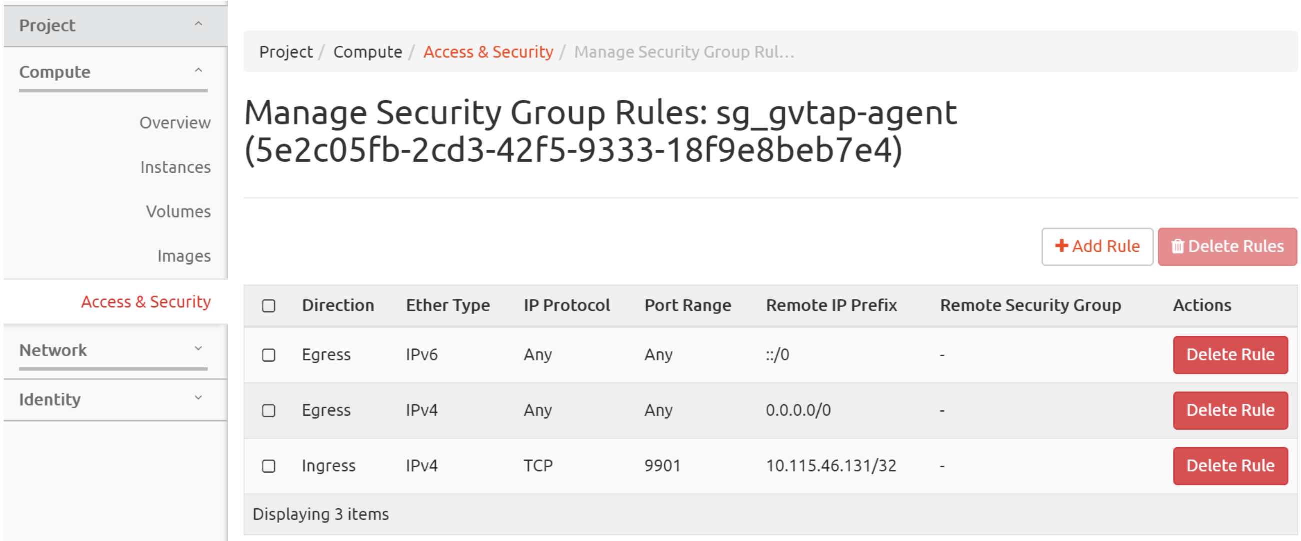


Access & Security

☐	Name	Description	Actions
☐	default	Default security group	Manage Rules
☐	sg_gvtap-agent		Manage Rules

Displaying 2 items

5. For the new security group added, click **Manage Rules**. The Manage Security Group Rules page is displayed.
6. Click **Add Rule**.The Add Rule page is displayed.
7. Enter the appropriate values in the respective fields.
8. Click **Add**. The Manage Rules page is displayed with the newly added rule.

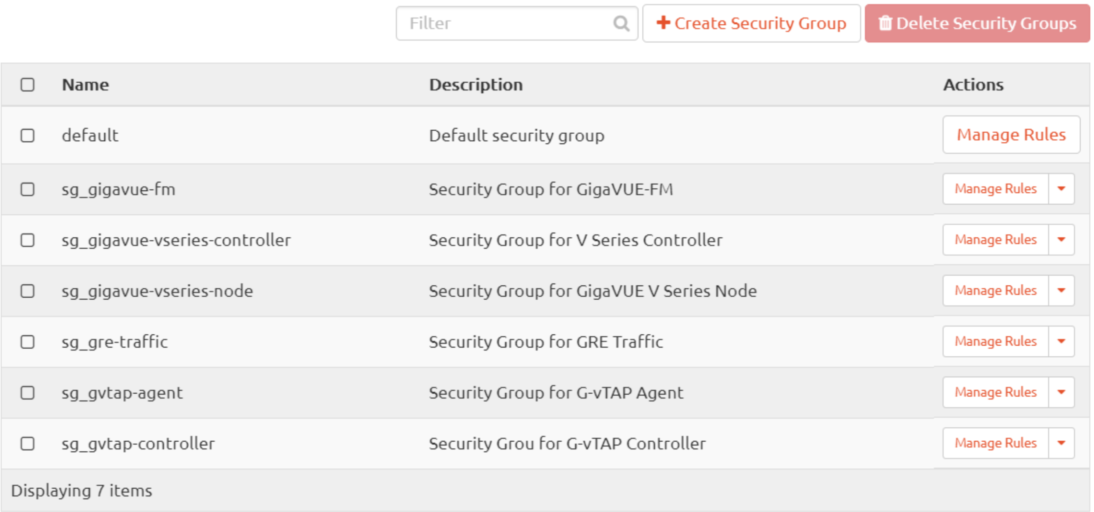


Manage Security Group Rules: sg_gvtap-agent (5e2c05fb-2cd3-42f5-9333-18f9e8beb7e4)

□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
□	Egress	IPv6	Any	Any	::/0	-	Delete Rule
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
□	Ingress	IPv4	TCP	9901	10.115.46.131/32	-	Delete Rule

Displaying 3 items

9. Repeat steps 2 to 8 to create security groups for all the components.



□	Name	Description	Actions
□	default	Default security group	Manage Rules
□	sg_gigavue-fm	Security Group for GigaVUE-FM	Manage Rules
□	sg_gigavue-vseries-controller	Security Group for V Series Controller	Manage Rules
□	sg_gigavue-vseries-node	Security Group for GigaVUE V Series Node	Manage Rules
□	sg_gre-traffic	Security Group for GRE Traffic	Manage Rules
□	sg_gvtap-agent	Security Group for G-vTAP Agent	Manage Rules
□	sg_gvtap-controller	Security Grou for G-vTAP Controller	Manage Rules

Displaying 7 items

Key Pairs

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

Uploading the 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-1.x-x -file gigamon-gigavue-vseries-cntlr-1.x-x.qcow2
```

OR

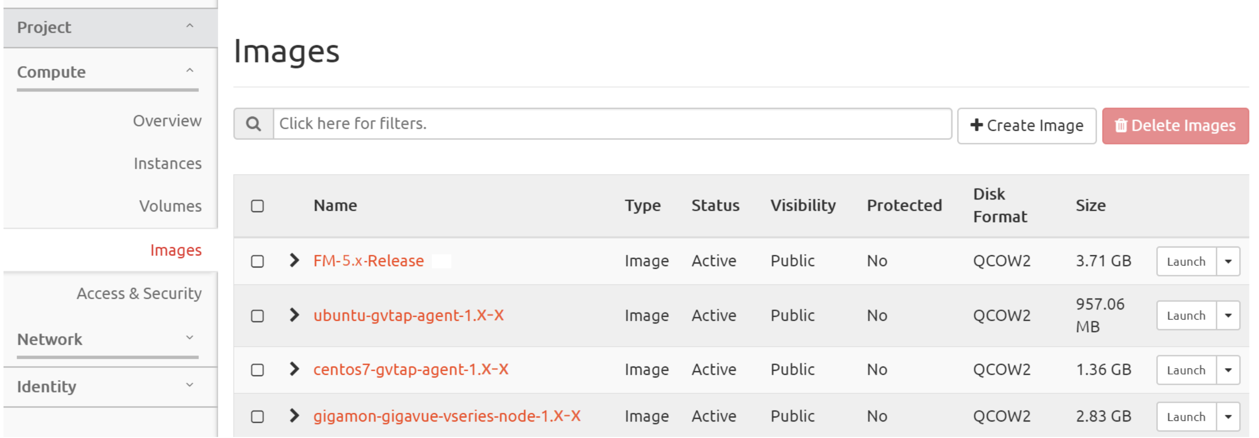
```
openstack image create --disk-format qcow2 --public --container-format bare --file gigamon-gigavue-vseries-cntlr-1.x-x gigamon-gigavue-vseries-cntlr-1.x-x.qcow2
```

> **NOTE:** The 1.x-x represents the version number of the image. Enter an appropriate version in the above commands.

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

Once the images are uploaded, they are displayed under **Compute** > **Images**.



□	Name	Type	Status	Visibility	Protected	Disk Format	Size	
□	FM-5.x-Release	Image	Active	Public	No	QCOW2	3.71 GB	Launch
□	ubuntu-gvtap-agent-1.X-X	Image	Active	Public	No	QCOW2	957.06 MB	Launch
□	centos7-gvtap-agent-1.X-X	Image	Active	Public	No	QCOW2	1.36 GB	Launch
□	gigamon-gigavue-vseries-node-1.X-X	Image	Active	Public	No	QCOW2	2.83 GB	Launch

Launching the GigaVUE-FM Instance

To launch the GigaVUE-FM instance inside the cloud:

1. Log into Horizon.
2. From the Horizon GUI, select the appropriate project, and select **Compute > Images**. The list of existing images is displayed.
3. Select the GigaVUE-FM image and click **Launch**. The Launch Instance dialog box is displayed.
4. In the **Details** tab, enter the following information and Click **Next**.

Parameter	Attribute
Instance Name	Initial hostname for the instance
Availability Zone	Availability zone where the image will be deployed.
Count	Number of instances to be launched

5. In the **Source** tab, verify that the selected GigaVUE-FM image is displayed under **Allocated** section and click **Next**.
6. In the **Flavor** tab, select a flavor complying the Minimum Compute Requirements and then move the flavor from the **Available** section to the **Allocated** section. The selected GigaVUE-FM flavor is displayed under Allocated and click **Next**.
7. In the **Networks** tab, select the specific network for the GigaVUE-FM instance from the **Available** section and then move the Network to the **Allocated** section. The selected network is displayed under Allocated and Click **Next**.
8. In the **Network Ports** tab, click **Next** again.
9. In the **Security Groups** tab, select the appropriate security group for the GigaVUE-FM instance from the **Available** section and then move the Security Group to the **Allocated** section. For information about the security groups, refer to Security Group . The selected security group is displayed under Allocated. Click **Next**.
10. (Optional) In the **Key Pair** tab, select the existing key pair from the **Available** section and then move the Key Pair to the **Allocated** section. or create a new key pair. For information about the key pairs, refer to Key Pairs. The selected key pair is displayed under Allocated. Click **Next**.
11. (Optional) In the **Configuration**, **Server Groups**, **Scheduler Hints**, **Metadata** tabs, enter/select the appropriate values and click **Next**.
12. Click **Launch Instance**. The GigaVUE-FM instance takes few minutes to fully initialize.
13. From the Horizon GUI, navigate to **Compute > Instances**. You can view the launched instance displayed in the **Instances** page. During the initial boot-up sequence, click **Associate Floating IP**. The **Manage Floating IP Associations** dialog box appears.

14. In the Manage Floating IP Associations dialog box, enter the following information and click **Associate**.

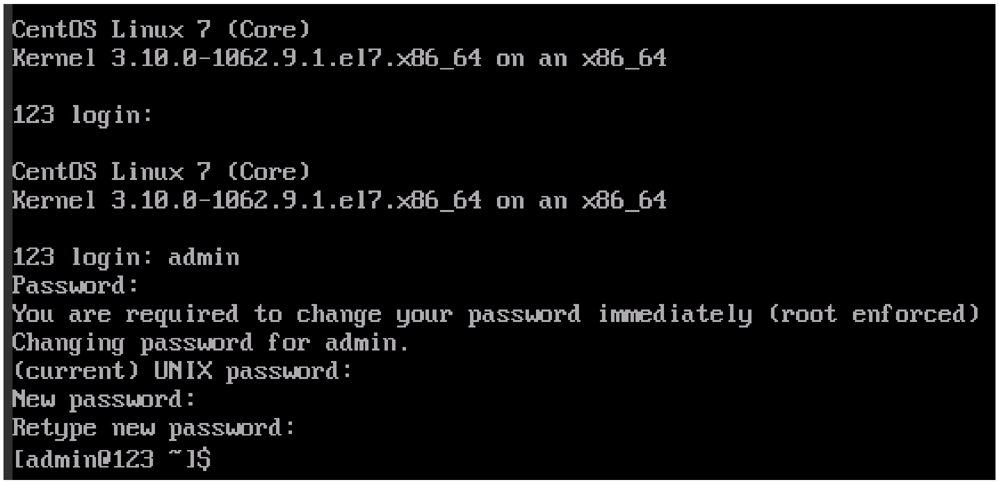
Parameter	Attribute
IP Address	Floating IP address of the instance
Port to be associated	Port for the GigaVUE-FM instance

The Floating IP is then displayed in the **IP Address** column of the corresponding Instance.

Initial GigaVUE-FM Configuration

After you have deployed a new GigaVUE-FM instance, you need to perform an initial configuration before you can start using GigaVUE-FM. This is a one-time activity that must be performed for each GigaVUE-FM instance deployed.

1. From the Horizon GUI, navigate to **Compute > Instances**.
2. In the Instances page, click the GigaVUE-FM instance name. The GigaVUE-FM instance **Overview** tab is displayed by default.
3. Click the **Console** tab and the **Instance Console** appears.
4. Log in as admin with password as admin123A! and then the console prompts you to change the default password.



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

123 login:

CentOS Linux 7 (Core)
Kernel 3.10.0-1062.9.1.el7.x86_64 on an x86_64

123 login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:
[admin@123 ~]$
```

> **NOTE:** You can also choose to perform the IP Networking and NTP configurations by running the **fmctl jump-start** command after you power on the GigaVUE-FM instance

5. To access GigaVUE-FM GUI, enter **wget -q -O - http://169.254.169.254/latest/meta-data/instance-id** command in the Instance Console and retrieve the instance ID in the format of **i-000000##** which is the default password for the admin user.

G-vTAP Agents

A 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 Cloud Suite® V Series node.

A source interface can be configured with one or more ENIs. 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.

Single vNIC Configuration

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

For example, assume that there is only one interface eth0 in the monitoring instance. 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.

Using a single vNIC as the source and the destination interface can sometimes cause increased latency in sending the traffic out from the instance.

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.

Installing the G-vTAP Agents

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

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

- Installing from an Ubuntu/Debian Package
- Installing from an RPM package

Installing from an Ubuntu/Debian Package

To install from a Debian package:

1. Download the latest version of G-vTAP Agent Debian (.deb) package from the Gigamon Customer Portal.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_1.x-x_amd64.deb
ubuntu@ip-10-0-0-246:~$ sudo dpkg -i    gvtap-agent_1.x-x_amd64.deb
```

> **NOTE:** The 1.x-x represents the version number of the G-vTAP agent. Enter the appropriate version in the configuration file.

3. 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 file contains an example, which you can use by uncommenting the last two lines. The following example registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

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 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 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. Reboot the instance.

The instance should have two interfaces. The G-vTAP agent status will be displayed as running. Check the status using the following command:

```
ubuntu@ip-10-0-0-246:~$ sudo service gvtap-agent status
G-vTAP Agent is running
```

Installing from an RPM package

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

1. Download the G-vTAP Agent RPM (.rpm) package from the Gigamon Customer Portal.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
[user@ip-10-0-0-214 ~]$ ls
 gvtap-agent_1.x-x_x86_64.rpm
[user@ip-10-0-0-214 ~]$ sudo rpm -i

 gvtap-agent_1.x-x_x86_64.rpm
```

> **NOTE:** The 1.x-x represents the version number of the G-vTAP agent. Enter the appropriate version in the configuration file.

3. Modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces.

The file contains an example, which you can use by uncommenting the last two lines. 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:

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 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 eth1 to send out the mirrored packets

4. Save the file.
5. 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
```

6. Save the G-vTAP agent running on an instance as an image. Install more number of G-vTAP agents on the deployed instances as needed.

Installing the G-vTAP OVS Agents 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.

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

- Installing the G-vTAP OVS Agent from an Ubuntu/Debian Package
- Installing the G-vTAP OVS Agents for OVS Mirroring

Installing the G-vTAP OVS Agent from an 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.x-x_amd64.deb
ubuntu@ip-10-0-0-246:~$ sudo dpkg -i    gvtap-ovs-agent_1.x-x_amd64.deb
```

> **Note:** The 1.x-x represents the version number of the G-vTAP OVS agent. Enter the appropriate version in the configuration file.

3. Once the G-vTAP OVS package is installed, start the agent:

```
$ sudo service gvtap-agent start
```

The G-vTAP OVS agent status will be displayed as running.

4. Check the status using the following command:

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

Installing the G-vTAP OVS Agent from an 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.x-x_x86_64.rpm
$ sudo rpm -ivh gvtap-ovs-agent_1.x-x_x86_64.rpm
```

> **NOTE:** The 1.x-x represents the version number of the G-vTAP agent. Enter the appropriate version in the configuration file.

3. After the installation completes, start the G-vTAP OVS agent service and verify its status.

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

Configuring the GigaVUE Cloud Suite Cloud in OpenStack

First, you must establish a connection between GigaVUE-FM and your OpenStack environment. Then, GigaVUE-FM lets you launch the G-vTAP Controllers or V Series Controllers and V Series nodes in the specified project.

Pre-Configuration Checklist

Table 5: Pre-configuration Checklist 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:

Table 5: Pre-configuration Checklist

	Required Information
□	Authentication URL
□	Project Name
□	Peering **NOTE:** Peering must be active between the projects within the same monitoring domain. This is required only when shared controller option is chosen for configuring the components.
□	Floating IP
□	Region name for the Project
□	Domain
□	SSH Key Pair
□	Networks
□	Security groups

Logging in to GigaVUE-FM

To login to GigaVUE-FM, do the following:

1. Enter the Floating IP address of GigaVUE-FM into a browser. The GigaVUE-FM login page is displayed. Refer to GigaVUE-FM Login Page.

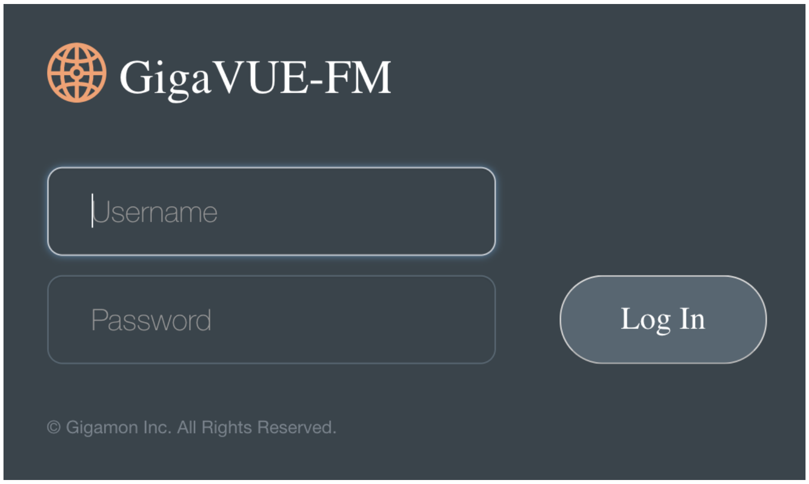
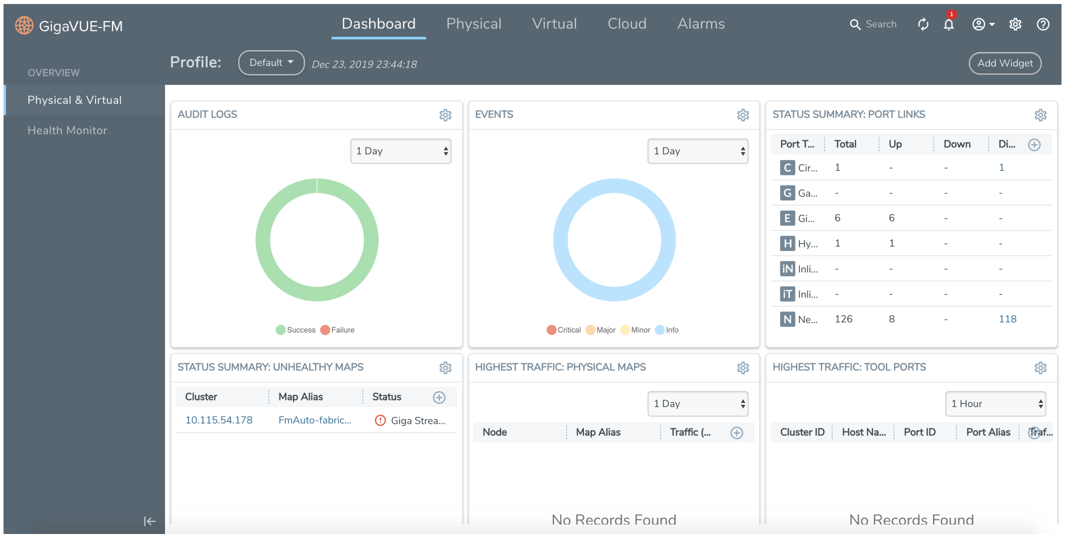


Figure 1 *GigaVUE-FM Login Page*

> **NOTE:** GigaVUE-FM must be able to resolve the hostname of the cloud controller for OpenStack, either through DNS or by manually adding it through the GigaVUE-FM CLI, using the ip host <hostname> < ip address> command.

2. Enter admin as the user name and admin123A! as the password. If the password is changed during the jump-start configuration as described in Initial GigaVUE-FM Configuration, enter the changed password.
3. Click **Login**. The GigaVUE-FM Dashboard page is displayed. Refer to GigaVUE-FM.



Port T...	Total	Up	Down	Di...
C Cir...	1	-	-	1
G Ga...	-	-	-	-
E Gi...	6	6	-	-
H Hy...	1	1	-	-
iN Inli...	-	-	-	-
IT Inli...	-	-	-	-
N Ne...	126	8	-	118

Cluster	Map Alias	Status
10.115.54.178	FmAuto-fabric...	Giga Strea...

Node	Map Alias	Traffic (...

Cluster ID	Host Na...	Port ID	Port Alias	Traf...

Figure 2 *GigaVUE-FM*

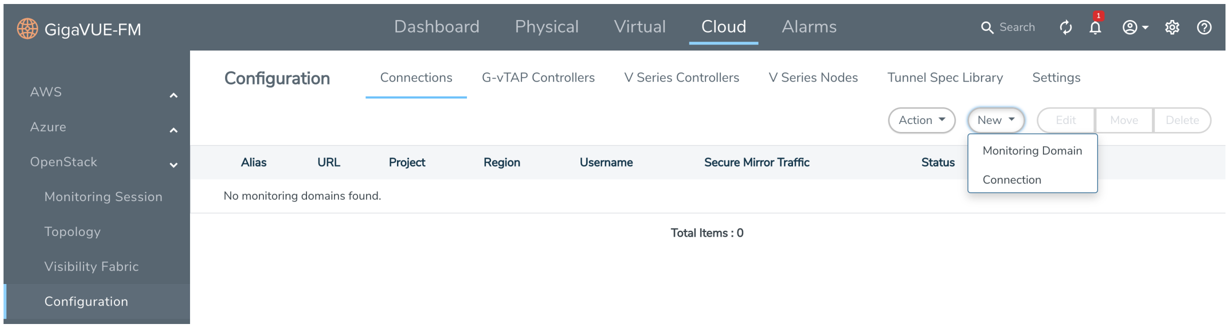
Connecting to OpenStack

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.

> **NOTE:** 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.

To create a new connection:

1. Click **Cloud** from the GigaVUE-FM top navigation.
2. Go to **OpenStack > Configuration > Connections**to view the OpenStack connections.

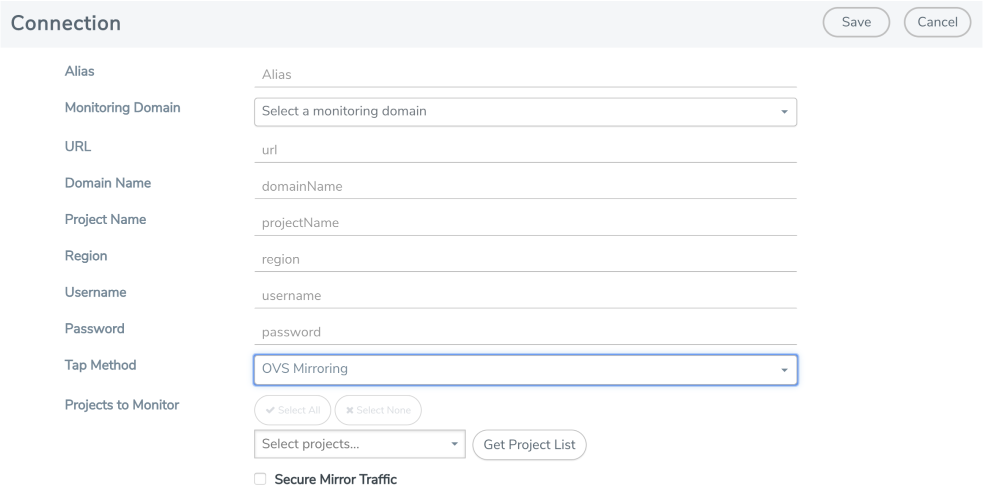


Alias	URL	Project	Region	Username	Secure Mirror Traffic	Status

No monitoring domains found.

Total Items : 0

3. Click the **New** drop-down menu. You can either create a new monitoring domain or a new connection.
   - If you select **Monitoring Domain**, then the **Create Monitoring Domain** dialog box is displayed. Enter the alias that is used to identify the monitoring domain.
   - If you select **Connection**, then the OpenStack Connection page is displayed.
4. Enter or select the appropriate information to set up the connection. Refer to Table 6: OpenStack Connectionfor field-level details.

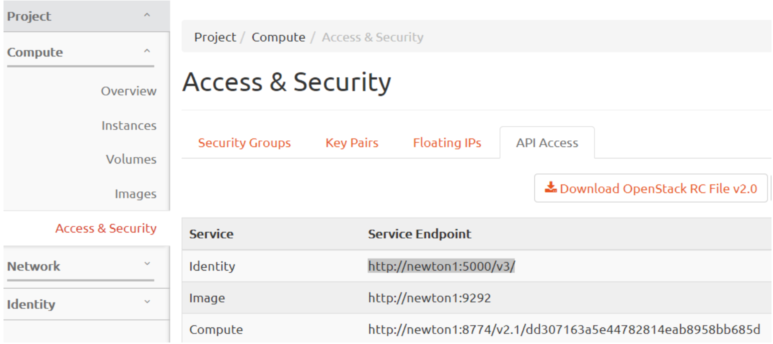


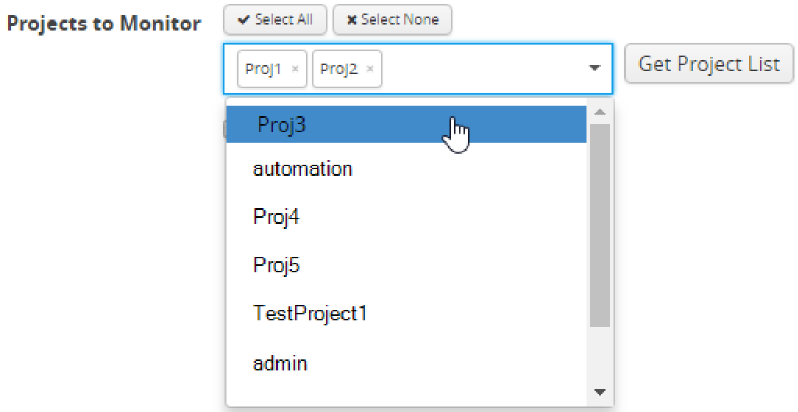
Connection

Alias	Alias
Monitoring Domain	Select a monitoring domain
URL	url
Domain Name	domainName
Project Name	projectName
Region	region
Username	username
Password	password
Tap Method	OVS Mirroring
Projects to Monitor	✔ Select All ✖ Select None Select projects... Get Project List □ Secure Mirror Traffic

Table 6: OpenStack Connection

Field	Description
Alias	An alias used to identify the connection to OpenStack.
Monitoring Domain	An alias used to identify the monitoring domain. You can either create a new monitoring domain or select an existing monitoring domain that is already created. **NOTE:** Monitoring domain consists of set of connections.
URL	The authentication URL is the Keystone URL of the OpenStack cloud. This IP address must be DNS resolvable. To get the authentication URL from the OpenStack dashboard: **a.** Login to OpenStack Horizon. **b.** Go to **Compute** > **Access & Security**. **c.** Click the **API Access** tab and copy the Identity URL.

Field	Description
	 Project Compute Overview Instances Volumes Images Access & Security Network Identity Project / Compute / Access & Security Access & Security Security Groups Key Pairs Floating IPs API Access Download OpenStack RC File v2.0 **Service** — **Service Endpoint** Identity — http://newton1:5000/v3/ Image — http://newton1:9292 Compute — http://newton1:8774/v2.1/dd307163a5e44782814eab8958bb685d Paste the Identity URL into the URL field.
Domain Name	The DNS domain name of the project.
Project Name	For GvTAP, this is the name of the project to monitor. For GvTAP-OVS (OVS Mirroring), this is the project name that will be used for authentication. This is a required field.
Region	The region where the Project resides. You can find your region by running one of these commands, depending on your OpenStack version. **keystone endpoint-list** or **openstack endpoint list**
Username	The user name used to connect to the OpenStack cloud. **NOTE:** The user must belong to a role that meets the OpenStack minimum requirements for OVS Mirroring. Refer to OVS Mirroring Prerequisites.
Password	The password for the OpenStack cloud.

Field	Description
Tap Method	Select the type of agent used to capture traffic for monitoring: • TaaS • G-vTAP • OVS Mirroring • OVS Mirroring + DPDK • None **NOTE:** 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	This field only appears, and is required, for OVS Mirroring or OVS Mirroring + DPDK. • Click the **Get Project List** button to view the list of projects. **NOTE:** The **Get Project List** button will only work if all the OpenStack credentials have been provided. Refer to OVS Mirroring Prerequisites. • Select the name of the project or projects you want to monitor from the list. (There is a limit of 128 projects.) • You can click **Select None** to clear existing selections or **Select All** to add all available projects to the connection configuration.  Projects to Monitor ✔ Select All ✖ Select None Proj1 × Proj2 × Get Project List Proj3 automation Proj4 Proj5 TestProject1 admin **NOTE:** OVS Mirroring or OVS Mirroring + DPDK supports multiple projects, without limit. As stated in the prerequisites for OVS Mirroring, you need permission to list all the projects in your OpenStack cloud environment.
