GigaVUE Cloud Suite for OpenStack– GigaVUE V Series 2 Guide

GigaVUE Cloud Suite

Product Version: 5.16

Document Version: 1.0

(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
5.16.00	1.0	05/26/2022	Original release of this document with 5.16.00 GA.

Contents

GigaVUE Cloud Suite for OpenStack

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

Refer to the following sections for details:

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

About GigaVUE Cloud Suite for OpenStack

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

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

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

In a multi-project OpenStack cloud, where project isolation is critical, the 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.

Refer to the following sections for details:

- Components of GigaVUE Cloud Suite for OpenStack
- Architecture of GigaVUE Cloud Suite for OpenStack

Components of GigaVUE Cloud Suite for OpenStack

The GigaVUE Cloud Suite for OpenStack includes the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud.

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

- G-vTAP Controllers (only if you are using G-vTAP Agent as the traffic acquisition method)
- GigaVUE V Series 2 Configuration
  - GigaVUE® V Series Proxy
  - GigaVUE® V Series 2 nodes

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

Architecture of GigaVUE Cloud Suite for OpenStack

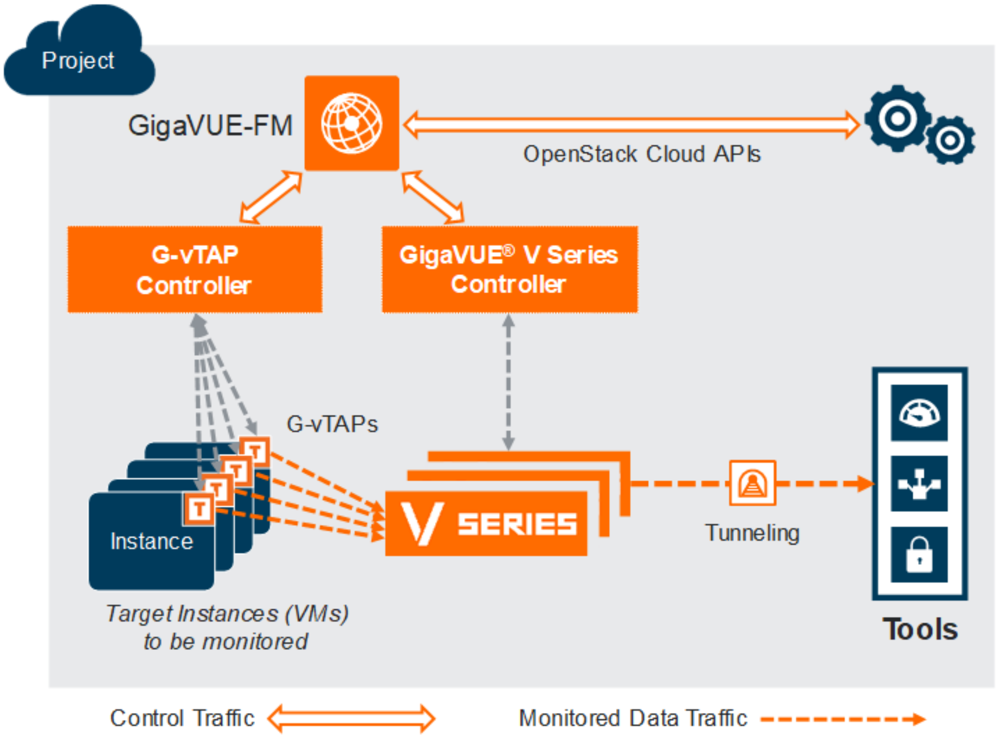
GigaVUE Cloud Suite for OpenStack captures traffic in OpenStack cloud using G-vTAP Agents directly or through the hypervisor as described in this section.

Refer to the following architectures for details:

- G-vTAP Agent
- Open vSwitch (OVS) Mirroring

G-vTAP Agent

A G-vTAP Agent is a tiny footprint user-space agent (G-vTAP) that is deployed in a project instance. This agent mirrors the traffic from a source interface to a destination mirror interface. The mirrored traffic is then sent to the GigaVUE® V Series node. The following figure shows a high-level architecture of GigaVUE Cloud Suite for OpenStack using G-vTAP Agents as the source for acquiring the traffic.



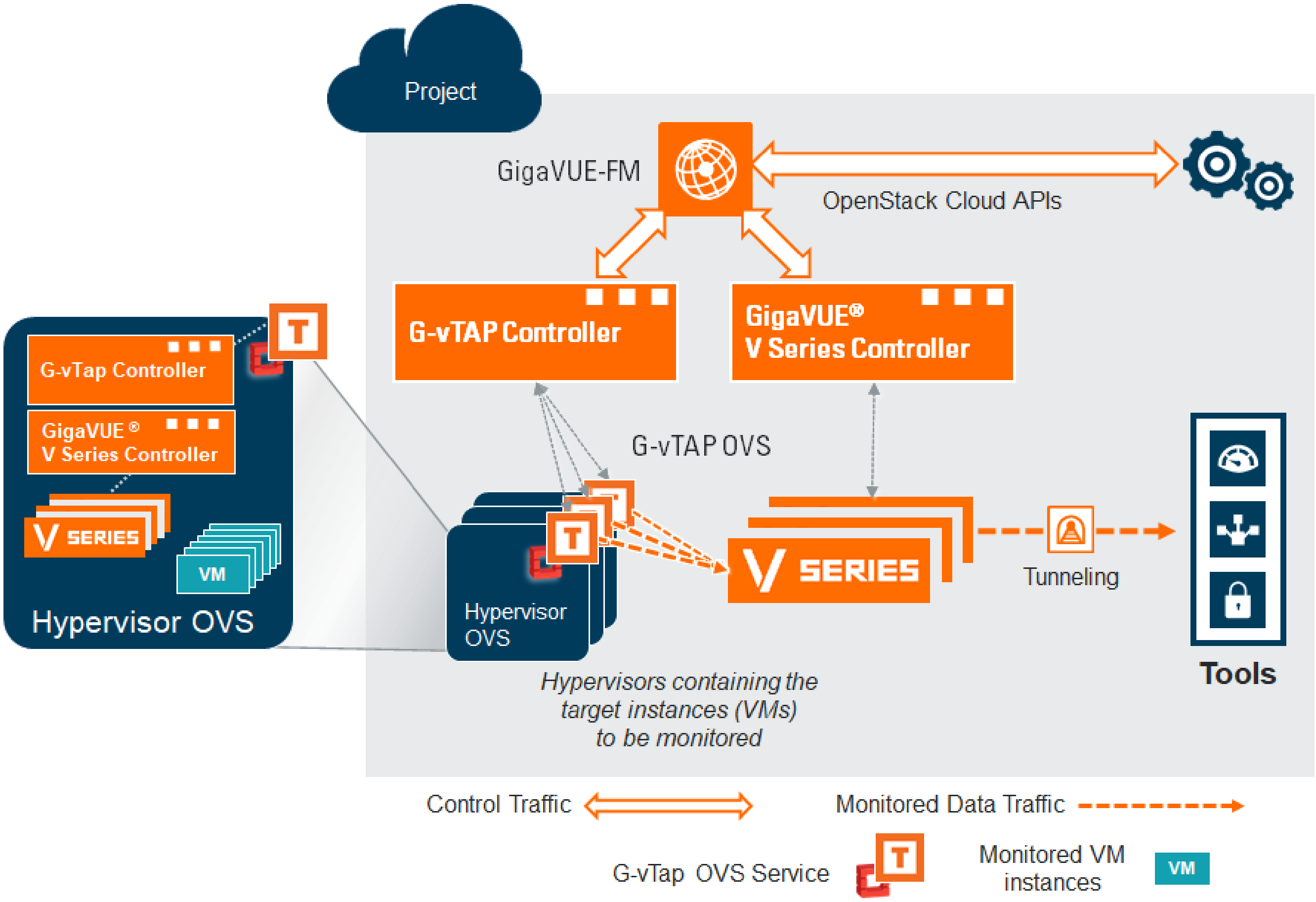
A G-vTAP Agent is deployed by installing the agent in the virtual instances. When a G-vTAP Agent is installed, a G-vTAP Controller must be configured in your environment. A G-vTAP Controller orchestrates the flow of mirrored traffic from G-vTAP Agents to the GigaVUE V Series nodes. A single G-vTAP Controller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

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

Open vSwitch (OVS) Mirroring

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

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



> **NOTE:** GigaVUE Cloud Suite for OpenStack supports both the access ports and the VLAN trunk ports for OVS traffic mirroring. To override the default values of OVS mirror tunnel ID range, refer to Configure the OpenStack Settings.

The G-vTAP Agents are deployed on the target hypervisors and the configuration file is to be modified based on the requirements and service. GigaVUE-FM connects to G-vTAP Controller and each G-vTAP Controller can talk to G-vTAP Agents. GigaVUE-FM identifies the interfaces to be monitored from the monitoring session details. GigaVUE-FM mirrors and forwards the traffic to the GigaVUE V Series nodes based on the deployed Monitoring Session.

> - G-vTAP configures traffic mirroring in the OVS (with or without DPDK) and the management of the mirrored traffic is completely based on OVS architecture and the server.

- OVS Mirroring also supports Open vSwitch with DPDK. The configuration steps for OVS Mirroring and OVS Mirroring with DPDK are the same.

Refer Deploying Gigamon CloudSuite on OpenStack to scale-in and scale-out monitoring tools for more detailed information.

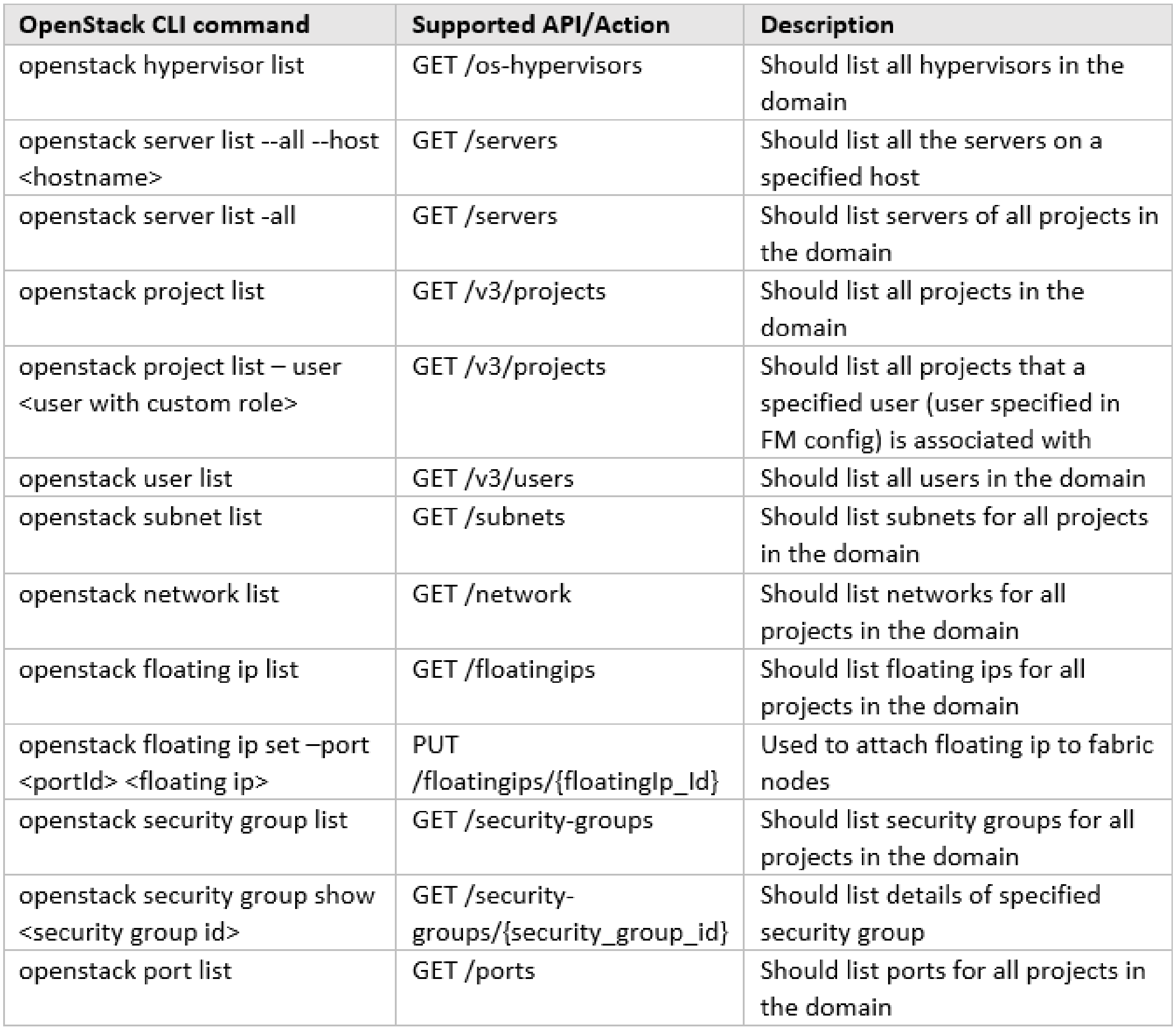
Prerequisites for OVS Mirroring

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

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

OpenStack Cloud Environment Requirements

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



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

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

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

- value: reachable IP for hypervisor

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

Get Started with GigaVUE Cloud Suite for OpenStack Deployment

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

- Before You Begin
- Install and Upgrade GigaVUE-FM

License Information

GigaVUE Cloud Suite for OpenStack supports the Volume Based License.

Volume Based License (VBL)

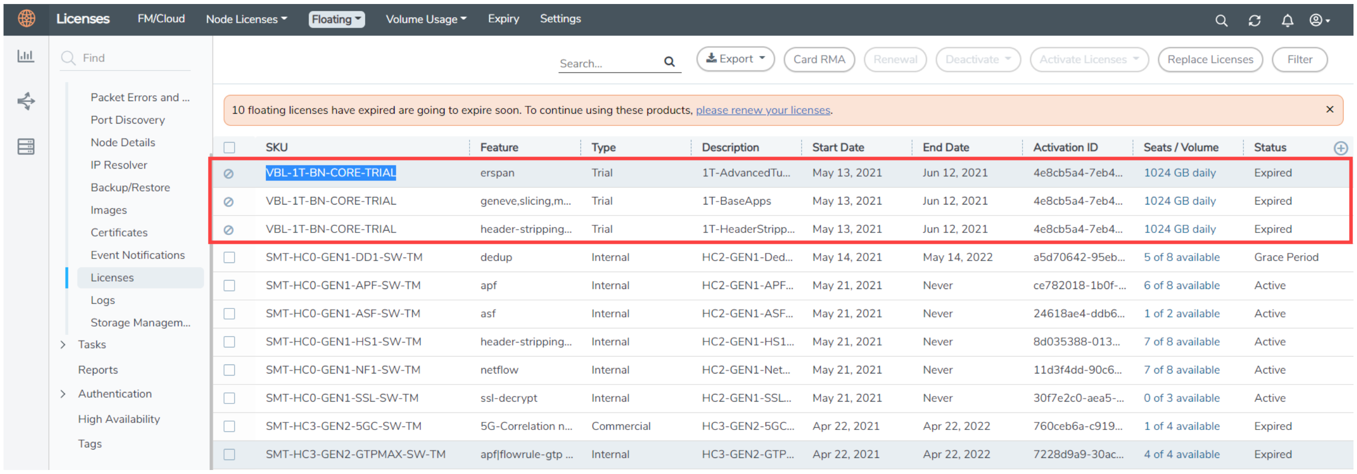
All the V Series 2 nodes connected to GigaVUE-FM reports the stats. All licensed applications, when running on the node, generate usage statistics. In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility into the actual amount of data, each licensed application is using on each node, and track the overuse if any. You will have grace period for each license that are conveyed in the license file.

For purchasing licenses with the VBL option, contact our Gigamon Sales. Refer to Contact Sales.

For details about:	Reference section	Guide
Volume-Based License Usage Details from GigaVUE-FM GUI	Volume Usage	GigaVUE Administration Guide
How to Generate Volume-Based License reports	Generate VBL Usage Reports	GigaVUE Administration Guide
Volume Based Licensed Report Details	Volume Based License Usage Report	GigaVUE Administration Guide
Fabric Health Analytics Dashboards for Volume Based Licenses Usage	Dashboards for Volume Based Licenses Usage	GigaVUE-FM User Guide

Default Trial Licenses

After you install GigaVUE-FM, a default free 1TB of CoreVUE trial volume-based license (VBL) is provided one-time for 30 days (from the date of installation).



10 floating licenses have expired are going to expire soon. To continue using these products, please renew your licenses.

SKU	Feature	Type	Description	Start Date	End Date	Activation ID	Seats / Volume	Status
VBL-1T-BN-CORE-TRIAL	erspan	Trial	1T-AdvancedTu...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	geneve,slicing,m...	Trial	1T-BaseApps	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	header-stripping...	Trial	1T-HeaderStripp...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
SMT-HC0-GEN1-DD1-SW-TM	dedup	Internal	HC2-GEN1-Ded...	May 14, 2021	May 14, 2022	a5d70642-95eb...	5 of 8 available	Grace Period
SMT-HC0-GEN1-APF-SW-TM	apf	Internal	HC2-GEN1-APF...	May 21, 2021	Never	ce782018-1b0f-...	6 of 8 available	Active
SMT-HC0-GEN1-ASF-SW-TM	asf	Internal	HC2-GEN1-ASF...	May 21, 2021	Never	24618ae4-ddb6...	1 of 2 available	Active
SMT-HC0-GEN1-HS1-SW-TM	header-stripping...	Internal	HC2-GEN1-HS1...	May 21, 2021	Never	8d035388-013...	7 of 8 available	Active
SMT-HC0-GEN1-NF1-SW-TM	netflow	Internal	HC2-GEN1-Net...	May 21, 2021	Never	11d3f4dd-90c6...	7 of 8 available	Active
SMT-HC0-GEN1-SSL-SW-TM	ssl-decrypt	Internal	HC2-GEN1-SSL...	May 21, 2021	Never	30f7e2c0-aea5-...	0 of 3 available	Active
SMT-HC3-GEN2-5GC-SW-TM	5G-Correlation n...	Commercial	HC3-GEN2-5GC...	Apr 22, 2021	Apr 22, 2022	760ceb6a-c919...	1 of 4 available	Expired
SMT-HC3-GEN2-GTPMAX-SW-TM	apf|flowrule-gtp ...	Internal	HC3-GEN2-GTP...	Apr 22, 2021	Apr 22, 2022	7228d9a9-30ac...	4 of 4 available	Expired

This license includes the following applications:

- ERSPAN
- Geneve
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap
- Header-stripping
- Add header

> **NOTE:** There is no grace period for the trial licenses. If you do not have any other Volume-based licenses installed, then after 30 days, on expiry of the trial licenses, any deployed monitoring sessions will be undeployed from the existing V series 2.0 nodes.

To deactivate the trial VBL refer to Delete Default Trial Licensessection for details.

How GigaVUE-FM tracks Volume-based License Usage

GigaVUE-FM tracks the license usage for each V series node as follows:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use the only those applications that are licensed at that point.
- When a license goes into grace period, you will be notified, along with a list of monitoring sessions that would be affected in the near future.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will be undeployed, but not deleted from the database.
- When a license is later renewed or newly imported, the undeployed monitoring sessions will be redeployed.