Secure Mirror Traffic	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) **NOTE:** Must be deselected for OVS Mirroring or OVS Mirroring + DPDK.

1. Click **Save**.

Viewing Connections

If GigaVUE-FM connects to OpenStack successfully, the status is displayed as "Connected" in the **Status** column on the Connections page. GigaVUE-FM discovers the inventory of the cloud in the background. The Connections page has the following controls:

Control	Description
Action	Allows to refresh inventory.
New	Opens the page for specifying the connection details for a new connection.
Edit	Allows to make changes to a connection.
Delete	Deletes the connection. **NOTE:** Deleting a connection destroys all GigaVUE V Series Nodes, G-vTAP Controllers, and the virtual maps on the project.

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 **Cloud** > **Audit Logs**.

Configuring the G-vTAP Controllers

Only if G-vTAP agents are used for capturing traffic, then the G-vTAP Controllers must be configured in the OpenStack cloud. If TaaS is used for capturing the traffic, then skip to Configuring the GigaVUE Cloud Suite V Series Controllers.

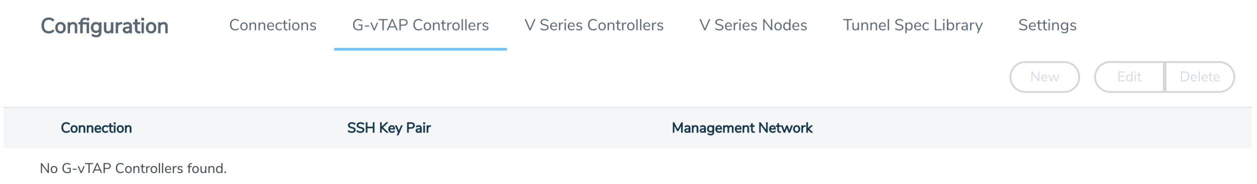
A G-vTAP Controller manages multiple G-vTAP agents and orchestrates the flow of mirrored traffic to GigaVUE Cloud Suite V Series nodes.

A G-vTAP Controller can only manage G-vTAP agents that have the same version. For example, the G-vTAP Controller v1.3 can only manage G-vTAP agents v1.3. So, if you have G-vTAP agents v1.2 still deployed in the instances, you must configure both G-vTAP Controller v1.2 and v1.3.

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 Cloud Suite V Series nodes. The tunnel type can be L2GRE or VXLAN.

To configure the G-vTAP Controllers:

1. Click **Cloud** from the GigaVUE-FM top navigation.
2. Go to **OpenStack** > **Configuration** > **G-vTAP Controllers**. The G-vTAP Configuration page is displayed.



Connection	SSH Key Pair	Management Network

No G-vTAP Controllers found.

a. Click **New** to create a new G-vTAP Controller configuration.

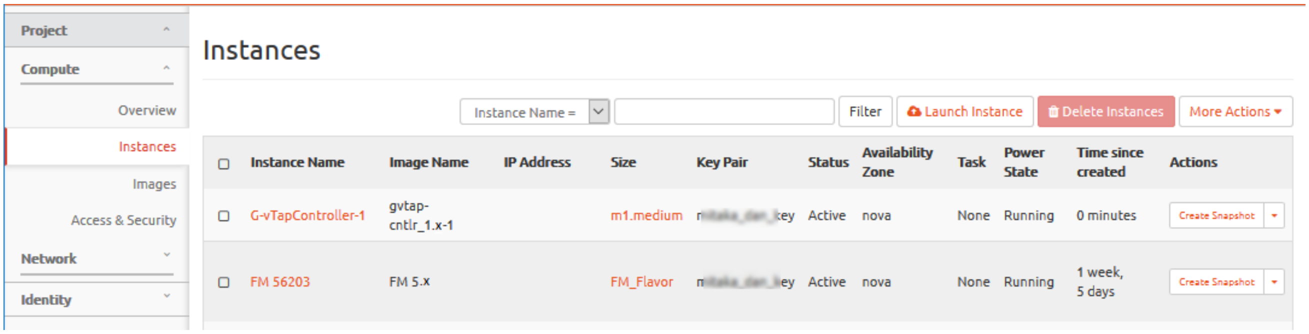
b. Click the check box of a configuration and click **Edit** to edit an existing configuration.

3. Complete the fields in the G-vTAP Configuration page to create or edit the controller's configuration settings. Refer to *The OpenStack G-vTAP Configuration Page* for details.
4. Click **Save** to save the configuration.
5. To verify your instance is running, refer to Verify the G-vTAP Controller Instance.

Verify the G-vTAP Controller Instance

After creating or editing the G-vTAP Controller, verify the instance is running:

1. Log in to OpenStack Horizon and view the compute instances for the project to verify the launch of the G-vTAP Controller.



□	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
□	G-vTapController-1	gvtap-cntlr_1.x-1		m1.medium	n[redacted]key	Active	nova	None	Running	0 minutes	Create Snapshot
□	FM 56203	FM 5.x		FM_Flavor	n[redacted]key	Active	nova	None	Running	1 week, 5 days	Create Snapshot

> **NOTE:** The above screen is an example only. It is not a GigaVUE-FM screen and is subject to change without notice. Refer to OpenStack documentation for how to use the OpenStack interface.

2. In GigaVUE-FM, select **OpenStack > Visibility Fabric > G-vTAP Controllers** to verify the launch of the G-vTAP Controller.

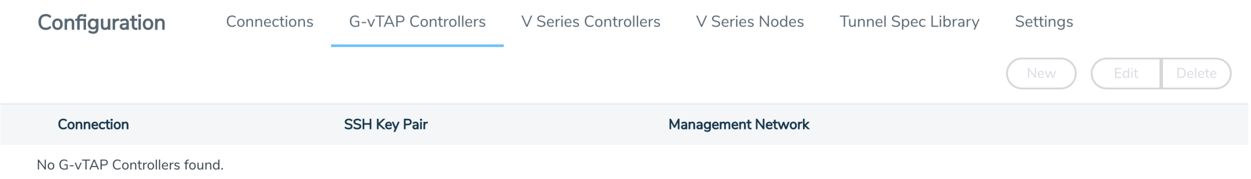
   The G-vTAP Controller is displayed with the status as**OK**.

> **NOTE:** The launch of the G-vTAP Controller is also displayed in **Cloud > Audit Logs**.

Delete a G-vTAP Controller

To delete a G-vTAP Controllers:

1. Click **Cloud** from the GigaVUE-FM top navigation.
2. Go to **OpenStack** > **Configuration** > **G-vTAP Controllers**. The G-vTAP Configuration page is displayed.



Connection	SSH Key Pair	Management Network

No G-vTAP Controllers found.

3. Click the check box to select an existing controller from the list.
4. Click **Delete**.

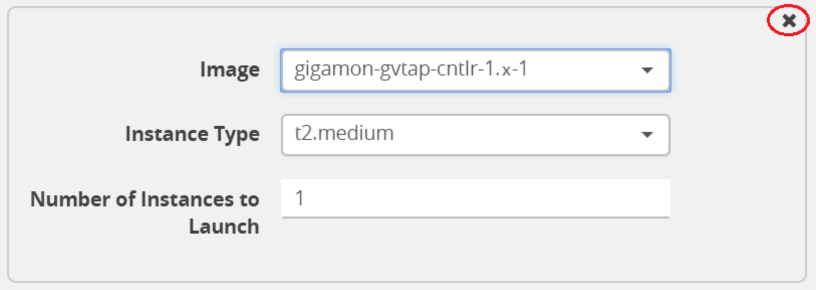
The OpenStack G-vTAP Configuration Page

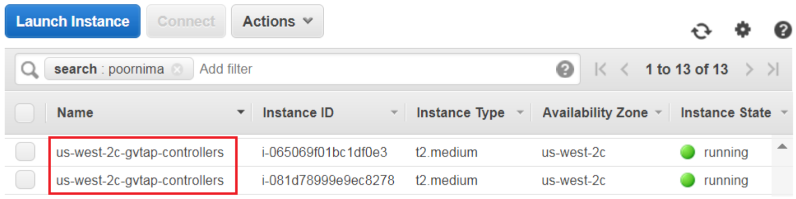
Use the G-vTAP Configuration page to the configuration settings of a G-vTAP Controller.

The following table provides a description of the fields in the G-vTAP Configuration page. The specific fields and options may vary based on your selection.

Table 7: Fields for G-vTAP Configuration

Fields	Description
Connection	The name of the connection. **NOTE:** For shared controller configuration, you must select the required connection for configuring the G-vTAP Controller. Peering must be active in the selected connection to allow the rest of the connections containing the V-series nodes to be monitored.
SSH KeyPair	The SSH key pair for the G-vTAP Controller. For more information about SSH key pair, refer to Key Pairs.
Project	Only available for OVS Mirroring or OVS Mirroring + DPDK. Select the OpenStack project where you want to deploy the fabric. **NOTE:** When setting up the V Series Controller, this field is populated with the project selected in the G-vTAP Controller setup. **NOTE:** If using with OVS Mirroring or OVS Mirroring + DPDK, a minimum of one project is required for OVS authentication.
Security	The security group created for the G-vTAP Controller. For example, sg_gvtap-controller. For more

Fields	Description
Groups	information, refer to Security Group .
Controller Version(s)	The G-vTAP Controller version that you configure must always have the same version number as the G-vTAP agents deployed in the instances. This is because the G-vTAP Controller v1.2-1 can only manage G-vTAP agents v1.2-1. Similarly, the G-vTAP Controller v1.3-1 can only manage G-vTAP agents v1.3-1. If there are multiple versions of G-vTAP agents deployed in the instances, then you must configure multiple versions of G-vTAP Controllers that matches the version numbers of the G-vTAP agents. **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. To add multiple versions of G-vTAP Controllers: **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** down-down list, select a flavor for the G-vTAP Controller. **d.** In **Number of Instances to Launch**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1. To delete a G-vTAP Controller version: An older version of G-vTAP Controller can be deleted once all the G-vTAP agents are upgraded to the latest version. **a.** Click **x** (delete) next to the G-vTAP Controller image to delete that version.  Image: gigamon-gvtap-cntlr-1.x-1 Instance Type: t2.medium Number of Instances to Launch: 1 **b.** When you delete a G-vTAP Controller image from the G-vTAP Configuration page, all the G-vTAP Controller instances of that version are also deleted.
Management Network	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. **Network** - Select the management network ID. **IP Address Type** The type of IP address GigaVUE-FM needs to communicate with G-vTAP controllers: • **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. • **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. Make sure that this floating IP will not be used by other instances in the cloud. **NOTE:** If GigaVUE-FM resides inside the same project, no floating IPs are necessary for the controllers.

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td></td><td><b>NOTE:</b> For V Series Nodes data network deployments, select <b>Floating</b> and then specify the IPs in the <b>Floating IPs</b> field.</td></tr>
<tr><td>Additional Network(s)</td><td>(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.
Click <b>Add</b> to specify additional networks (subnets), if needed. Also, make sure that you specify a list of security groups for each additional network.</td></tr>
<tr><td>Tag(s)</td><td>(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 GvTAP Controller Version for OVS Mirroring and OVS Mirroring + DPDK.
To add a tag:
<b>a.</b> Click <b>Add</b>.