Before You Begin

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

- Supported Hypervisor
- Minimum Compute Requirements
- Network Requirements
- Virtual Network Interface Cards (vNICs)
- Security Group
- Create a Security Group
- Key Pairs

Supported Hypervisor

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

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

Minimum Compute Requirements

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

Compute Instances	vCPU	Memory	Disk Space	Description
G-vTAP Agent	2 vCPU	4GB	N/A	Available as rpm or debian package. Instances can have a single vNIC or dual vNICs configured for monitoring the traffic.
G-vTAP Controller	1 vCPU	4GB	8GB	Based on the number of agents being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE V Series Node	2 vCPU	3.75GB	20GB	NIC 1: Monitored Network IP; Can be used as Tunnel IP NIC 2: Tunnel IP (optional) NIC 3: Management IP
GigaVUE V Series Proxy	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	4 vCPU	8GB	40GB	GigaVUE-FM must be able to access the controller instance for relaying the commands. Use a flavor with a root disk of minimum 40GB and an ephemeral disk of minimum 41GB.

The instance size of the GigaVUE V Series is configured and packaged as part of the qcow2 image file.

Network Requirements

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

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

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 V Series Proxies, GigaVUE 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.

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

Direction	Ether Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	HTTPS	TCP	443	Any IP address	Allows users to connect to the GigaVUE-FM GUI.
Inbound	IPv4	UDP	53	Any IP address	Allows GigaVUE-FM to communicate with standard DNS server
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with V Series node
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers

Direction	Ether Type	Protocol	Port	CIDR	Purpose
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP Agents
G-vTAP OVS Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP OVS Controllers
G-vTAP OVS Agent					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP OVS Controller IP	Allows G-vTAP OVS Controllers to communicate with G-vTAP OVS Agents
GigaVUE V Series Proxy					
Inbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite V Series Proxys.
Outbound	Custom TCP Rule	TCP	8889	V Series 2 node IP	Allows V Series Proxy to communicate with V Series node
GigaVUE V Series 2 Node					
Inbound	Custom TCP Rule	TCP(6)	8889	GigaVUE V Series Proxy IP address	Allows GigaVUE V Series Proxys to communicate with GigaVUE V Series nodes
Outbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE V Series Node to communicate with GigaVUE V Series Proxy
Outbound	Custom UDP Rule	UDP	● VXLAN (default 4789) ● L2GRE (IP 47)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool

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.

Key Pairs

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

Install and Upgrade GigaVUE-FM

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

- Cloud—To install GigaVUE-FM inside your OpenStack environment, you can simply launch the GigaVUE-FM instance in your Project. For installing the GigaVUE-FM instance, refer to *GigaVUE-FM Installation and Upgrade Guide*.

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

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

Deploy GigaVUE Cloud Suite for OpenStack

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

Refer to the following sections for details:

- Upload Fabric Images
- Prepare G-vTAP Agent to Monitor Traffic
- Pre-Configuration Checklist
- Create Monitoring Domain
- Configure GigaVUE Fabric Components
- Configure GigaVUE Fabric Components in OpenStack
- Upgrade Virtual Fabric in OpenStack

Refer to the following Gigamon Validated Designs for more detailed information:

- Deploying V Series 2 visibility solution for OpenStack
- Gaining Visibility and Optimizing the Traffic Between Containerized Workloads for Seamless Monitoring

Upload Fabric Images

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

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

```
$ source admin_openrc.sh
```

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

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

Or

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

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

- gigamon-gigavue-vseries-node-2.x.x
- gigamon-gigavue-vseries-proxy-2.x.x
- gigamon-gigavue-gvtap-cntlr-1.x.x
- gigamon-gigavue-gvtap-ovs-cntlr-1.x.x

> **NOTE:** After uploading the V Series 2 nodes, you must set the image properties.
> openstack image set --property hw_vif_multiqueue_enabled=true $IMAGE_ID

Prepare G-vTAP Agent to Monitor Traffic

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

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

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

Refer to the following sections for more information:

- Linux G-vTAP Agent Installation
- Install G-vTAP OVS Agent for OVS Mirroring
- Windows G-vTAP Agent Installation

Linux G-vTAP Agent Installation

Refer to the following sections for Linux agent installation:

- Single vNIC Configuration
- Multiple vNICs Configuration
- Install G-vTAP Agents

Single vNIC Configuration

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

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

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

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

Grant permission to monitor ingress and egress traffic at iface

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

Multiple vNICs Configuration

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

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

Install G-vTAP Agents

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

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

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

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

Refer to the following topics for details:

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

Install G-vTAP from Ubuntu/Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent **1.8-5** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_1.8-5_amd64.deb
ubuntu@ip-10-0-0-246:~$ sudo dpkg -i    gvtap-agent_1.8-5_amd64.deb
```

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 following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

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

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

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

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

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

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

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

4. Save the file.

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

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

6. Reboot the instance.

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

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

Install G-vTAP from RPM package

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

1. Download the G-vTAP Agent `1.8-5` RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

   ```
   [user@ip-10-0-0-214 ~]$ lsgvtap-agent_1.8-5_x86_64.rpm[user@ip-10-0-0-214 ~]$ sudo rpm -i
   gvtap-agent_1.8-5_x86_64.rpm
   ```

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

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

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

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

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

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

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

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

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

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

6. Reboot the instance.

Check the status with the following command:

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

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

1. Launch the RHEL/CentOS agent AMI image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**1.8-5**_x86_64.rpm
   - gvtap.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
5. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_1.8-5_x86_64.rpm
   ```
6. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   # sudo /etc/init.d/gvtap-agent restart
   ```
7. Install strongSwan:
   ```
   tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
   cd strongswan-5.7.1-1.el7.x86_64
   sudo sh ./swan-install.sh
   ```
8. Reboot the instance.

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent `1.8-5` MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator** and the G-vTAP Agent service starts automatically.
3. Once the G-vTAP package is installed, modify the file **C:\ProgramData\Gvtap-agent\gvtap-agent.conf** to configure and register the source and destination interfaces.

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

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

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

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

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

   ```
   # 192.168.1.0/24   mirror-src-ingress mirror-src-egress
   # 192.168.2.0/24   mirror-dst
   ```
4. Save the file.

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

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

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

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

Windows G-vTAP Agent Installation Using ZIP Package

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

1. Download the Windows G-vTAP Agent `1.8-5` ZIP package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Extract the contents of the .zip file into a convenient location.
3. Run ‘install.bat’ as an **Administrator** and the G-vTAP Agent service starts automatically.

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

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

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

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

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

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

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

5. Save the file.

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

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

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

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

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

Install G-vTAP OVS Agent for OVS Mirroring

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

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

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

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

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

To install from a Debian package:

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

```
$ ls gvtap-ovs-agent_1.8-1_amd64.deb
$ sudo dpkg -i gvtap-ovs-agent_1.8-1_amd64.deb
```

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

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

   ```
   br-int mirror-dst

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

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

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

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

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

Install the G-vTAP OVS Agent from RPM package

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

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

   ```
   $ ls gvtap-ovs-agent_1.8-1_x86_64.rpm
   $ sudo rpm -ivh gvtap-ovs-agent_1.8-1_x86_64.rpm
   ```