<b>b.</b> In the <b>Key</b> field, enter the key. For example, enter Name.
<b>c.</b> In the <b>Value</b> field, enter the key value. For example, us-west-2-gvtap-controllers.
When the G-vTAP Controllers are launched in the VPC, they will appear with the custom tag:


<table>
<tr><th>Name</th><th>Instance ID</th><th>Instance Type</th><th>Availability Zone</th><th>Instance State</th></tr>
<tr><td>us-west-2c-gvtap-controllers</td><td>i-065069f01bc1df0e3</td><td>t2.medium</td><td>us-west-2c</td><td>● running</td></tr>
<tr><td>us-west-2c-gvtap-controllers</td><td>i-081d78999e9ec8278</td><td>t2.medium</td><td>us-west-2c</td><td>● running</td></tr>
</table>
</td></tr>
<tr><td>Agent Tunnel Type</td><td>The type of tunnel used for sending the traffic from G-vTAP agents to GigaVUE Cloud Suite V Series nodes. The options are GRE or VXLAN tunnels.</td></tr>
<tr><td>G-vTAP Agent MTU (Maximum Transmission Unit)</td><td>The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP agent to the GigaVUE Cloud Suite V Series node.
• For GRE, the default value is 1450.
• For VXLAN, the default value is 1400. However, the G-vTAP agent tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.</td></tr>
</table>

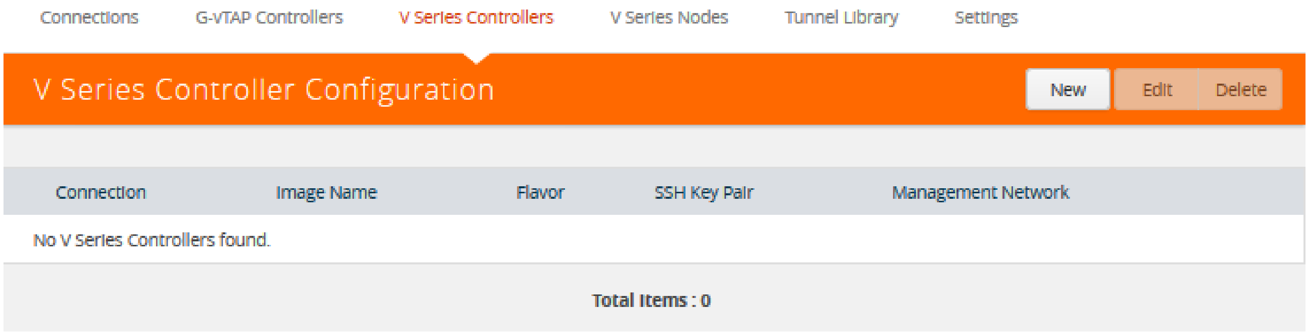
Configuring the GigaVUE Cloud Suite V Series Controllers

The GigaVUE Cloud Suite V Series Controller Configuration page defines the parameters for a GigaVUE Cloud Suite V Series Controller. Creating a GigaVUE Cloud Suite V Series Controller profile automatically launches the controllers.

To configure a GigaVUE Cloud Suite V Series Controller:

1. Click **Cloud** from the GigaVUE-FM top navigation.

2. Go to **OpenStack** > **Configuration** > **V Series Controllers**. The V Series Controller Configuration page is displayed.



Connection	Image Name	Flavor	SSH Key Pair	Management Network
No V Series Controllers found.				

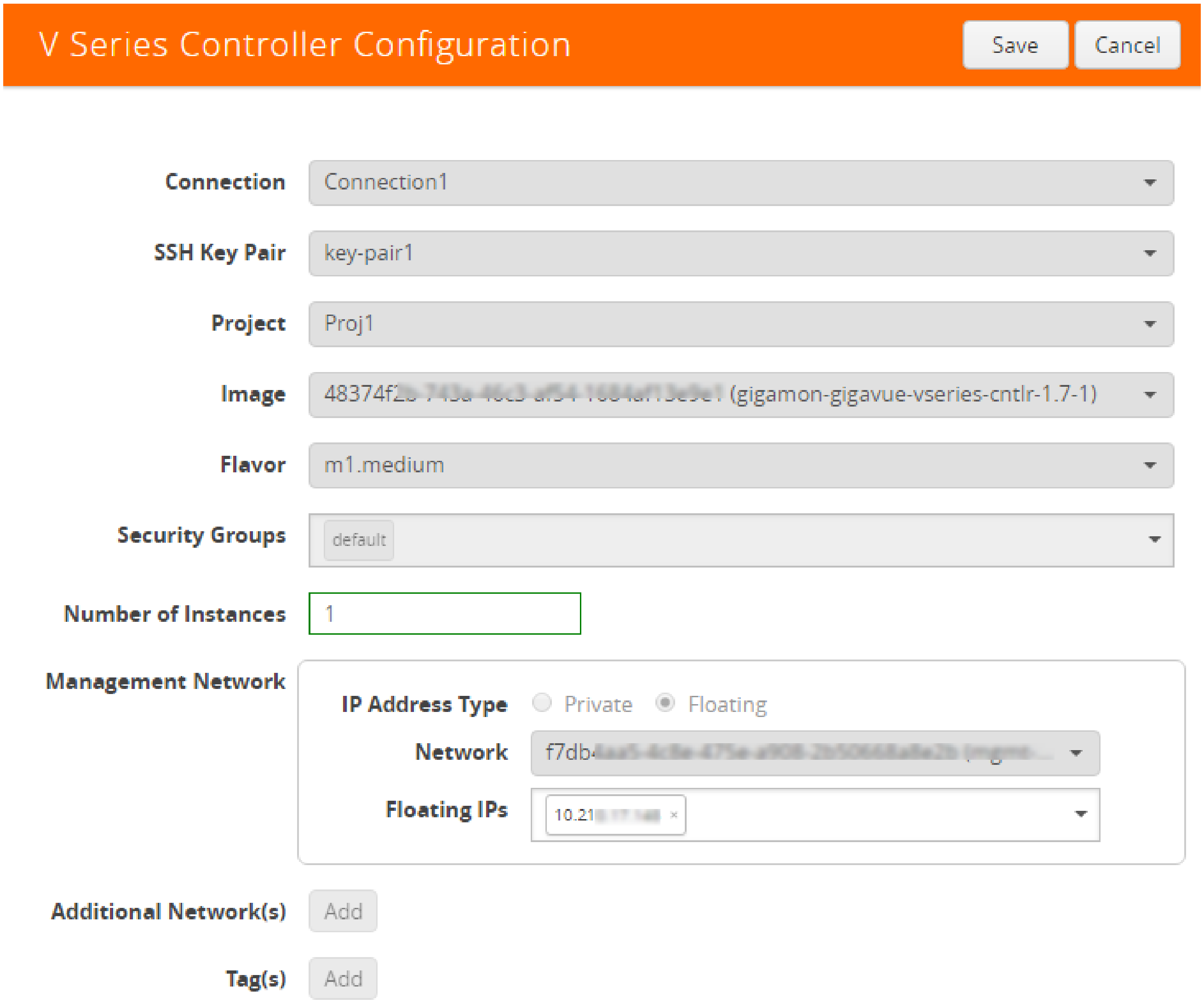
Total Items : 0

Options:

a. Click **New** to create a new V Series Controller configuration.

b. Click the check box of a configuration and click **Edit** to edit an existing configuration.

3. Complete the fields in the GigaVUE V Series Controller Configuration page to create or edit the controller's configuration settings. The fields in this page are the same as those on the G-vTAP Configuration page. Refer to The OpenStack G-vTAP Configuration Page for the common fields.



V Series Controller Configuration

Connection: Connection1

SSH Key Pair: key-pair1

Project: Proj1

Image: 48374f2[redacted] (gigamon-gigavue-vseries-cntlr-1.7-1)

Flavor: m1.medium

Security Groups: default

Number of Instances: 1

Management Network

IP Address Type: ○ Private ● Floating

Network: f7db[redacted]

Floating IPs: 10.21[redacted] ×

Additional Network(s): Add

Tag(s): Add

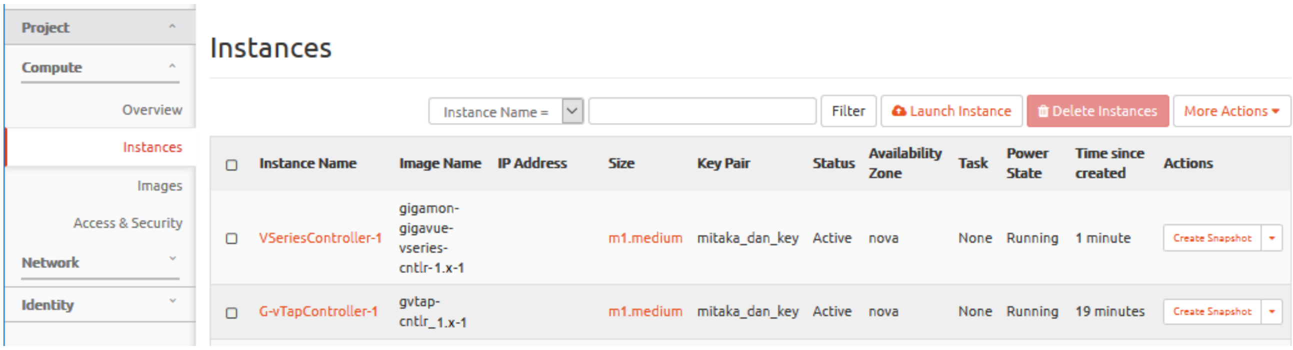
> **NOTE:** For shared controller configuration, you must select the required connection for configuring the V Series Controller. Peering must be active in the selected connection to allow the rest of the connections to be monitored.

4. Click **Save** to save the configuration.
5. To verify your instance is running, refer to Verify the V Series Controller Instance.

Verify the V Series Controller Instance

After creating or editing the V Series Controller, verify the instance is running:

1. Log in to OpenStack Horizon and view the compute instances for the project to verify the launch of the V Series Controller.

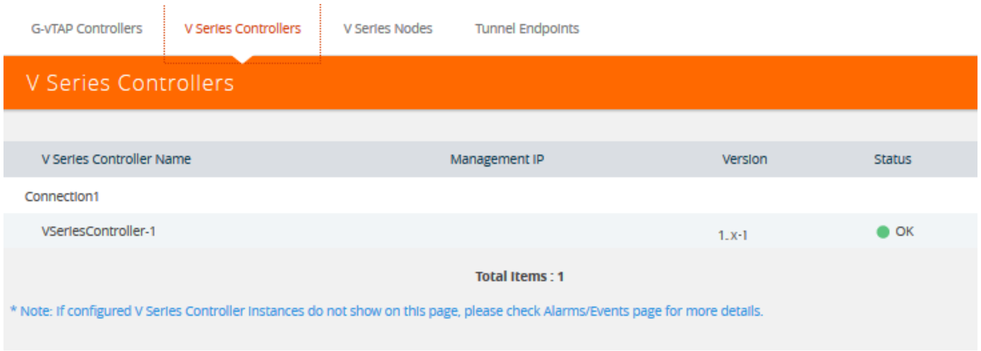


□	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
□	VSeriesController-1	gigamon-gigavue-vseries-cntlr-1.x-1		m1.medium	mitaka_dan_key	Active	nova	None	Running	1 minute	Create Snapshot
□	G-vTapController-1	gvtap-cntlr_1.x-1		m1.medium	mitaka_dan_key	Active	nova	None	Running	19 minutes	Create Snapshot

> **NOTE:** The above screen is an example only. It is not a GigaVUE-FM screen and is subject to change without notice. Refer to OpenStack documentation for how to use the OpenStack interface.

2. In GigaVUE-FM, select **OpenStack > Visibility Fabric > V Series Controllers** to verify the launch of the V Series Controller.

   The V Series Controller should appear with the status as OK.



V Series Controller Name	Management IP	Version	Status
Connection1			
VSeriesController-1		1.x-1	● OK

Total Items : 1

* Note: If configured V Series Controller Instances do not show on this page, please check Alarms/Events page for more details.

> **NOTE:** The launch of the G-vTAP Controller is also displayed in **Cloud > Audit Logs**.

Configuring the GigaVUE V Series Node

GigaVUE® V Series node is a visibility node that aggregates mirrored traffic from multiple G-vTAP agents. 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 the standard IP GRE tunnels.

GigaVUE Cloud Suite V Series nodes can be successfully launched only after GigaVUE Cloud Suite V Series Controller is fully initialized and the status is displayed as OK.

The V Series Node Configuration page defines the parameters for a GigaVUE Cloud Suite V Series node. Creating a GigaVUE Cloud Suite V Series node profile automatically launches the V Series node.

To configure a GigaVUE V Series node profile:

1. Click **Cloud** from the GigaVUE-FM top navigation.
2. Go to **OpenStack** > **Configuration** > **V Series Nodes**.
   a. Click **New** to create a new V Series node configuration.
   b. Click the check box of a configuration and click **Edit** to edit an existing configuration.
3. Complete the fields in the GigaVUE V Series Node Configuration page to create or edit the node's configuration settings. The fields in this page are the same as those on the G-vTAP Configuration page.

   Refer to The OpenStack G-vTAP Configuration Page for the common fields. For additional configuration settings, refer to Table 8: Fields for GigaVUE Cloud Suite V Series Node Launch Configuration.
4. Click **Save** to save the configuration.

Table 8: Fields for GigaVUE Cloud Suite V Series Node Launch Configuration

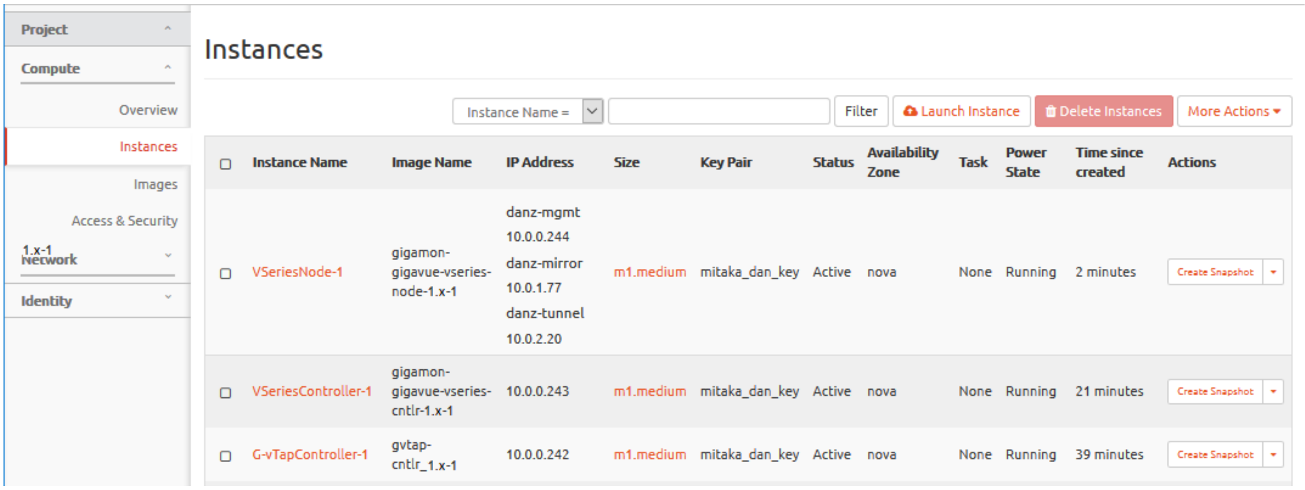
Parameter	Description
Management Network	For the V Series Node, the Management Network is what is used by the V Series Controller to communicate with the V Series Nodes. Select the management network ID.
Data Network	**Network 1** Click **Add** to add additional networks . This is the network that the GigaVUE Cloud Suite V Series node uses to communicate with the monitoring tools. Multiple networks are supported.

Parameter	Description
	IP Address Type The type of IP address GigaVUE-FM needs to communicate with G-vTAP or G-vTAP-OVS controllers: • **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. • **Floating**—A floating IP address specified here will be where the monitored traffic is tunneled to. The monitored traffic must be able to reach the V Series Node. **NOTE:** 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. **NOTE:** A provider network 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.
Min Instances to Launch	The minimum number of GigaVUE Cloud Suite V Series nodes to be launched in OpenStack. The minimum number can be 0. • 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 monitoring session, the V Series nodes will automatically be deployed based on the # of VMs being monitored. **NOTE:** GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances to Launch	The maximum number of GigaVUE Cloud Suite V Series nodes that can be launched in OpenStack.
Tunnel MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is applied on the outgoing tunnel endpoints of the GigaVUE Cloud Suite V Series node when a monitoring session is deployed. The default value is 1450.
Shared	Only one V Series node configuration can be shared in a monitoring domain. **NOTE:** Not used for OpenStack configurations.

Verify the V Series Node Instance

After creating or editing the V Series Node Controller, verify the instance is running:

1. Log in to OpenStack Horizon and view the compute instances for the project to verify the launch of the V Series Node .



□	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