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

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

   ```
   # br-int mirror-dst

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

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

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

> When you are installing a self-signed RPM package, you must execute the following command to import the signing key into the RPM db.
>
> ```
> sudo rpm --import /path/to/YOUR-RPM-GPG-KEY
> ```

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

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

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

Pre-Configuration Checklist

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

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

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

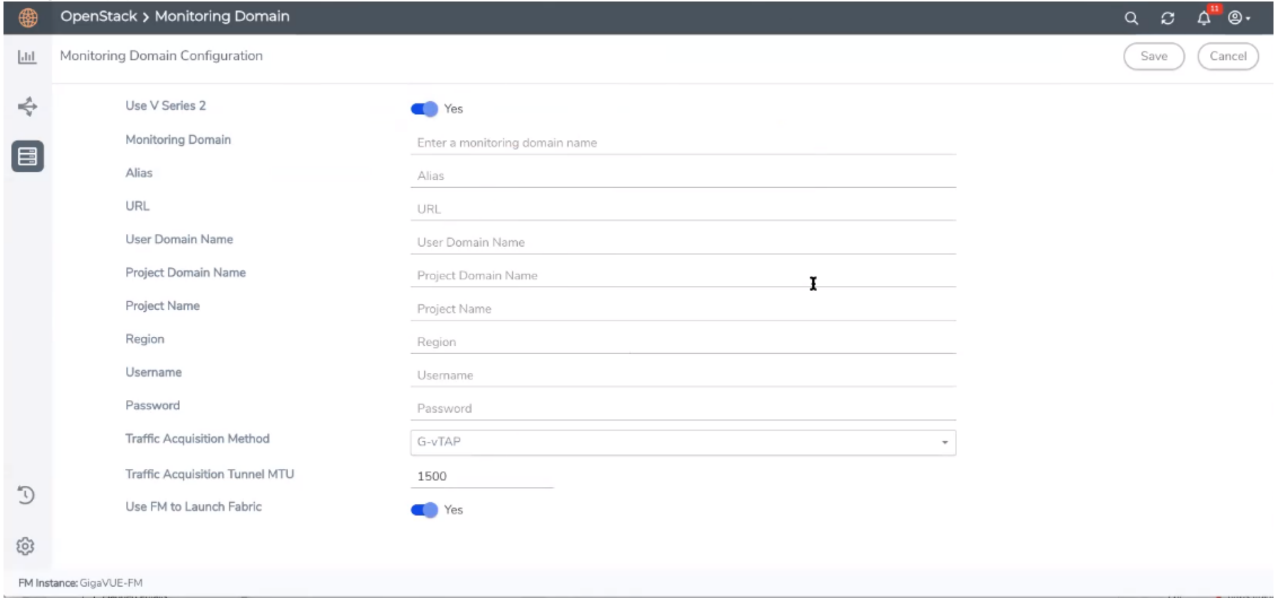
NOTE: If you are not using DNS, you must manually enter the host entry in /etc/hosts on GigaVUE-FM for the OpenStack Controller. On using DNS you can directly enter the host entry in GigaVUE-FM.

	Required Information
□	Authentication URL
□	Project Name
□	Floating IP
□	Region name for the Project
□	Domain
□	SSH Key Pair
□	Networks
□	Security groups

Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > OpenStack > Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, click **New**. The **Monitoring Domain Configuration** page appears.


OpenStack > Monitoring Domain
Monitoring Domain Configuration
Save
Cancel
FM Instance: GigaVUE-FM

Use V Series 2: Yes

Monitoring Domain: Enter a monitoring domain name

Alias: Alias

URL: URL

User Domain Name: User Domain Name

Project Domain Name: Project Domain Name

Project Name: Project Name

Region: Region

Username: Username

Password: Password

Traffic Acquisition Method: G-vTAP

Traffic Acquisition Tunnel MTU: 1500

Use FM to Launch Fabric: Yes

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

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

Field	Description
Use V Series 2	Select **Yes** for V Series 2 configuration.
Monitoring Domain	A name for the monitoring domain.
Alias	An alias used to identify the monitoring domain.
URL	The authentication URL is the Keystone URL of the OpenStack cloud. This IP address must be DNS resolvable. Refer to the OpenStack User Manual for more information on retrieving the authentication URL from the OpenStack.
User Domain Name	The domain name of your OpenStack authentication domain. NOTE: • If you are using a separate domain for AUTH, enter that domain name as User Domain Name. • If you are not using a separate domain, you can use the same domain for User and Project Domain Name.
Project Domain Name	The domain name of your OpenStack project.
Project Name	The name of the project used for OpenStack authentication.
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** or looking at the RC file in OpenStack to view your credentials.
Username	The username used to connect to your OpenStack cloud. NOTE: If you are using OVS mirroring, you must belong to a role that meets the OpenStack minimum requirements for OVS Mirroring. Refer to OVS Mirroring Prerequisites for more information.
Password	The password of your OpenStack cloud.
Traffic Acquisition Method	Select the type of agent used to capture traffic for monitoring: ● **G-vTAP:** If you select G-vTAP as the tapping method, the traffic is acquired from the G-vTAP Agents installed on the VMs. You must configure the G-vTAP Controller to monitor the G-vTAP Agents.

Field	Description
	- **OVS Mirroring:** If you select OVS Mirroring as your tapping method, the traffic is acquired from the G-vTAP Agents installed on the hypervisors. Refer to Open vSwitch (OVS) Mirroring for detailed information. You must configure the G-vTAP Controller to monitor the G-vTAP Agents. - **Tunnel:** If you select Tunnel as the tapping method, you can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying G-vTAP Agents or G-vTAP controllers.
Projects to Monitor (Only for OVS Mirroring traffic acquisition method)	This field only appears for OVS Mirroring traffic acquisition method. - Click the **Get Project List** 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 projects that you want to monitor from the list. - You can click **Select None** to clear existing selections or **Select All** to add all available projects to the connection configuration.
Traffic Acquisition Tunnel MTU (Maximum Transmission Unit)	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 default MTU size.

4. Click **Save**. The **OpenStack Fabric Launch Configuration** page appears. Refer to Configure GigaVUE Fabric Components for detailed information.

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

Configure GigaVUE Fabric Components

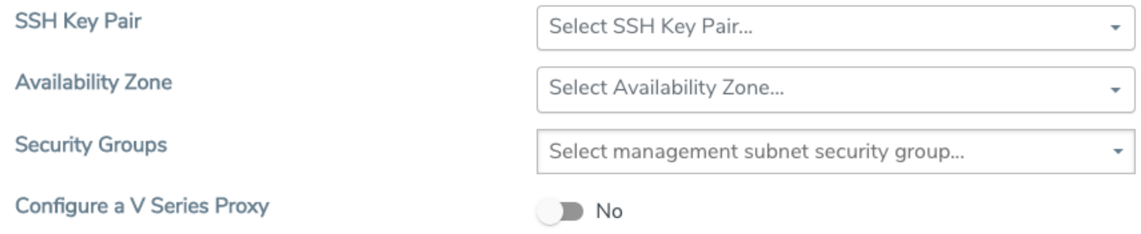
After configuring the Monitoring Domain, you will be navigated to the OpenStack Fabric Launch Configuration page. In the same **OpenStack Fabric Launch Configuration** page, you can configure the following fabric components:

- Configure G-vTAP Controller
- Configure GigaVUE V Series Proxy
- Configure GigaVUE V Series Node

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

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

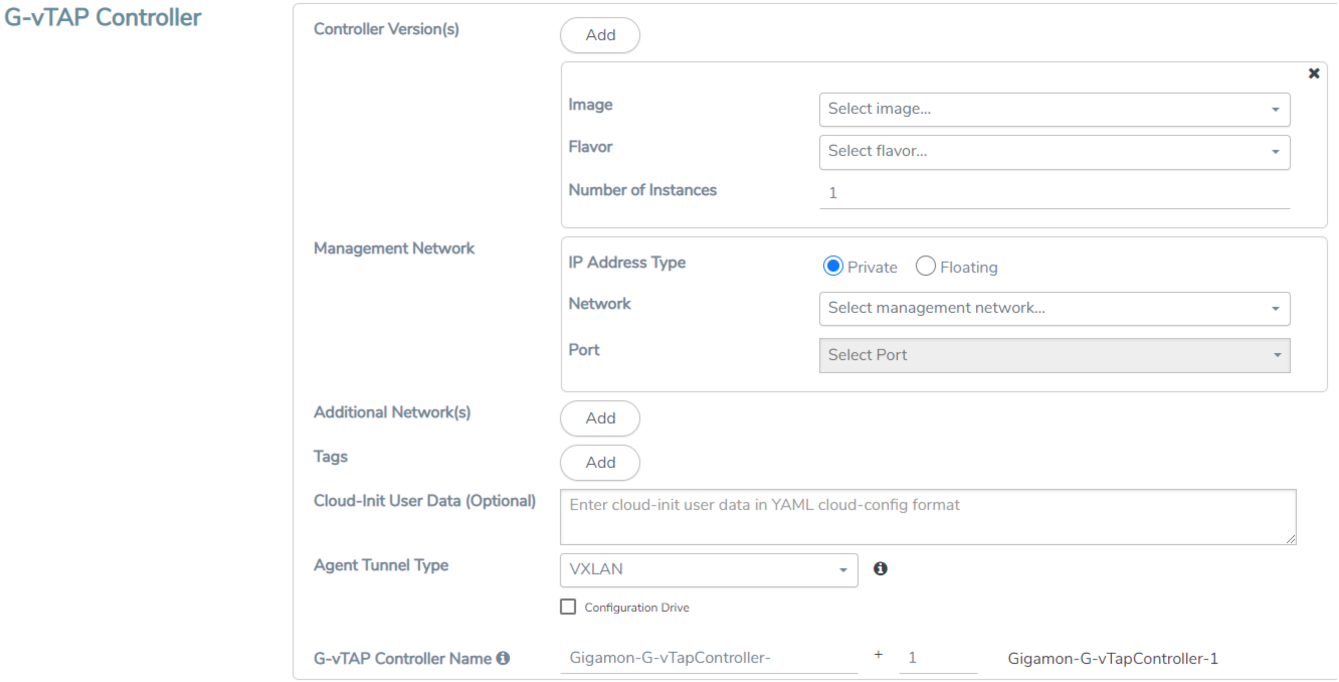
Select **Yes** to configure a GigaVUE V Series Proxy.



SSH Key Pair	Select SSH Key Pair...
Availability Zone	Select Availability Zone...
Security Groups	Select management subnet security group...
Configure a V Series Proxy	No

Configure G-vTAP Controller

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



G-vTAP Controller

Controller Version(s): Add
- Image: Select image...
- Flavor: Select flavor...
- Number of Instances: 1

Management Network:
- IP Address Type: ● Private ○ Floating
- Network: Select management network...
- Port: Select Port

Additional Network(s): Add

Tags: Add

Cloud-Init User Data (Optional): Enter cloud-init user data in YAML cloud-config format

Agent Tunnel Type: VXLAN

□ Configuration Drive

G-vTAP Controller Name: Gigamon-G-vTapController- + 1 Gigamon-G-vTapController-1

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

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

Fields	Description
Controller Version(s)	The G-vTAP Controller version that you configure must always have the same version number as the G-vTAP Agents deployed in the instances. For more detailed information refer GigaVUE-FM Version Compatibility Matrix. 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 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** drop-down list, select a size for the G-vTAP Controller. d. In **Number of Instances**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.