□	VSeriesNode-1	gigamon-gigavue-vseries-node-1.x-1	danz-mgmt 10.0.0.244 danz-mirror 10.0.1.77 danz-tunnel 10.0.2.20	m1.medium	mitaka_dan_key	Active	nova	None	Running	2 minutes	Create Snapshot
□	VSeriesController-1	gigamon-gigavue-vseries-cntlr-1.x-1	10.0.0.243	m1.medium	mitaka_dan_key	Active	nova	None	Running	21 minutes	Create Snapshot
□	G-vTapController-1	gvtap-cntlr_1.x-1	10.0.0.242	m1.medium	mitaka_dan_key	Active	nova	None	Running	39 minutes	Create Snapshot

> **NOTE:** The above screen is an example only. It is not a GigaVUE-FM screen and is subject to change without notice. Refer to OpenStack documentation for how to use the OpenStack interface.

2. In GigaVUE-FM, select **OpenStack > Visibility Fabric > V Series Node** to verify the launch of the GigaVUE Cloud Suite V Series node. The V Series Node Controller is displayed with the status as OK.

> **NOTE:** The launch of the V Series Controller is also displayed in **Cloud > Audit Logs**.

Configuring Monitoring Sessions

This chapter describes how to setup tunnel endpoints in a monitoring session to receive and send traffic to the GigaVUE Cloud Suite 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:

- Overview of Visibility Components
- Creating Tunnel Endpoints
- Create a Monitoring Session
- Configuring the OpenStack Settings

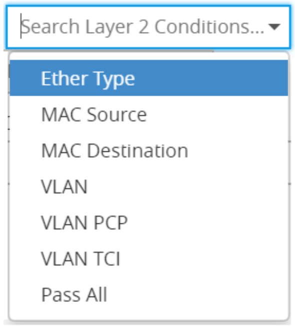
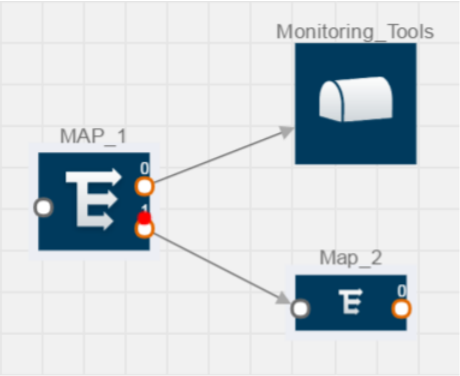
Overview of Visibility Components

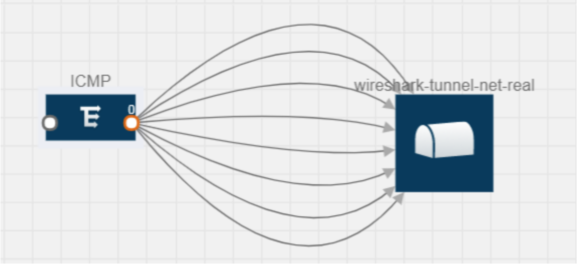
The GigaVUE Cloud Suite V Series node aggregates the traffic from multiple G-vTAP agents or TaaS and filters them using maps. It applies intelligence and optimization to the aggregated traffic using GigaSMART applications such as Flow Mapping®™, sampling, slicing, and masking, and distributes them to the tunnel endpoints.

Table 1: Components of Traffic Visibility Sessions lists the components of the monitoring session:

Table 1: Components of Traffic Visibility Sessions

Parameter	Description
Map	A map (M) is used to filter the traffic flowing through the V Series node. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.
Rule	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic. The rules must contain the appropriate Layer 2 (L2) to Layer 4 (L4) filters defined in them. For example, if you want to filter the traffic for HTTP Port 80, you must select the following criteria: • Layer 2—Ethertype IPv4 • Layer 3—Protocol TCP • Layer 4—Port Destination 80 By default, a rule always displays conditions based on the attributes of L2.

Parameter	Description
	 Search Layer 2 Conditions... Ether Type MAC Source MAC Destination VLAN VLAN PCP VLAN TCI Pass All **Figure 1** *Default Rule Conditions* A rule is also associated with priority and action set.
Priority	A priority determines the order in which the rules are executed. The greater the value, the higher the priority. The priority value can range from 0 to 99.
Action Set	An Action Set is an exit point in a map that you can drag and create links to the other maps, applications, and monitoring tools. A single map can have multiple action sets. A single action set can have multiple links connecting to maps and applications. You can create an Action Set when you create a rule for a map. In the following example (refer to Figure 2Action Set), Map 1 has two action sets: Action Set 0 and Action Set 1. The packets that match the rules in Action Set 0 are forwarded to monitoring tools. The packets that match the rules in Action Set 1 are forwarded to Map 2.  **Figure 2** *Action Set* A single action set can have up to 8 links connecting the same destination point. The same packets from the map are replicated in 8 different links.

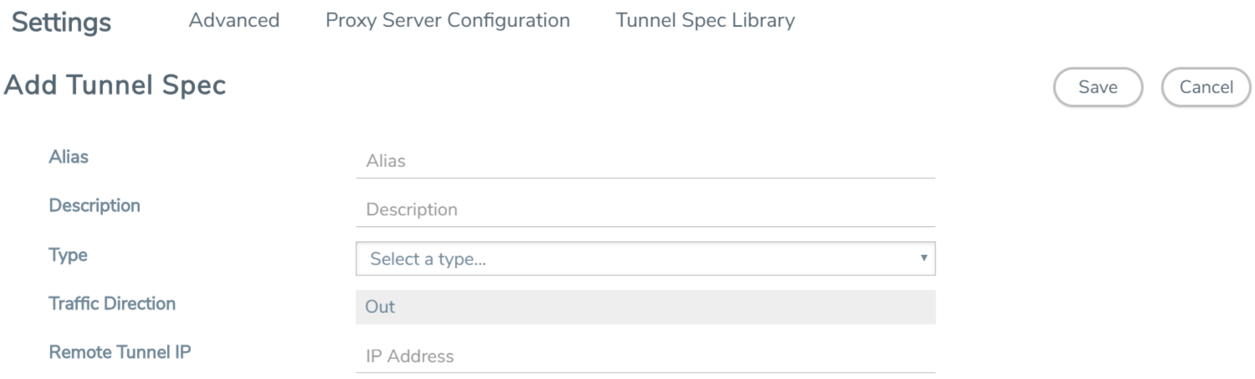
Parameter	Description
	 **Figure 3** *Action Set with Multiple Links*
Link	A link directs the packets to flow from a map to the destination. The destination could be the other maps, applications, and the monitoring tools. In Figure 2Action Set, the link originating from action set 0 is moving the traffic from MAP_1 to Monitoring_Tools. A link lets you add header transformation to the packets passing through it before they are sent to the destination. This transformation is supported only with GigaVUE Cloud Suite V Series node v1.2-1 and above. For more information about Header Transformation, refer to Adding Header Transformations.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.
Application	An application performs operations such as sampling, slicing, and masking on the traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Target	A target determines the instances that are to be monitored. Targets are determined based on the following formula: Target = (Maps ∩ Inclusion map) – Exclusion map
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the maps, inclusion maps, and exclusion maps in the monitoring session. For OVS Mirroring and OVS Mirroring + DPDK, the hypervisors will be selected as targets although this will not be displayed in the topology graph. It will be shown in the monitoring session deployment report. The instance targets will be selected based on two additional criteria: • they must be in one of the projects selected in the monitored projects list from the connection page, and • they must reside on a hypervisor that has the GvTAP Agent installed on it.
Tunnel	A tunnel lists the monitoring tools to which the traffic matching the filtered criteria is routed.

Creating 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 Virtual Extensible LAN (VXLAN) tunnel.

To create a tunnel endpoint:

1. In GigaVUE-FM, on the top navigation pane, select **Cloud**.
2. On the left navigation pane, select **OpenStack > Configuration.**
3. Select the **Tunnel Spec Library** tab. The Tunnel Library page appears.
4. Click **New**. The Edit Tunnel page appears.



Alias	Alias
Description	Description
Type	Select a type...
Traffic Direction	Out
Remote Tunnel IP	IP Address

5. On the **Edit Tunnel** page, select or enter the appropriate information in the fields as described in the following table.

Table 2: Field Descriptions for Tunnel Endpoint

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 L2GRE or VXLAN to create a tunnel. If you choose VXLAN, you must enter the remote IP interface.
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 in the current release.
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.

6. Click **Save**.
7. Select **OpenStack > Visibility Fabric > Tunnel Endpoints** and verify the tunnel endpoint added to GigaVUE-FM.

Create a Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances available in your OpenStack 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 OpenStack environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

> **NOTE:** In vTAP connections, Tool VM instances (Source and Destination IP) must be excluded using Exclusion Map.

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

- Creating a New Session
- Cloning a Monitoring Session
- Splitting a Monitoring Session
- Creating a Map
- Adding Applications to the Monitoring Session
- Deploying the Monitoring Session
- Viewing the Statistics
- Viewing the Topology

Creating a New Session

You can create multiple monitoring sessions within a single project connection.

To create a new session:

1. In GigaVUE-FM, on the top navigation pane, select **Cloud**.
2. Select **OpenStack > Monitoring Session**. The Monitoring Sessions page appears.
3. Click **New** to open the Create a New Monitoring Session page.
4. Enter the appropriate information for the monitoring session. Refer to Table 3: Fields for Monitoring Session Info for more information about the fields.
5. Click **Create**. The Monitoring Session details page appears displaying the specified session information and target VMs.

6. If multiple projects had been selected in the connections page, the topology view will show instances in all of the selected projects.

Table 3: Fields for Monitoring Session Info

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain.
Connection	The OpenStack 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.
Agent Pre-filtering	When enabled, traffic is filtered at the G-vTAP agent-level, before mirroring to the V Series Nodes, which reduces the load on the V Series Nodes and the Cloud networks. Refer to Agent Pre-filtering. **NOTE:** Agent Pre-filtering must be deselected for OVS Mirroring or OVS Mirroring + DPDK.

Cloning a Monitoring Session

You can clone an existing monitoring session.

To clone a monitoring session:

1. Select the monitoring session that you need to clone from the **Monitoring Sessions** page.
2. Click **Clone**.
3. Enter the appropriate information in the **Clone Monitoring Session** dialog box as shown in Table 3: Fields for Monitoring Session Info.

Table 4: Fields for Cloning the Monitoring Session.

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

4. Click **Create** to create the cloned monitoring session.

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

Creating a Map

Each map can have up to 32 rules associated with it. Table 6: Fields for Creating a New Maplists the various rule conditions that you can select for creating a map, inclusion map, and exclusion map.

Table 5: Conditions for the Rules

Conditions	Description
L2, L3, and L4 Filters	
Ether Type	The packets are filtered based on the selected ethertype. The following conditions are displayed: • IPv4 • IPv6 • ARP • RARP • Other **L3 Filters** If you choose IPv4 or IPv6, the following L3 filter conditions are displayed: • Protocol • IP Fragmentation • IP Time to live (TTL) • IP Type of Service (TOS) • IP Explicit Congestion Notification (ECN) • IP Source • IP Destination **L4 Filters** If you select TCP or UDP protocol, the following L4 filter conditions are displayed: • Port Source • Port Destination
MAC Source	The egress traffic 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.

Conditions	Description
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 Ether Type as IPv4, TCP as the protocol, and do not specify IPv4 source or destination, then both egress and ingress traffic is selected for monitoring purpose.

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

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

To create a new map:

1. Select **OpenStack > Monitoring Session**.
2. Click **New**. The Monitoring Sessions page is displayed.
3. Create a new session. Refer to Creating a New Session.
4. From **Maps**, drag and drop a new map template to the workspace.
5. Click on the map, then click details.

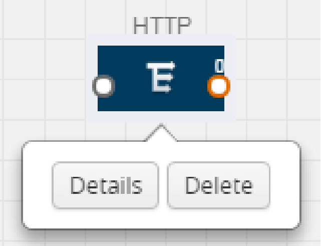
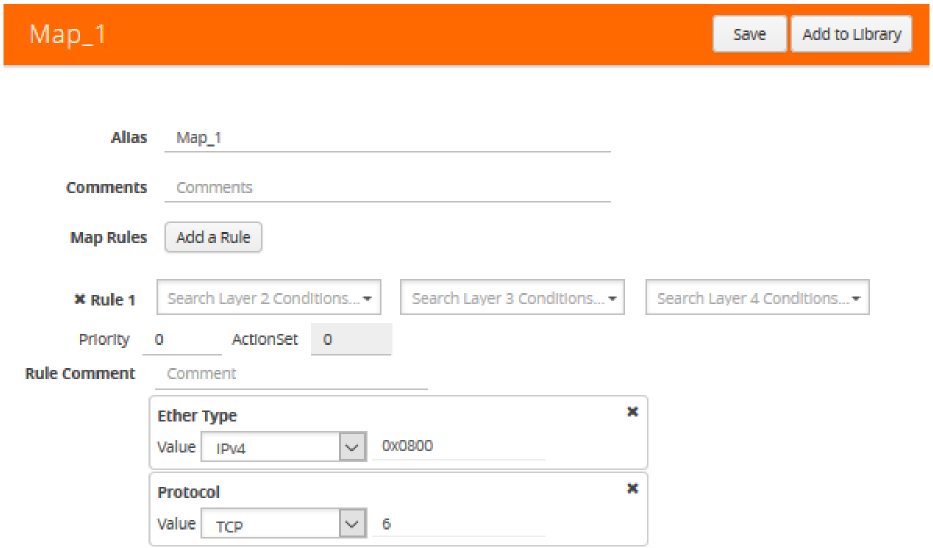


Figure 5 *Map Details*

The map rules quick view is displayed as shown in Figure 6Creating a New Map.


Map_1
Save
Add to Library
Add a Rule
✖ Rule 1
Search Layer 2 Conditions...
Search Layer 3 Conditions...
Search Layer 4 Conditions...
✖
✖

Alias: Map_1

Comments: Comments

Map Rules

Priority: 0 ActionSet: 0

Rule Comment: Comment

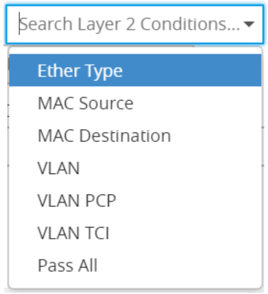
Ether Type
Value: IPv4 0x0800

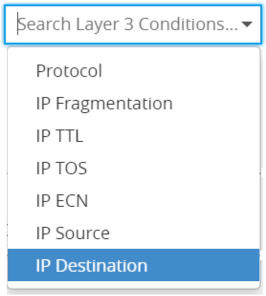
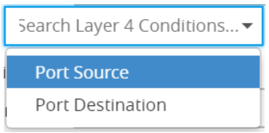
Protocol
Value: TCP 6

Figure 6 *Creating a New Map*

6. Enter the appropriate information for creating a new map as shown in Table 6: Fields for Creating a New Map.

Table 6: Fields for Creating a New Map

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.
Rule Conditions **Map Rules**	The rules for filtering the traffic in the map. To add a map rule: **a.** Click **Add a Rule**. **b.** Select a condition from the **Search L2 Conditions** drop-down list and specify a value. Based on this selection, the Search L3 Conditions drop-down list is automatically updated.  Search Layer 2 Conditions... Ether Type MAC Source MAC Destination VLAN VLAN PCP VLAN TCI Pass All **c.** Select a condition from the **Search L3 Conditions** drop-down list and specify a value.

Parameter	Description
	 Search Layer 3 Conditions... Protocol IP Fragmentation IP TTL IP TOS IP ECN IP Source IP Destination **d.** (Optional) If you have selected TCP or UDP as the protocol in the L3 conditions, then select Port Source or Port Destination from the Search L4 Conditions drop-down list and specify a value. If you have selected conditions other than TCP or UDP, then the Search L4 Conditions drop-down list is disabled.  Search Layer 4 Conditions... Port Source Port Destination **e.** (Optional) In the Priority and Action Set box, assign a priority and action set. **f.** (Optional) In the Rule Comment box, enter a comment for the rule. **NOTE:** Repeat steps **b** through **f** to add more conditions. **NOTE:** Repeat steps **a** through **f** to add nested rules.

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

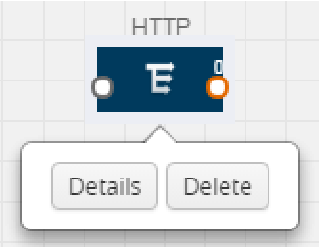
7. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
   - Select an existing group from the **Select Group** list and click **Save**.
   - Enter a name for the new group in the **New Group** field and click **Save.**

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

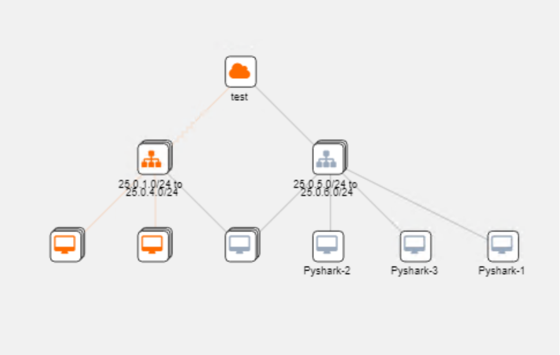
8. Click **Save**.

Options:

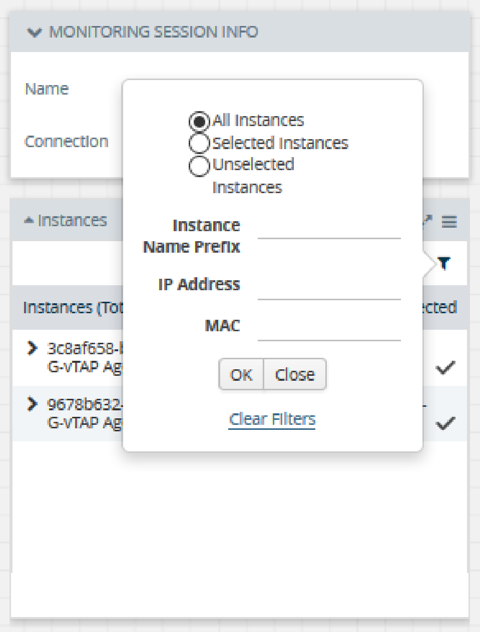
- To edit or delete a map, click a map and select **Details** to edit the map or **Delete** to delete the map.



- Click the **Show Targets** button to view the monitoring targets highlighted in blue.



- Click on ⤢ to expand the **Targets** dialog box. Click on ≡
- Click on the Filter icon to filter Instances based on the Instance Name Prefix, IP address, or MAC address.



MONITORING SESSION INFO

Name

Connection

Instances

Instances (Tot

3c8af658-
G-vTAP Ag

9678b632-
G-vTAP Ag

cted

● All Instances
○ Selected Instances
○ Unselected Instances

Instance Name Prefix

IP Address

MAC

OK | Close

Clear Filters

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 Capabilities and Benefits

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.

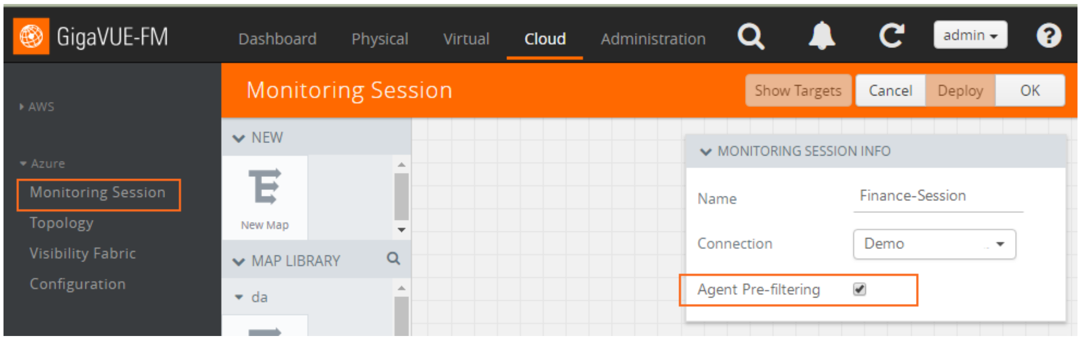
- Rules that span all monitoring sessions will be merged for an G-vTAP agent, if applicable
- If the max-rule limit of 16 is reached, then all the traffic is passed to the V Series node; no filtering will be performed.

Enable/Disable G-vTAP Agent Pre-filtering

Agent pre-filtering can be enabled or disabled by the user at the monitoring-session level. This ensures that we provide a knob to the user to turn it on or off at the G-vTAP level according to the requirements.

To change the G-vTAP Agent Pre-filtering option setting:

1. **Cloud** > **OpenStack**> **Monitoring Session**
2. Open a monitoring session by doing one of the following:
   a. Click **New** to create a new session.
   b. Click the check box next to a session and then click **Edit** to edit an existing session.



MONITORING SESSION INFO

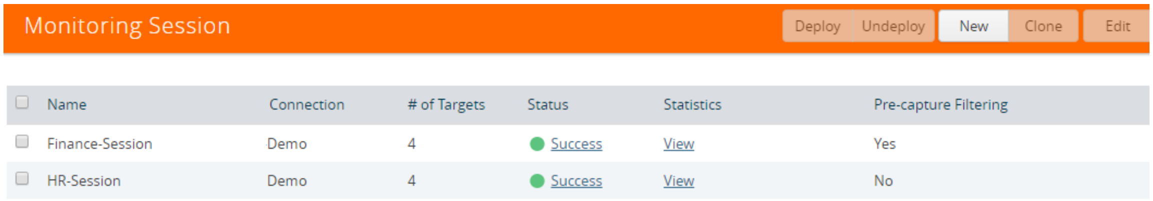
Name: Finance-Session

Connection: Demo

Agent Pre-filtering ☑

3. Select or deselect the **Agent Pre-filtering** check box in the MONITORING SESSION INFO box to change the setting. It is enabled by default.
   a. Deselect the check box to disable it.
   b. Select the check box to enable it.
4. Click **OK**.

   The Monitoring Session view displays the setting in the Agent Pre-filtering column



□	Name	Connection	# of Targets	Status	Statistics	Pre-capture Filtering
□	Finance-Session	Demo	4	● Success	View	Yes
□	HR-Session	Demo	4	● Success	View	No

Add Applications to Monitoring Session

Gigamon supports the following GigaSMART applications with GigaVUE Cloud Suite Cloud for AWS:

- Sampling
- Slicing
- Masking
- NetFlow

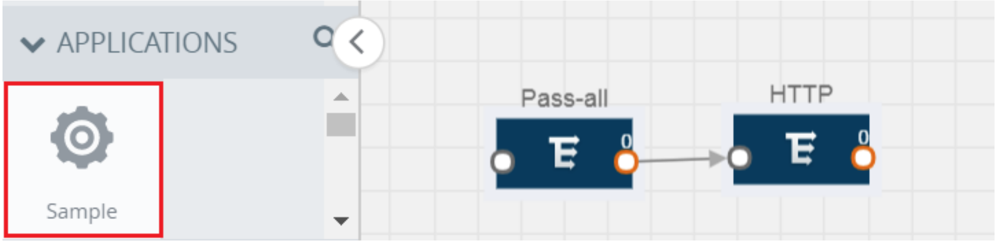
You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools.

Sampling

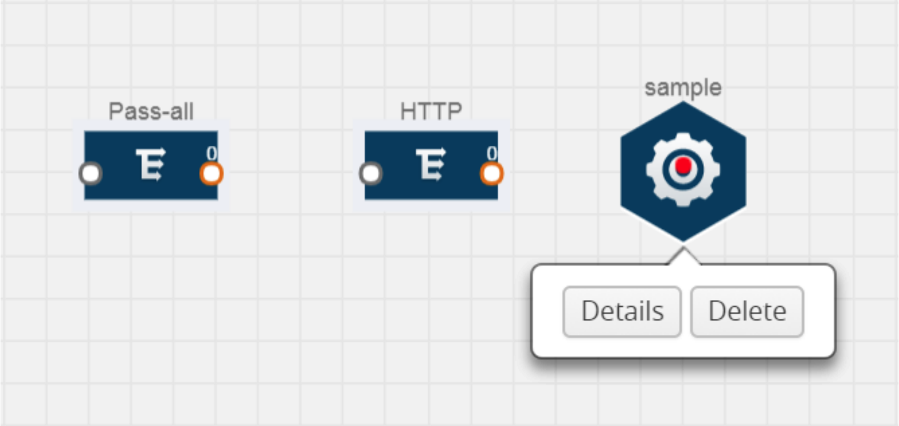
Sampling lets you sample the packets randomly based on the configured sampling rate and then forwards the sampled packets to the monitoring tools.

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.

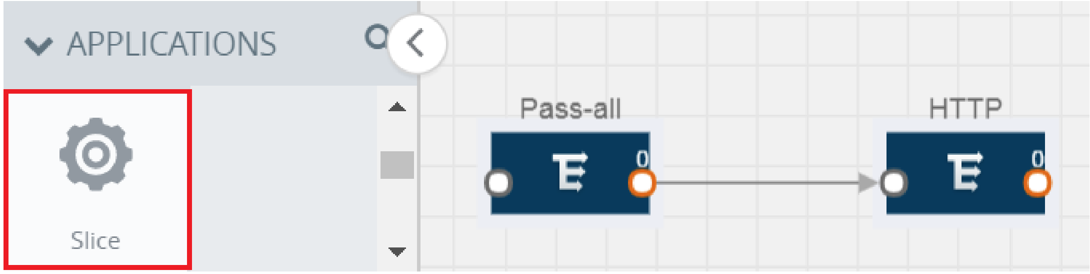
6. In the **Sampling Rate** field, enter the ratio of packets to be selected. The default ratio is 1:1.