Management Network	This segment defines the management network that GigaVUE-FM uses to communicate with G-vTAP Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes. **Network** - Select the management network ID. **Ports** - Select a port, you can choose a port related to the selected management network ID. **IP Address Type** The type of IP address GigaVUE-FM needs to communicate with G-vTAP controllers: o **Private**—A private IP can be used when GigaVUE-FM, the G-vTAP Controller, or the GigaVUE V Series Proxy reside inside the same project. o **Floating**—A floating IP is needed only if GigaVUE-FM is not in the same project in the cloud or is outside the cloud. GigaVUE-FM needs a floating IP to communicate with the controllers from an external network.
Additional Network(s)	(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 **Add** to specify additional networks (subnets), if needed. Also, make sure that you specify a list of security groups for each additional

Fields	Description
	network. **Ports**: Select a port associated with the network.
Tag(s)	(Optional) The key name and value that helps to identify the G-vTAP Controller instances in your environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-gvtap-controllers. There is a specific GvTAP Controller Version for OVS Mirroring and OVS Mirroring + DPDK. To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-gvtap-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Agent Tunnel Type	The type of tunnel used for sending the traffic from G-vTAP Agents to GigaVUE V Series nodes. The options are GRE or VXLAN tunnels.
G-vTAP Controller Name	(Optional) Enter the name of the G-vTAP Controller. The G-vTAP Controller name must meet the following criteria: o The entire name can be a minimum of 1 to a maximum of 128 characters. o The suffix must only be a numeral and it should range between 0 to 999999999. o When deploying multiple G-vTAP Controllers, the suffix of the consecutive G-vTAP Controller name is updated successively. E.g., 000, 001, 002, 003, etc..

Configure GigaVUE V Series Proxy

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

Configure GigaVUE V Series Node

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

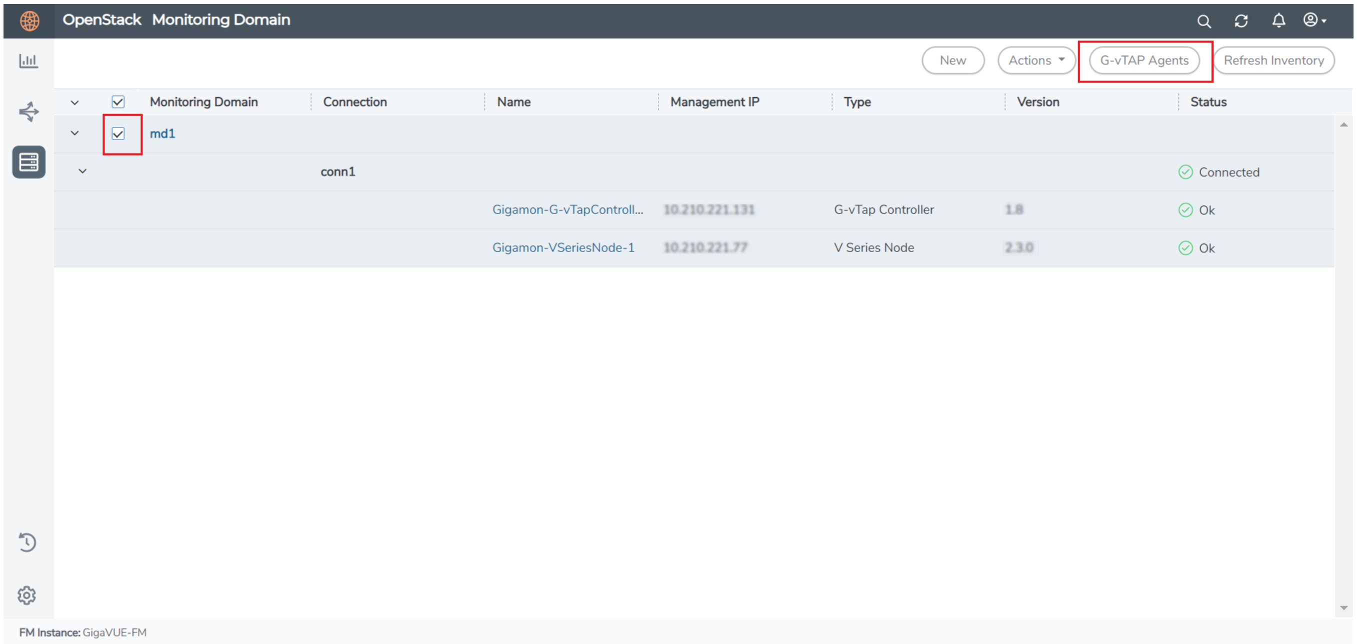
Parameter	Description
Image	Select the GigaVUE V Series node image file.
Flavor	Select the form of the GigaVUE V Series node.
Management Network	For the GigaVUE V Series Node, the Management Network is what is used by the GigaVUE V Series Proxy to communicate with the GigaVUE V Series Nodes. Select the management network ID. **Ports**— Select a port, you can choose a port related to the selected management network ID. NOTE: When both IPv4 and IPv6 addresses are available, IPv6 address is preferred, however if IPv6 address is not reachable then IPv4 address is used.
Data Network	Click **Add** to add additional networks. This is the network that the GigVUE V Series node uses to communicate with the monitoring tools. Multiple networks are supported. • **Tool Subnet**—Select a tool subnet, this is the default subnet that the GigaVUE-FM use to egress traffic to your tools. This subnet must have proper connectivity to your endpoint. • **IP Address Type** ◦ **Private**—A private IP can be used when GigaVUE-FM, the G-vTAP Controller, or the GigaVUE V Series Proxy, or the GigaVUE V Series node 2 reside inside the same project. ◦ **Floating**—A floating IP address specified here will be where V Series node 2x.x can be directly managed by GigaVUE-FM or can optionally managed by controllers. • **Network 1**—Select a network type. • **Ports** —Select a port associated with the network. • 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. • A network provider that is able to receive the monitored traffic may also be used here for OVS Mirroring and OVS Mirroring + DPDK. In this case, you would not need to provide a floating IP; but could select "private" and choose the provider network.
Tag(s)	(Optional) The key name and value that helps to identify the G-vTAP Controller instances in your environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2-gvtap-controllers.

Parameter	Description
	To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-gvtap-controllers.
Cloud-Init User Data (Optional)	Enter the cloud-init user data in cloud-config format.
Min Instances	The minimum number of GigaVUE V Series nodes to be launched in OpenStack. The minimum number can be 1. ● When you deploy an OVS Mirroring or OVS Mirroring + DPDK monitoring session, the V Series nodes will automatically be deployed based on the # of hypervisors being monitored. ● When you deploy a G-vTAP based monitoring session, the V Series nodes will automatically be deployed based on the # of VMs being monitored and the instance per V Series node ratio defined in the OpenStack Setttings page. NOTE: GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances	The maximum number of GigaVUE V Series nodes that can be launched in OpenStack. NOTE: Max Instances is applicable only for V Series node 1 works with G-vTAP connections and OVS mirroring.
V Series Node Name	(Optional) Enter the name of the V Series Node. The V Series Node name must meet the following criteria: o The entire name can be a minimum of 1 to a maximum of 128 characters. o The suffix must only be a numeral and it should range between 0 to 999999999. o When deploying multiple V Series Nodes, the suffix of the consecutive V Series Node name is updated successively. E.g., 000, 001, 002, 003, etc..
Tunnel MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is applied on the outgoing tunnel endpoints of the GigaVUE-FM V Series node when a monitoring session is deployed. The default value is 1450. The value must be 42 bytes less than the default MTU for GRE tunneling, or 50 bytes less than default MTU for VXLAN tunnels.

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

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

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



☑ Monitoring Domain	Connection	Name	Management IP	Type	Version	Status
☑ md1						
	conn1					✓ Connected
		Gigamon-G-vTapControll...	10.210.221.131	G-vTap Controller	1.8	✓ Ok
		Gigamon-VSeriesNode-1	10.210.221.77	V Series Node	2.3.0	✓ Ok

FM Instance: GigaVUE-FM

Configure GigaVUE Fabric Components in OpenStack

You can use your own OpenStack orchestration system to deploy GigaVUE fabric nodes and use GigaVUE-FM to configure the advanced features supported by these nodes. These nodes register themselves with GigaVUE-FM using the information provided by your OpenStack orchestration system. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM. Health status of the registered nodes are determined by the heartbeat messages sent from the respective nodes.

> **NOTE:** Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms. Refer to Linux G-vTAP Agent Installation and Windows G-vTAP Agent Installation for detailed information.

In your OpenStack dashboard, you can configure the following GigaVUE fabric components:

- Configure V Series Nodes and Proxy in OpenStack
- Configure G-vTAP Controller in OpenStack
- Configure G-vTAP Agent in OpenStack

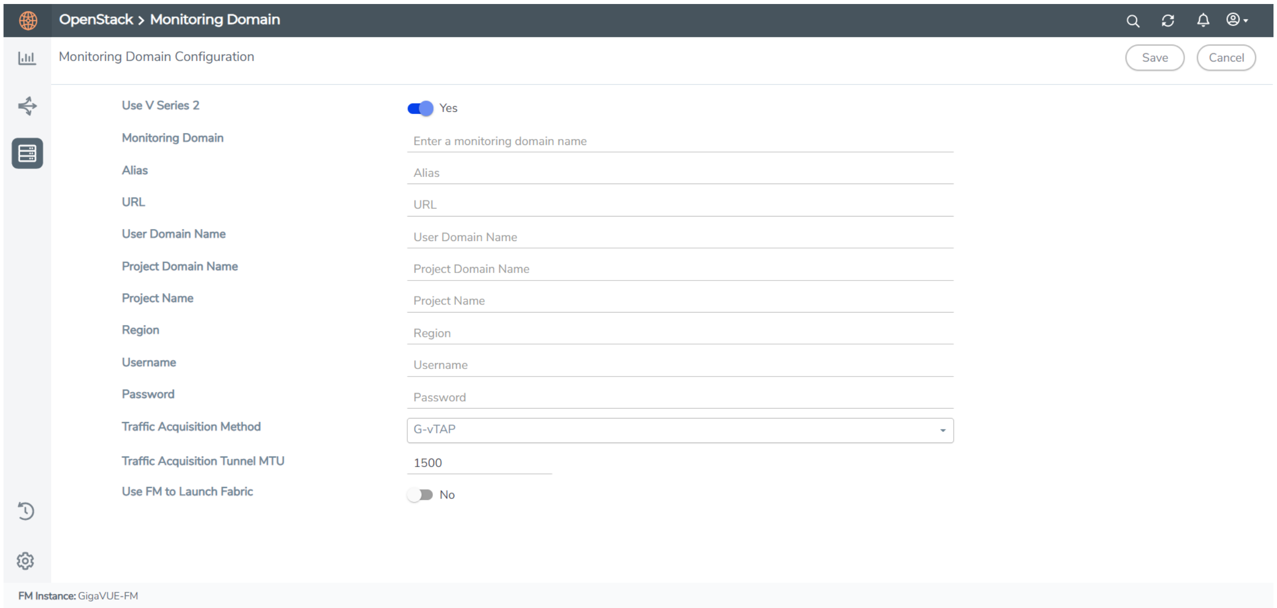
Configure V Series Nodes and Proxy in OpenStack

To configure V Series Nodes and V Series Proxy in OpenStack platform:

1. Before configuring GigaVUE fabric components through OpenStack, you must create a monitoring domain in GigaVUE-FM. Refer to Create Monitoring Domain for detailed instructions.

   > **NOTE:** You can use OpenStack Orchestrator for GigaVUE fabric node configuration only using V Series 2 nodes.

2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in OpenStack Orchestrator.



Monitoring Domain Configuration

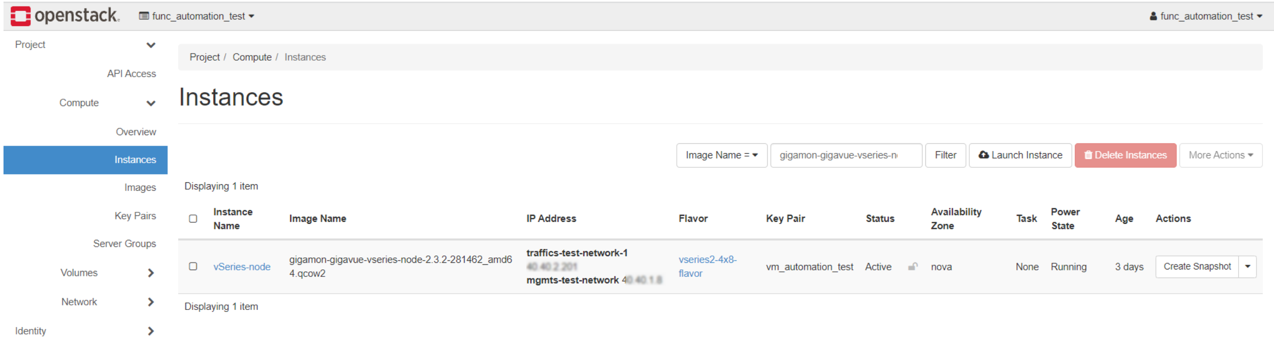
Use V Series 2	Yes
Monitoring Domain	Enter a monitoring domain name
Alias	Alias
URL	URL
User Domain Name	User Domain Name
Project Domain Name	Project Domain Name
Project Name	Project Name
Region	Region
Username	Username
Password	Password
Traffic Acquisition Method	G-vTAP
Traffic Acquisition Tunnel MTU	1500
Use FM to Launch Fabric	No

3. In your OpenStack environment, you can deploy V Series nodes or V Series proxy using the following methods:
   - Register V Series Nodes or V Series Proxy using OpenStack GUI
   - Register V Series Node or V Series Proxy using a configuration file

Register V Series Nodes or V Series Proxy using OpenStack GUI

To register V Series nodes or proxy using the user data in OpenStack GUI:

1. On the Instance page of OpenStack dashboard, click **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.



Instances

Displaying 1 item

□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	vSeries-node	gigamon-gigavue-vseries-node-2.3.2-281462_amd64.qcow2	traffics-test-network-1 [redacted] mgmts-test-network [redacted]	vseries2-4x8-flavor	vm_automation_test	Active	nova	None	Running	3 days	Create Snapshot

Displaying 1 item

2. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The V Series nodes or V Series proxy uses this customization script to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
 - path: /etc/gigamon-cloud.conf
 owner: root:root
 permissions: '0644'
 content:
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: orchestration
        password: orchestration123A!
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

- You can register your V Series node directly with GigaVUE-FM or you can use V Series proxy to register your V Series node with GigaVUE-FM. If you wish to register V Series node directly, enter the `remotePort` value as 443 or if you wish to deploy V Series node using V Series proxy then, enter the `remotePort` value as 8891.
- Use only the default `user` and `password` details given in the user data.
- If there is no monitoring domain in GigaVUE-FM with the same monitoring domain name and connection name as given in your user data, then GigaVUE-FM automatically creates a monitoring domain under AnyCloud and your V Series nodes or proxys gets deployed under that monitoring domain.
- In this case, the Traffic Acquisition Tunnel MTU is set to the default value 1500. to edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** and click Save.

Register V Series Node or V Series Proxy using a configuration file

To register V Series node or proxy using a configuration file:

1. Log in to the V Series node or proxy.
2. Edit the local configuration file (/etc/gigamon-cloud.conf) and enter the following customization script.

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: orchestration
        password: orchestration123A!
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

> **NOTE:** If you wish to register V Series node using V Series proxy then, enter the `remotePort` value as 8891.

3. Restart the V Series node or proxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps stop
     ```

   The deployed V Series node or V Series proxy registers with the GigaVUE-FM. After successful registration the V Series node or proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing ,the fabric node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the V Series node or proxy and if that fails as well then GigaVUE-FM unregisters the V Series node or proxy and it will be removed from GigaVUE-FM.

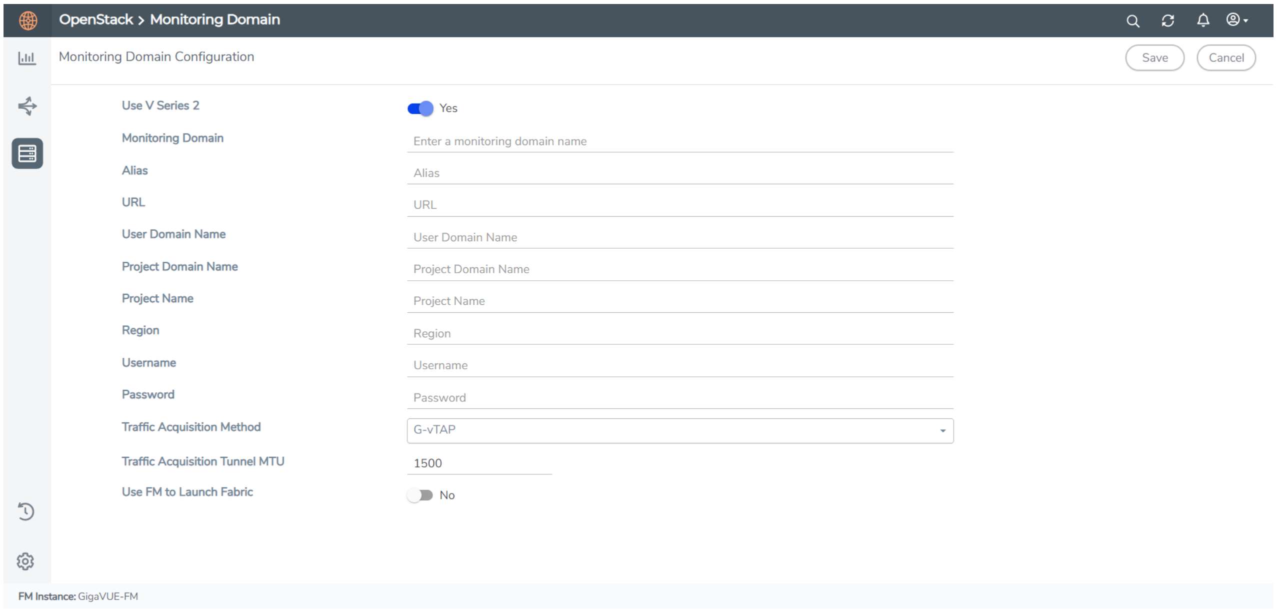
Configure G-vTAP Controller in OpenStack

To configure GigaVUE fabric components in OpenStack platform:

1. Before configuring GigaVUE fabric components through OpenStack, you must create a monitoring domain in GigaVUE-FM. While creating the monitoring domain, select **G-vTAP** as the Traffic Acquisition Method. Refer to Create Monitoring Domain for detailed instructions.

> **NOTE:** You can use OpenStack Orchestrator for GigaVUE fabric node configuration only using V Series 2 nodes.

2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in OpenStack Dashboard.



Monitoring Domain Configuration

Use V Series 2	Yes
Monitoring Domain	Enter a monitoring domain name
Alias	Alias
URL	URL
User Domain Name	User Domain Name
Project Domain Name	Project Domain Name
Project Name	Project Name
Region	Region
Username	Username
Password	Password
Traffic Acquisition Method	G-vTAP
Traffic Acquisition Tunnel MTU	1500
Use FM to Launch Fabric	No

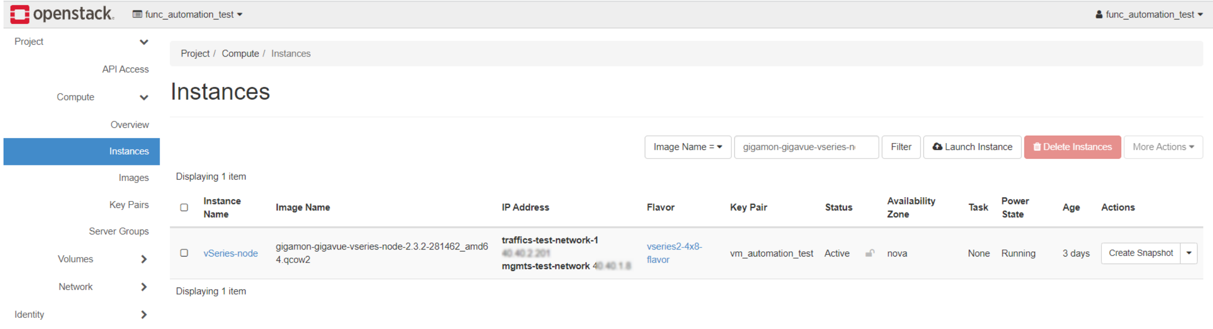
FM Instance: GigaVUE-FM

3. In your OpenStack environment, launch the G-vTAP Controller using any of the following methods:
   - Register G-vTAP Controller using OpenStack GUI
   - Register G-vTAP Controller using a configuration file

Register G-vTAP Controller using OpenStack GUI

To register G-vTAP Controller using the user data in OpenStack GUI:

a. On the Instance page of OpenStack dashboard, click **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.



Displaying 1 item

□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status		Availability Zone	Task	Power State	Age	Actions
□	vSeries-node	gigamon-gigavue-vseries-node-2.3.2-281462_amd64.qcow2	traffics-test-network-1 [redacted] mgmts-test-network [redacted]	vseries2-4x8-flavor	vm_automation_test	Active		nova	None	Running	3 days	Create Snapshot

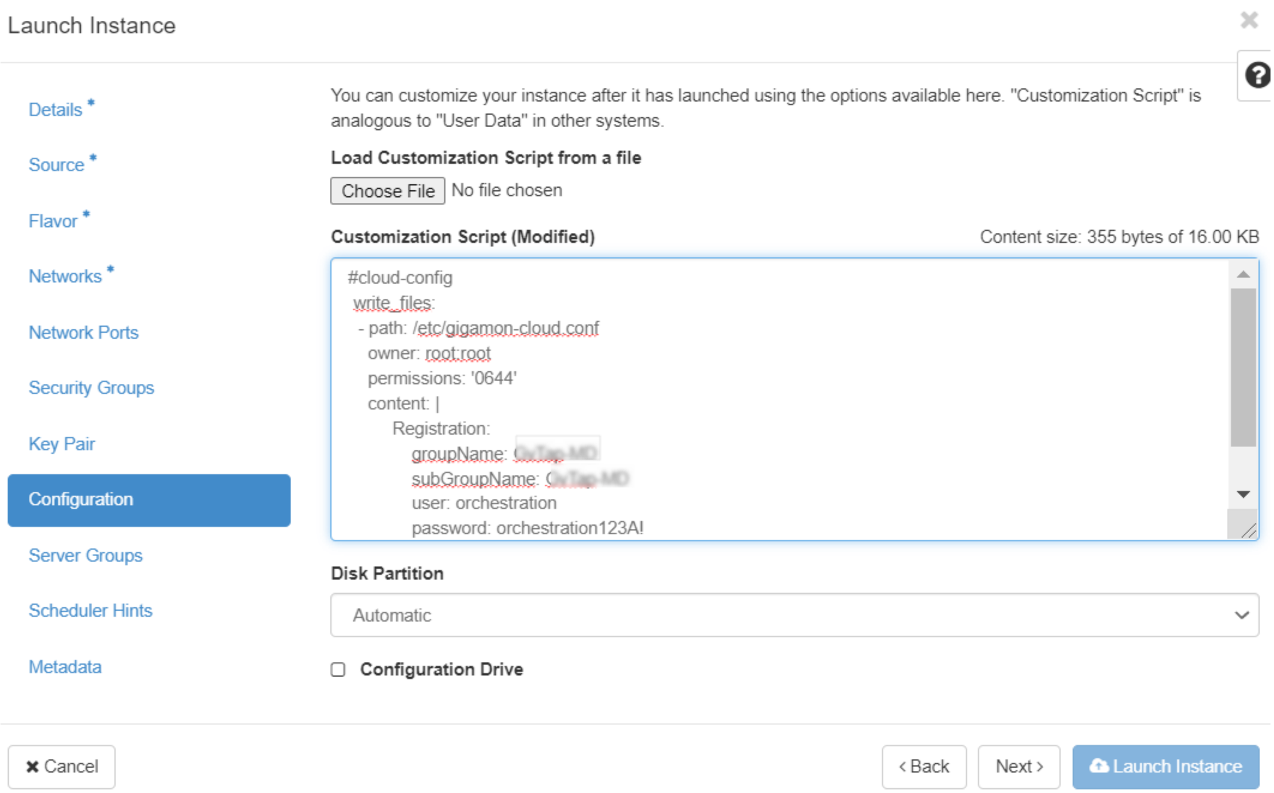
Displaying 1 item

b. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The G-vTAP Controller uses this customization script to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
 - path: /etc/gigamon-cloud.conf
 owner: root:root
 permissions: '0644'
 content:
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: orchestration
        password: orchestration123A!
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

> - Use only the default `user` and `password` details given in the user data.
> - If there is no monitoring domain in GigaVUE-FM with the same monitoring domain name and connection name as given in your user data, then GigaVUE-FM automatically creates a monitoring domain under AnyCloud and your V Series nodes or proxys gets deployed under that monitoring domain.

- In this case, the Traffic Acquisition Tunnel MTU is set to the default value 1500. to edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** and click Save.



You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Load Customization Script from a file

Choose File No file chosen

Customization Script (Modified) Content size: 355 bytes of 16.00 KB