7. Click **Save**.

Slicing

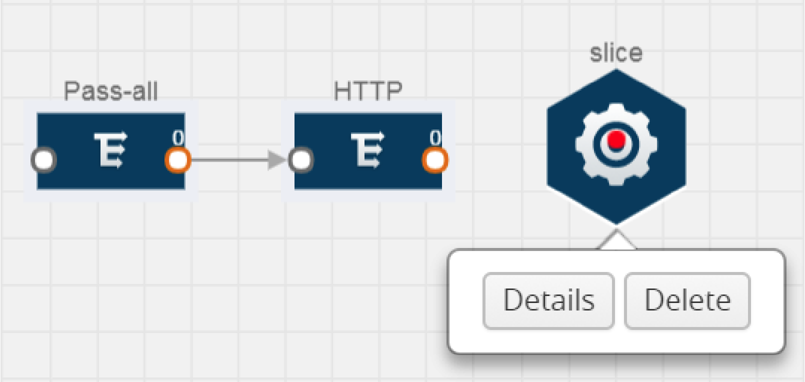
Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes.

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 the **On** check box to determine that the application is slicing packets. Select the **Off** check box to determine that the application is not currently slicing the packets. 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.

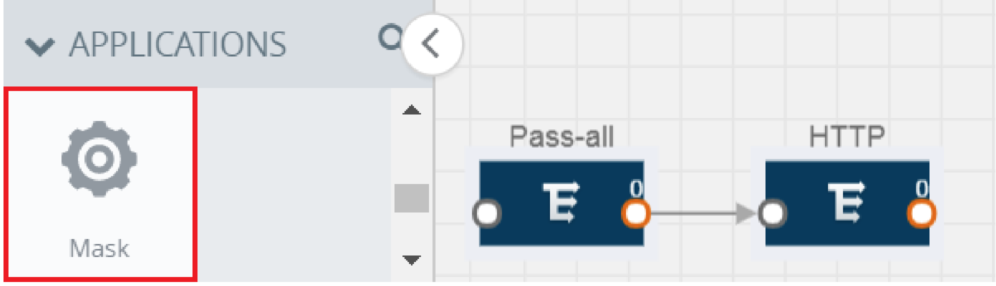
6. From the Protocol drop-down list, specify an optional parameter for slicing the specified length of the protocol. The options are as follows:
    - None
    - IPv4
    - IPv6
    - UDP
    - TCP
7. Click **Save**.

Masking

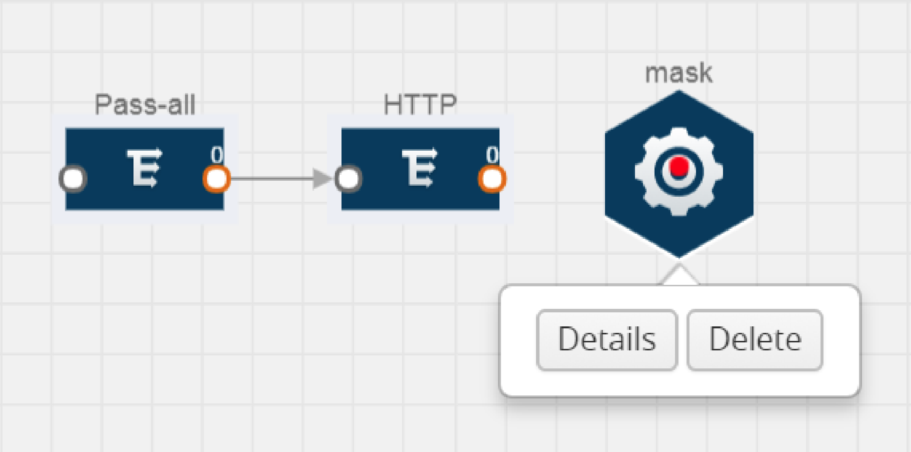
Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.

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 the **On** check box to determine that the application is masking packets. Select the **Off** check box to determine that the application is not currently masking the packets. 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 AWS.
- 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 Cloud Suite V Series node in the monitoring session.

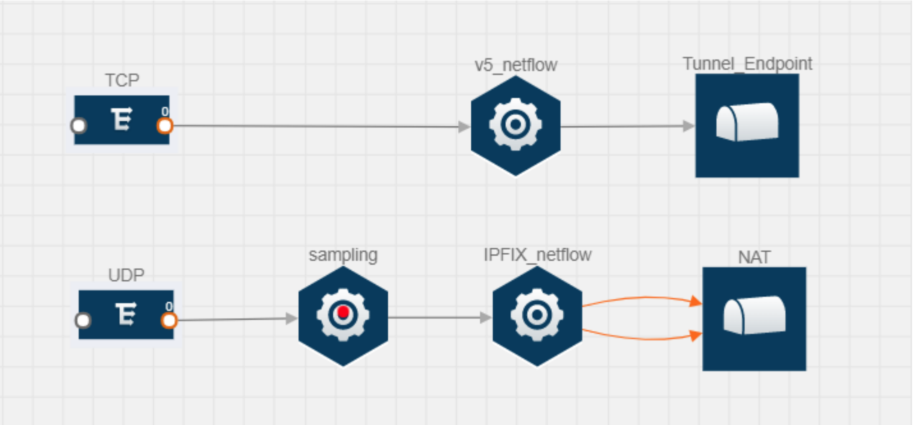


Figure 7 *NetFlow on GigaVUE Cloud Suite V Series Node*

The NetFlow record generation is performed on GigaVUE Cloud Suite V Series node running the NetFlow application. In Figure 7NetFlow on GigaVUE Cloud Suite V Series Node, incoming packets from G-vTAP agents are sent to the GigaVUE Cloud Suite 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:

Table 7: Match/Key Elements

	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.	IPFIX

	Description	Supported NetFlow Versions
	For IPv6, configures the value of the Hop Limit 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:

Table 8: Collect/Non-Key Elements

	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
Flow Start Sec	Configures the absolute timestamp of the first packet of this flow as a non-key field.	IPFIX

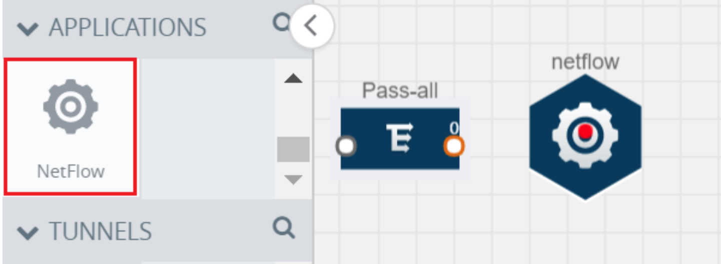
	Description	Supported NetFlow Versions
Flow Startup Time	Configures the flow start SysUp time as a non-key field.	v9 and IPFIX
Flow		
Flow End Reason	Configures the reason for Flow termination as a non-key field.	IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP message as a non-key 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
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	IPFIX

	Description	Supported NetFlow Versions
	header as a non-key field.	
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

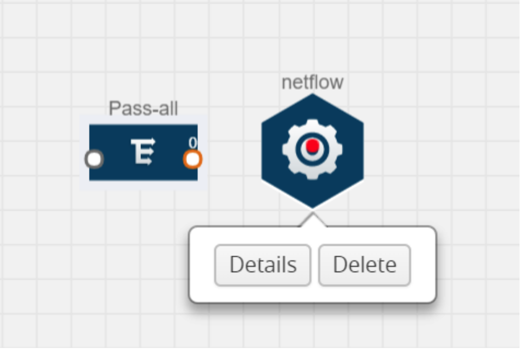
Add Version 5 NetFlow Application

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.



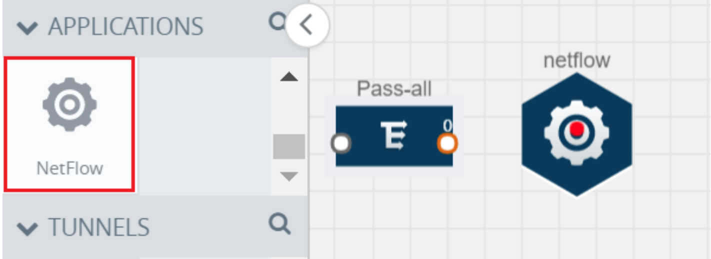
3. In the **Alias** field, enter a name for the v5 NetFlow application.
4. For State, select the **On** check box to determine that the application is currently running. Select the **Off** check box to determine that the application is currently not running. The state can be changed at anytime whenever 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.

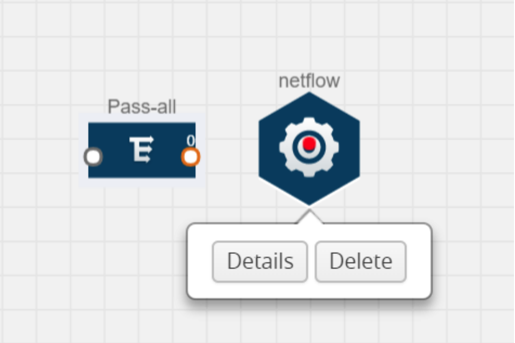
Add Version 9 and IPFIX NetFlow Application

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

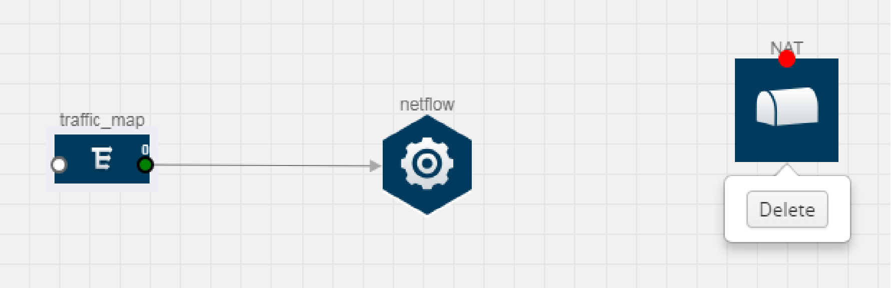
The NetFlow records are exported to the collector over UDP protocol with the configurable source IP and destination IP.

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

Add NAT

To add a NAT device:

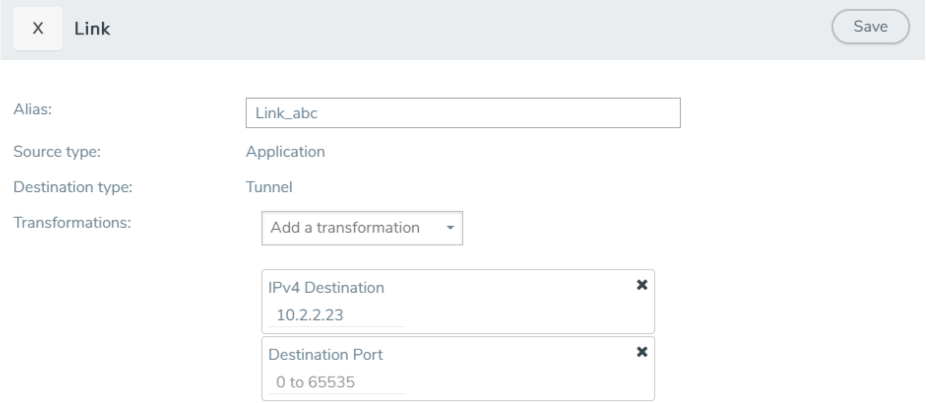
Drag and drop **NAT** to the graphical workspace.



Link NetFlow Application to NAT

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

1. 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.



Alias: Link_abc

Source type: Application

Destination type: Tunnel

Transformations: Add a transformation

IPv4 Destination: 10.2.2.23

Destination Port: 0 to 65535

Figure 8 *Creating a Link from NetFlow to NAT*

2. In the **Alias** field, enter a name for the link.
3. 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.

4. In **IPv4 Destination**, enter the IP address of the NetFlow collector.
5. (Optional) By default, the Destination Port is 2055. To change the destination port, enter a port number.

6. Click **Save**. The transformed link is displayed in Orange.
7. Repeat steps 7 to 10 to send additional NetFlow records to NAT.

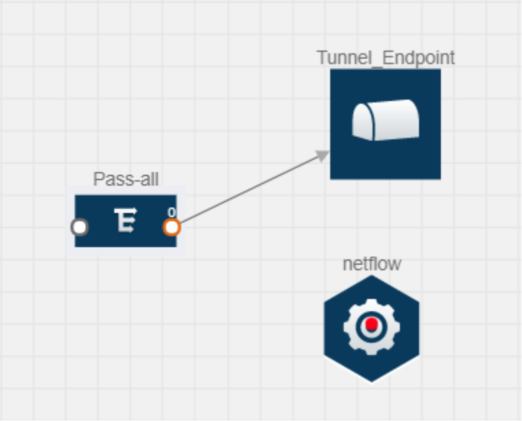
NetFlow Examples

This section provides an example to demonstrate the NetFlow application configuration in the GigaVUE Cloud Suite V Series nodes. Refer Example 1 below.

Example 1

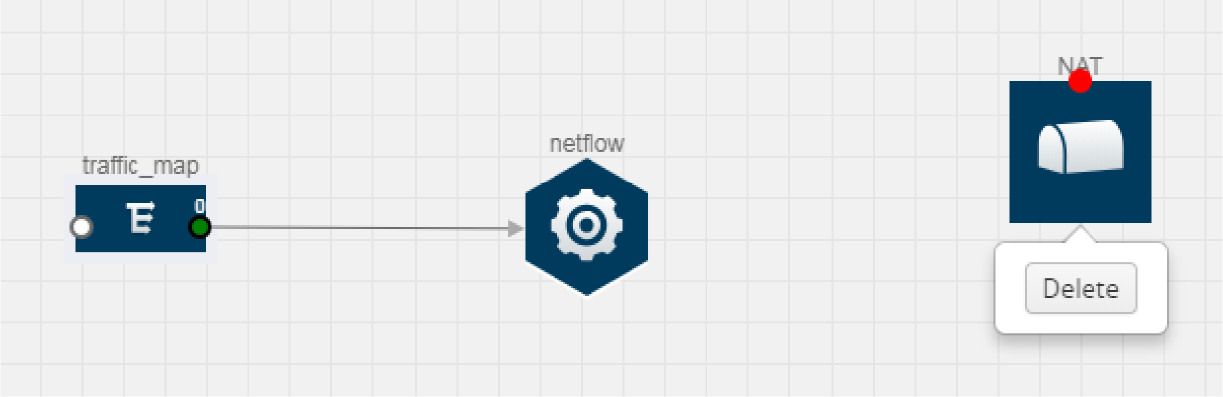
In this example, a pass all map is created and the entire traffic from a VPC is sent to a tool for full packet inspection. At the same time, a NetFlow application is added to generate flow records for flow inspection.

1. Create a monitoring session. For steps, refer to Create 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. For steps, refer to Clone Monitoring Session.
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.

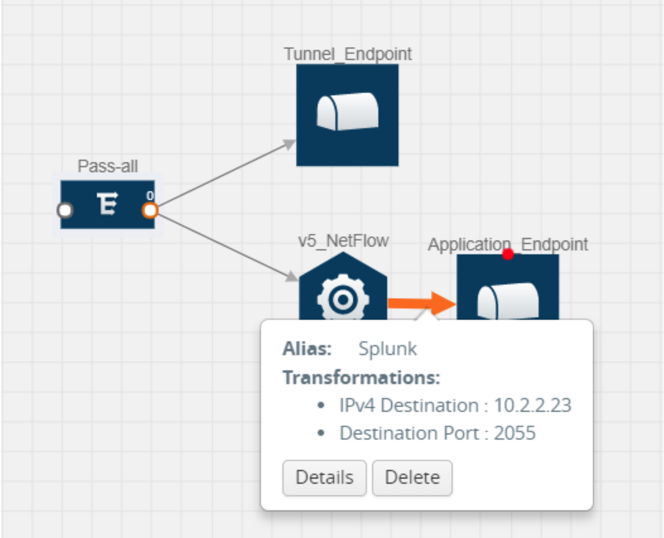


6. Click the NetFlow application and select **Details**. The Application quick view is displayed. For steps to configure the v5 NetFlow application, refer to Add Version 5 NetFlow Application.
7. Create a link from the Pass all map to the v5 NetFlow application.

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 Cloud Suite V Series node interface. For steps to configure the link, refer to Link NetFlow Application to NAT.
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.



Alias: Splunk
Transformations:
- IPv4 Destination : 10.2.2.23
- Destination Port : 2055

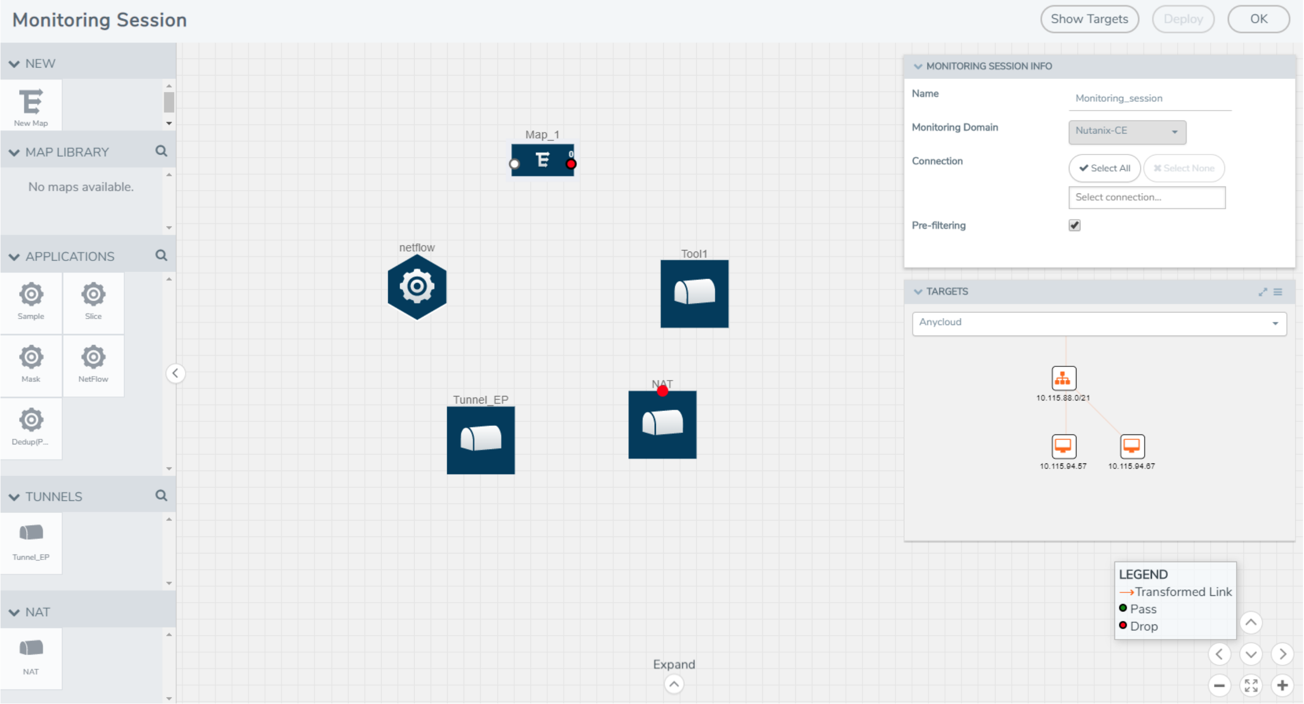
Deploying the Monitoring Session

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. Figure 9Dragging and Dropping the Maps, Applications, and Monitoring Tools illustrates three maps, one exclusion map, one application, and two tunnel endpoints that have been dragged and dropped to the workspace. The tunnel endpoints are named Monitoring_Tool_1 and Monitoring_Session_2.


Monitoring Session

MONITORING SESSION INFO

Name: Monitoring_session

Monitoring Domain: Nutanix-CE

Connection: Select connection...

Pre-filtering: ☑

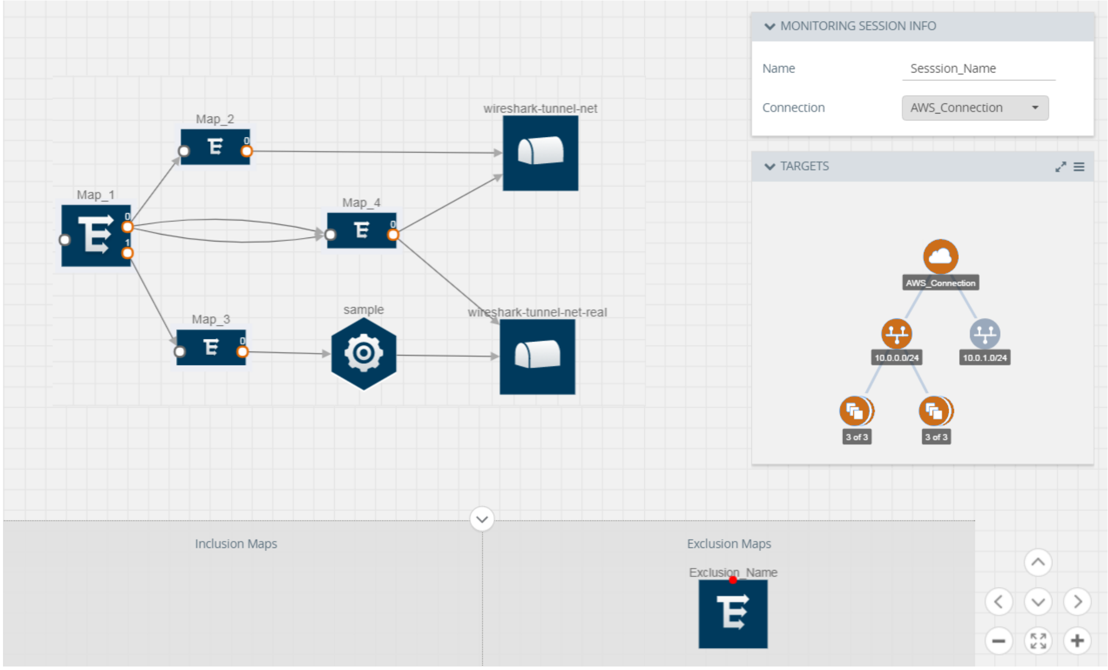
TARGETS: Anycloud

Figure 9 *Dragging and Dropping the Maps, Applications, and Monitoring Tools*

5. Hover your mouse on the map, click the red dot, and drag the arrow over to another map, application, or tunnel. Refer to Figure 10Connecting the Maps, Applications, and Monitoring Tools.

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

6. Hover your mouse on the application, click the red dot, and drag the arrow over to the tunnel endpoints. In Figure 10Connecting the Maps, Applications, and Monitoring Tools, the traffic matching the rules in each action set is routed to maps, applications, or monitoring tools.



MONITORING SESSION INFO

Name: Sesssion_Name

Connection: AWS_Connection

Figure 10 *Connecting the Maps, Applications, and Monitoring Tools*

7. 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.
8. 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 or TaaS. 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 TaaS or V Series node failure.
- Failure—The session is not deployed on any of the V Series nodes and G-vTAP agents or TaaS.

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

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.

Adding 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 VPCs 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 VPCs 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.

In Figure 11Action Set with Multiple Links, 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.

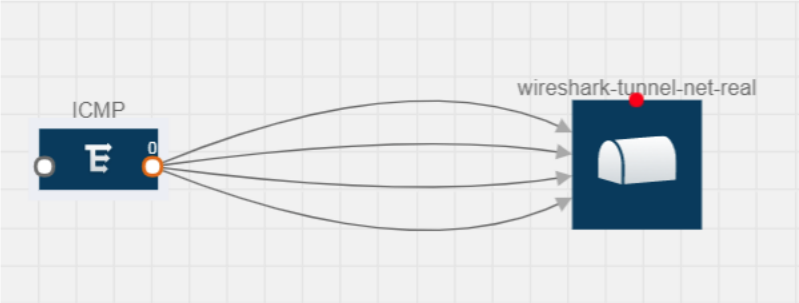


Figure 11 *Action Set with Multiple Links*

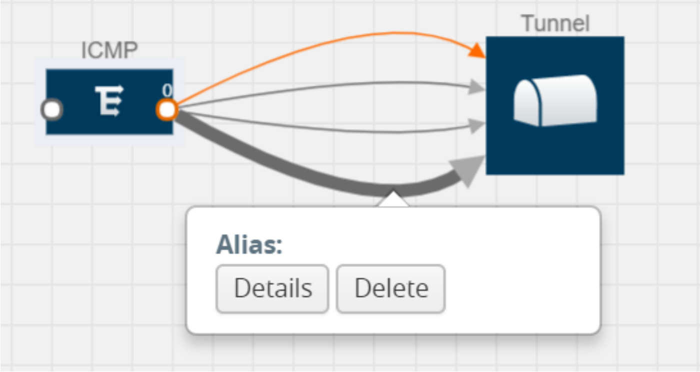
GigaVUE Cloud Suite V Series node supports the following header transformations:

Table 9: Header Transformations

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

Viewing the 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.

> **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.

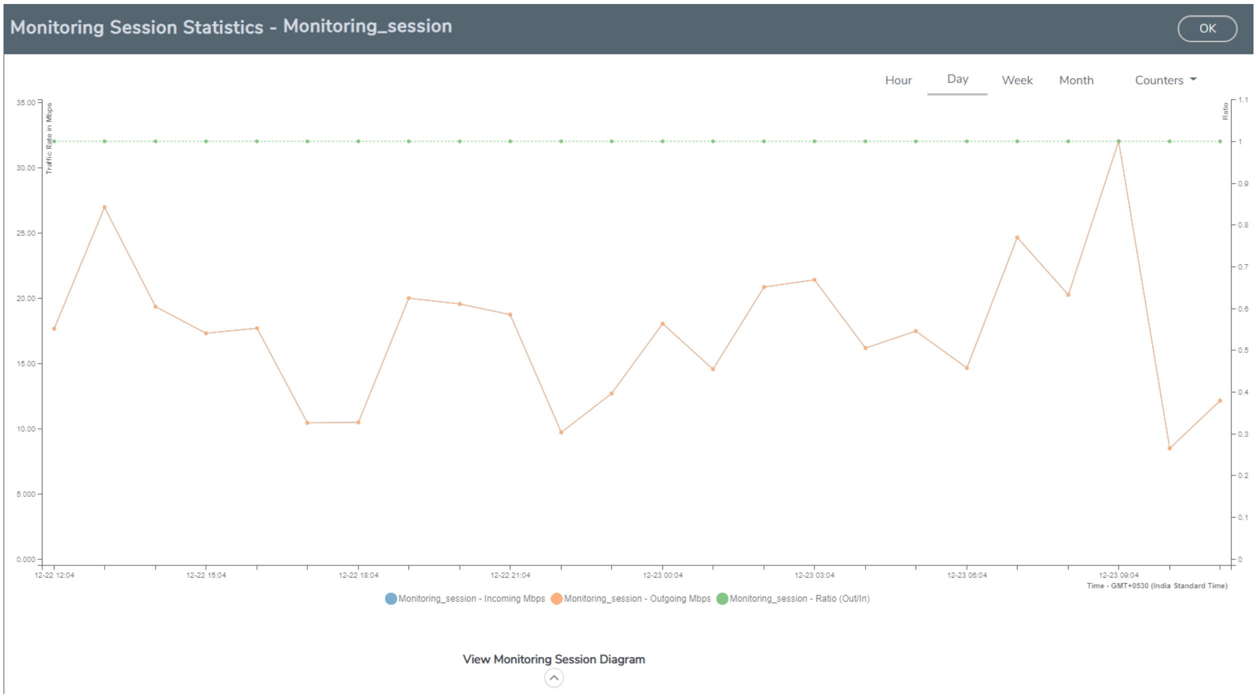

Monitoring Session Statistics - Monitoring_session
OK
Hour
Day
Week
Month
Counters
Traffic Rate in Mbps
35.00
30.00
25.00
20.00
15.00
10.00
5.000
0.000
Ratio
1.1
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
12-22 12:04
12-22 15:04
12-22 18:04
12-22 21:04
12-23 00:04
12-23 03:04
12-23 06:04
12-23 09:04
Time - GMT+0530 (India Standard Time)
Monitoring_session - Incoming Mbps
Monitoring_session - Outgoing Mbps
Monitoring_session - Ratio (Out/In)
View Monitoring Session Diagram

Figure 12 *Monitoring Session Statistics View*

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

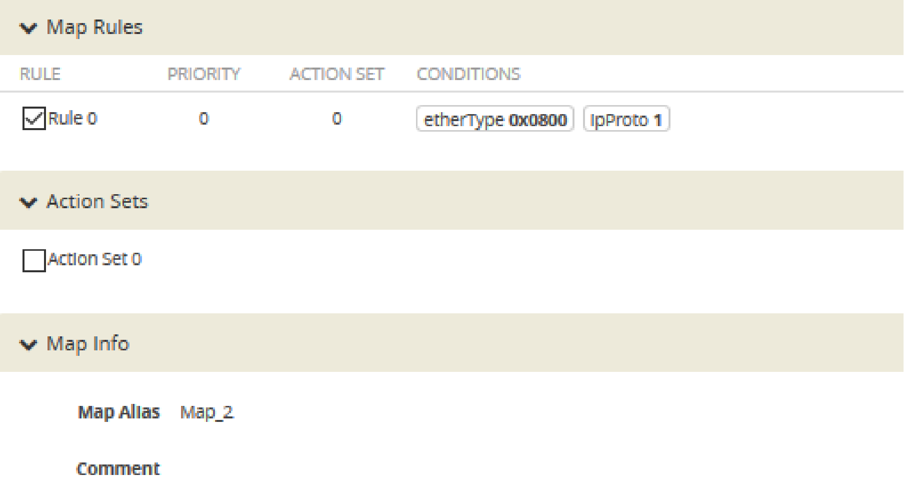
The Monitoring Session Statistics page appears where you can analyze incoming and outgoing traffic.

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

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

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

You can also scroll down the Map Statistics Quick View to see 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.



Map Rules

RULE	PRIORITY	ACTION SET	CONDITIONS
☑ Rule 0	0	0	etherType **0x0800** IpProto **1**

Action Sets

□ Action Set 0

Map Info

Map Alias Map_2

Comment

Viewing the Topology

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

To view the topology diagram:

1. Select **OpenStack > Topology**. The Topology page appears.
2. Select a connection from the **Select connection...** drop-down list. The topology view of the subnets and instances is displayed.
3. (Optional) Select a monitoring session from the **Select Monitoring Session...** drop-down list. The monitored subnets and instances change to blue.
4. Select one of the following check boxes:
   - **Source**— Displays the topology view of the source target interfaces that are being monitored.
   - **Destination**—Displays the topology view of the destination target interfaces where the traffic is being mirrored.
   - **Other**—Displays the topology view of the non-G-vTAP agents such as GigaVUE Cloud Suite V Series Controllers, G-vTAP Controllers, monitoring tools, and instances that are being used in the connection.

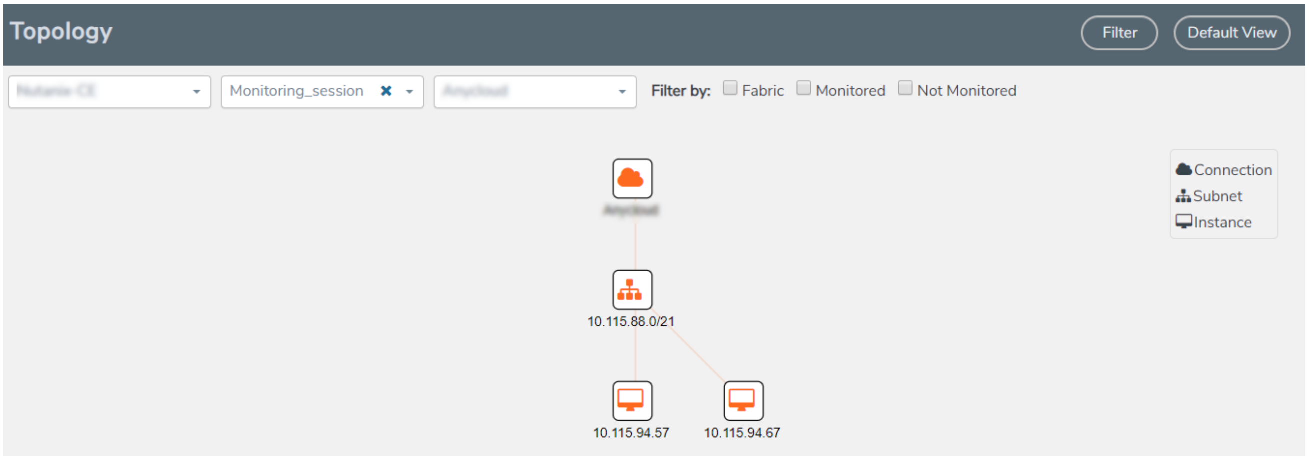


Figure 13 *Viewing the Topology*

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.

At the right-bottom corner of the Topology page, there are arrows to move the page up, down, left, or right. There are also plus, minus, and full screen icons to zoom in and zoom out.

On the Topology page, you can also use the **Filter** button to filter instances based on the Instance Name Prefix, Instance IP, Subnet ID, or Subnet IP to view the topology based on the filtered results.

To remove a filter, click the **Clear Filter** button.

Configuring the OpenStack Settings

To configure the OpenStack Settings:

1. In GigaVUE-FM, on the top navigation pane, select **Cloud**.
2. On the left navigation pane, select **OpenStack > Configuration.**
3. Select **Settings** to edit the OpenStack settings. The **Settings** page appears.

4. Click **Edit** to edit the Settings fields. Refer to Table 10: OpenStack Settings for descriptions of the Settings fields:

Table 10: OpenStack Settings

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of project connections you can establish in GigaVUE-FM.
Refresh interval for instance inventory (secs)	Specifies the frequency for updating the state of cloud instances in OpenStack.
Number of instances per V Series Node	Specifies the maximum number of instances 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.

Compatibility Matrix

This appendix provides information about GigaVUE-FM version compatibility and the features supported in various versions of GigaVUE Cloud Suite V Series nodes and G-vTAP agents.

Refer to the following sections for details:

- GigaVUE-FM Version Compatibility
- Supported Features in GigaVUE Cloud Suite V Series Nodes
- Supported Features in G-vTAP Agents

GigaVUE-FM Version Compatibility

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

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Controller	GigaVUE Cloud Suite-V Series Nodes
5.3.01	v1.4-1	v1.4-1	v1.4-1	v1.4-1
5.4.00	v1.4-1	v1.4-1	v1.4-1	v1.4-1

Supported Features in GigaVUE Cloud Suite V Series Nodes

The following table lists the features supported in various versions of GigaVUE Cloud Suite V Series nodes:

Features	GigaVUE Cloud Suite V Series v1.4-x
Header Transformation	Yes
Multi-link Support	Yes
NetFlow Application	Yes
NAT Support	Yes

Supported Features in G-vTAP Agents

The following table lists the features supported in various versions of G-Tap Agents:

Features	G-vTAP Agent v1.4-x
Dual ENI Support	Yes
Single ENI Support	Yes
VXLAN Support	Yes
Agent Pre-filtering	Yes

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 Cloud Suite V Series Node or G-vTAP Controller is Unreachable

If GigaVUE Cloud Suite 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 Gigamon Community

Documentation

> **ATTENTION**: 5.10.00 was delivered as embedded software on new hardware only. The updated PDFs for the 5.10.01 software release are coming soon! Check back on 8/29/2020 for the latest.

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.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
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
***G-TAP A Series 2 Installation Guide**
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide *(now including TA25)*
***GigaVUE-OS Installation Guide for DELL S4112F-ON** how to install GigaVUE-OS and configure ports on COTS DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide how to install GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM how to migrate GigaVUE-FM on VMware ESXi, Hardware Appliance, and AWS
GigaVUE-OS Upgrade Guide

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
how to upgrade the embedded GigaVUE-OS on GigaVUE H Series and GigaVUE TA Series nodes
Administration
GigaVUE-OS and GigaVUE-FM Administration Guide how to administer the GigaVUE-OS and GigaVUE-FM software (note, new file name for PDF)
Fabric Management
GigaVUE-FM User's Guide how to install, deploy, and operate GigaVUE-FM how to configure GigaSMART operations includes instructions for GigaVUE-FM and GigaVUE-OS features
Cloud Configuration and Monitoring how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the respective cloud platform
GigaVUE Cloud Suite for AnyCloud Configuration Guide how to deploy the GigaVUE Cloud Suite solution in any cloud platform
GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS Quick Start Guide quick view of AWS deployment used in conjunction with the GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS SecretRegions Configuration Guide
GigaVUE Cloud Suite for Azure Configuration Guide
GigaVUE Cloud Suite for Kubernetes Configuration Guide
GigaVUE Cloud Suite for Nutanix Configuration Guide
GigaVUE Cloud Suite for OpenStack Configuration Guide
GigaVUE Cloud Suite for VMware Configuration Guide
Gigamon Containerized Broker
Reference
GigaVUE-OS-CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
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 .
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Docs** 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 & Documentation** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," 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

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

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

Contact Technical Support

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

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.

- Submit and vote on feature enhancements and share product feedback. (Customers only)
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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