```
#cloud-config
 write_files:
  - path: /etc/gigamon-cloud.conf
    owner: root:root
    permissions: '0644'
    content: |
        Registration:
          groupName: [redacted]
          subGroupName: [redacted]
          user: orchestration
          password: orchestration123A!
```

Disk Partition

Automatic

□ **Configuration Drive**

The G-vTAP Controller deployed in OpenStack appears on the Monitoring Domain page of GigaVUE-FM.

Register G-vTAP Controller using a configuration file

To register G-vTAP Controller using a configuration file:

a. Log in to the G-vTAP Controller.

b. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: orchestration
        password: orchestration123A!
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

c. Restart the G-vTAP Controller service.

```
$ sudo service gvtap-cntlr restart
```

The deployed G-vTAP Controller registers with the GigaVUE-FM. After successful registration the G-vTAP Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing ,the fabric node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the G-vTAP Controller and if that fails as well then GigaVUE-FM unregisters the G-vTAP Controller and it will be removed from GigaVUE-FM.

NOTE: When you deploy V Series nodes or G-vTAP Controllers using 3rd party orchestration, you cannot delete the monitoring domain without unregistering the V Series nodes or G-vTAP Controllers.

Configure G-vTAP Agent in OpenStack

G-vTAP Agent should be registered via the registered G-vTAP Controller and communicates through PORT 8891.

Deployment of G-vTAP Agents through third-party orchestrator is supported on Linux and Windows platforms.

To register G-vTAP Agent using a configuration file:

1. Install the G-vTAP Agent in the Linux or Windows platform. For detailed instructions, refer to Linux G-vTAP Agent Installation and Windows G-vTAP Agent Installation.
2. Log in to the G-vTAP Agent.
3. Edit the local configuration file and enter the following user data.

   - /etc/gigamon-cloud.conf is the local configuration file in Linux platform.
   - C:\ProgramData\gvtap-agent\gigamon-cloud.conf is the local configuration file in Windows platform.

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: orchestration
        password: orchestration123A!
        remoteIP: <IP address of the G-vTAP Controller 1>,
                  <IP address of the G-vTAP Controller 2>
        remotePort: 8891
```

   NOTE: Use only the default **user** and **password** details given in the user data.

4. Restart the G-vTAP Agent service.
   - Linux platform:
     ```
     $ sudo service gvtap-agent restart
     ```
   - Windows platform: Restart from the Task Manager.

NOTE: You can configure more than one G-vTAP Controller for a G-vTAP Agent, so that if one G-vTAP Controller goes down, the G-vTAP Agent registration will happen through another Controller that is active.

The deployed G-vTAP Agent registers with the GigaVUE-FM through the G-vTAP Controller. After successful registration the G-vTAP Agent sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, G-vTAP Agent status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the G-vTAP Agent and if that fails as well then GigaVUE-FM unregisters the G-vTAP Agent and it will be removed from GigaVUE-FM.

Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnel, maps, applications in a monitoring session to receive and send traffic to the GigaVUE V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools.

Refer to the following sections for details:

- Create a Monitoring Session
- Create Ingress and Egress Tunnels
- Create a New Map
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics
- Visualize the Network Topology

Create a Monitoring Session

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

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

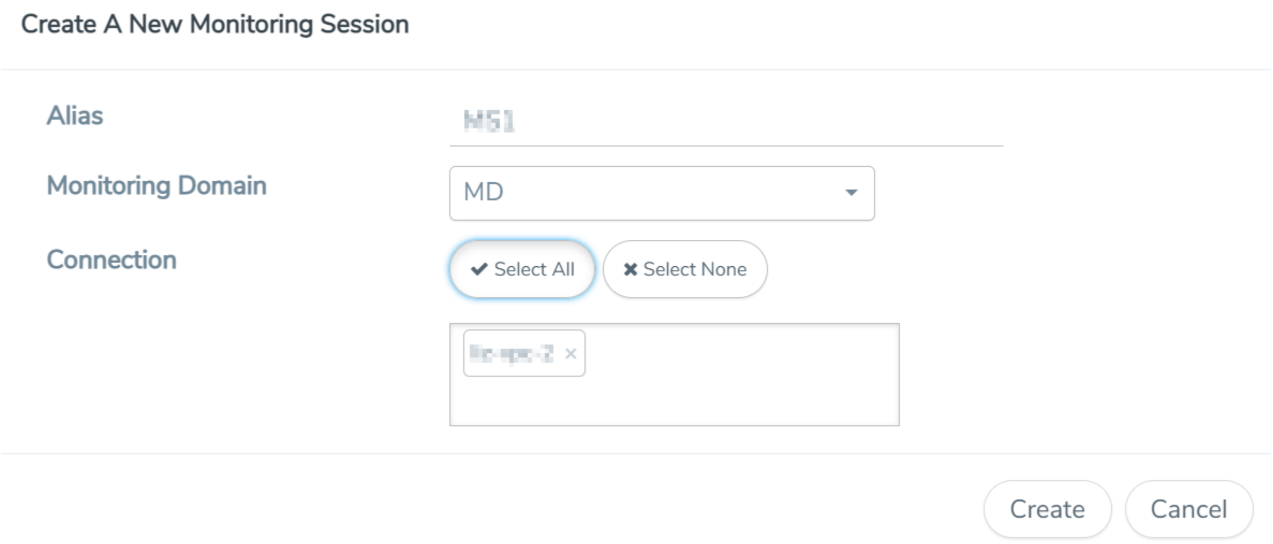
For the connections without G-vTAPs there is no targets that are automatically selected. You can use Tunnel as a Source in the monitoring session to accept a tunnel from anywhere.

You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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



Create A New Monitoring Session

Alias: [redacted]

Monitoring Domain: MD

Connection: [redacted]

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

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

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

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

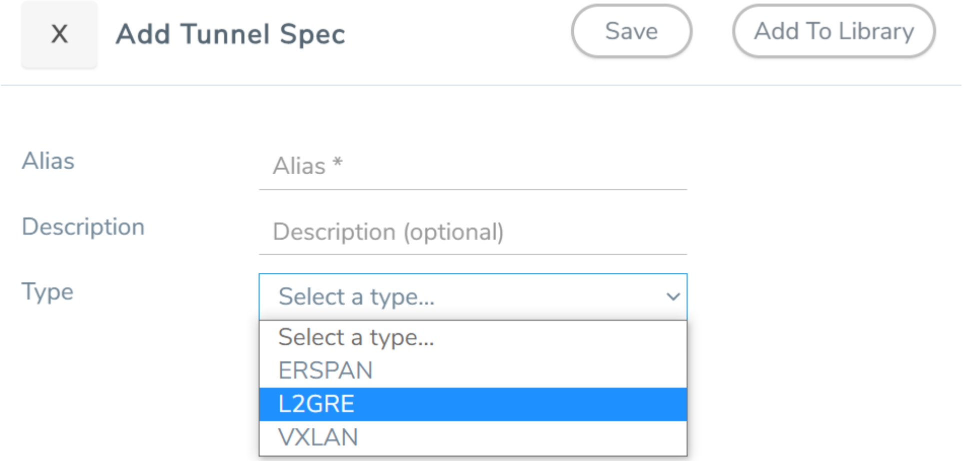
Create Ingress and Egress Tunnels

Traffic from the V Series node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel.

> **NOTE:** ERSPAN is not supported for AWS solution.

To create a new tunnel endpoint:

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



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

Field	Description
Alias	The name of the tunnel endpoint. NOTE: Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Type	The type of the tunnel. Select ERSPAN, or L2GRE, or VXLAN to create a tunnel.
Traffic Direction	The direction of the traffic flowing through the V Series node. • Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node. Enter values for the Key. • Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key. • ERSPAN, L2GRE, and VXLAN are the supported **Ingress tunnel** types. You can configure Tunnel Endpoint as your first level entity in Monitoring Session. • L2GRE and VXLAN are the supported **Egress tunnel** types.
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
Remote Tunnel IP	For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.

4. Click **Save**.

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

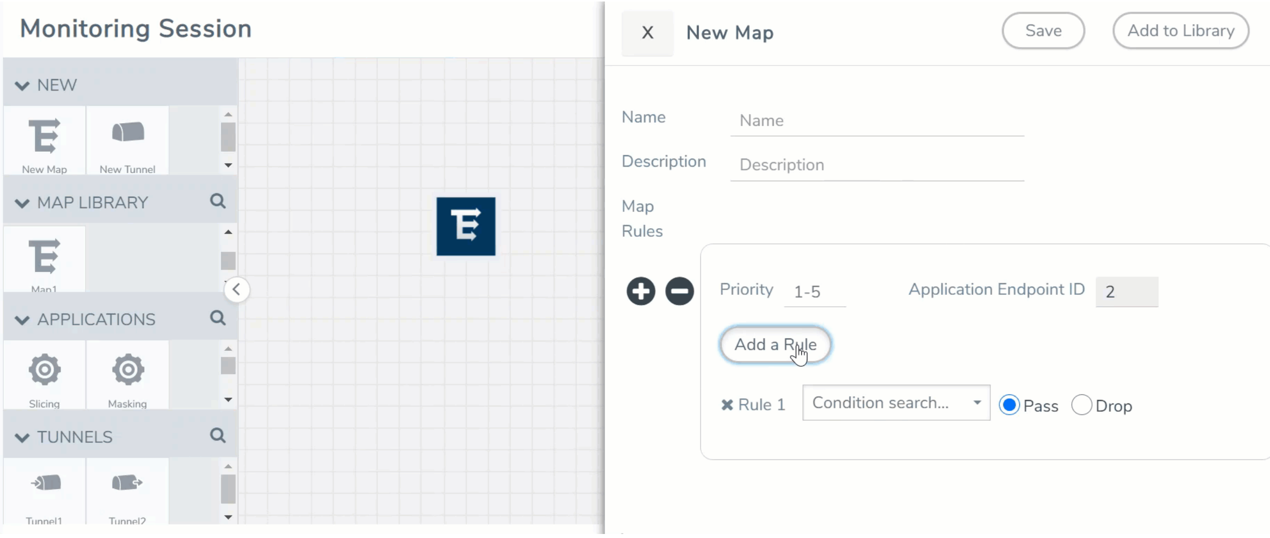
Create a New Map

You must have the flow map license to deploy a map in monitoring session.

For new users, the free trial bundle will expire after 30 days and the GigaVUE-FM prompts you to buy a new license. For detailed information on GigaVUE-FM licenses, refer to "Licenses" section in the *GigaVUE Administration Guide*.

To create a new map:

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



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

Field	Description
Name	Name of the new map
Description	Description of the map
Map Rules	The rules for filtering the traffic in the map. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add multiple rule sets on a map. Use the **+** and **-** buttons to add or remove a rule set in the map. A rule set can have maximum of 25 rules. To add a map rule: a. Enter a **Priority** value from 1 to 5 for the rule with 5 being the highest and 1 is the lowest priority. b. Click **Add a Rule**. The new rule field appear for the Application Endpoint. c. Select a required condition from the drop-down list. d. Select the rule to **Pass** or **Drop** through the map. If two rules with same condition are configured as pass and drop, • on a same tunnel endpoint, the traffic filtering precedence will be based on the priority value. • on two different tunnel endpoints, the traffic will be passed or dropped to the respective tunnel endpoints. For detailed information on filtering fragmented and unfragmented packets, refer to "GigaSMART Adaptive Packet Filtering (APF)" section on the *GigaVUE Fabric Management Guide*.

Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:

- Traffic Map—Only Pass rules for ATS
- Inclusion Map—Only Pass rules for ATS
- Exclusion Map—Only Drop rules for ATS

4. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
   a. Select an existing group from the **Select Group** list or create a **New Group** with a name.
   b. Enter a description in the **Description** field, and click **Save**.
5. Click **Save**.

NOTE: If a packet is fragmented then all the fragments will be destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. Refer to "Map Statistics" section in *GigaVUE Fabric Management Guide*for detailed information.

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

Add Applications to Monitoring Session

GigaVUE Cloud Suite with GigaVUE V Series 2 node supports the following GigaSMART applications in the GigaVUE-FM canvas:

- Slicing
- Masking
- Dedup
- Load Balancing
- PCAPng

You can also configure the following GigaSMART operations from the **Traffic > Solutions > Application Intelligence**:

- Application Metadata Intelligence
- Application Filtering Intelligence

For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

For the detailed list of GigaSMART Operation supported for V Series 2 nodes, refer to "Supported GigaSMART Operation" topic in the *GigaVUE Fabric Management Guide*.

You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools. Refer to the Volume Based License (VBL) section for more information on Licenses for using V Series 2 Nodes.

To add a GigaSMART application:

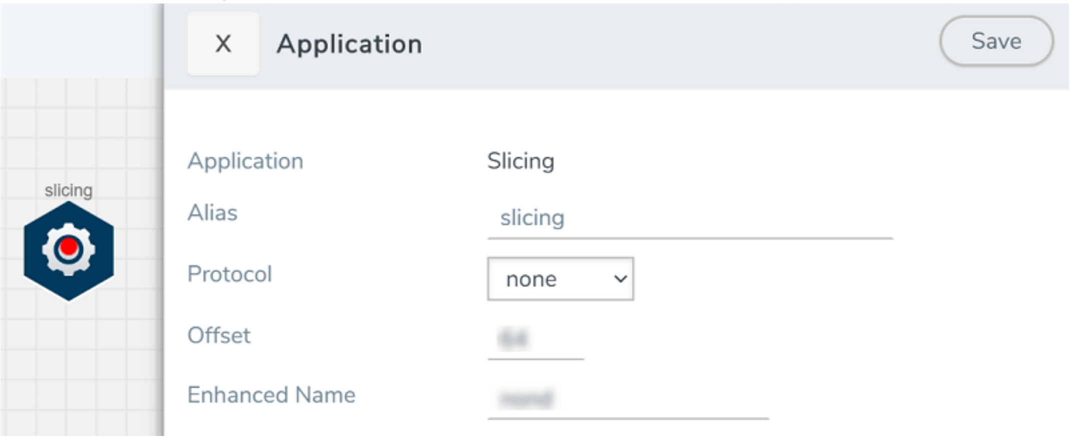
1. Drag and drop an application from **APPLICATIONS** to the canvas.
2. In the canvas, click the application and select **Details**.
3. Enter or select the required values for the selected application and click **Save**.

Slicing

Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. For detailed information on Slicing, refer to GigaSMART Packet Slicing "GigaSMART Packet Slicing" topic in the *GigaVUE Fabric Management Guide*.

To add a slicing application:

1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.
2. Click the Slicing application and select **Details**. The Application quick view appears.



Application: Slicing
Alias: slicing
Protocol: none
Offset: [illegible]
Enhanced Name: [illegible]

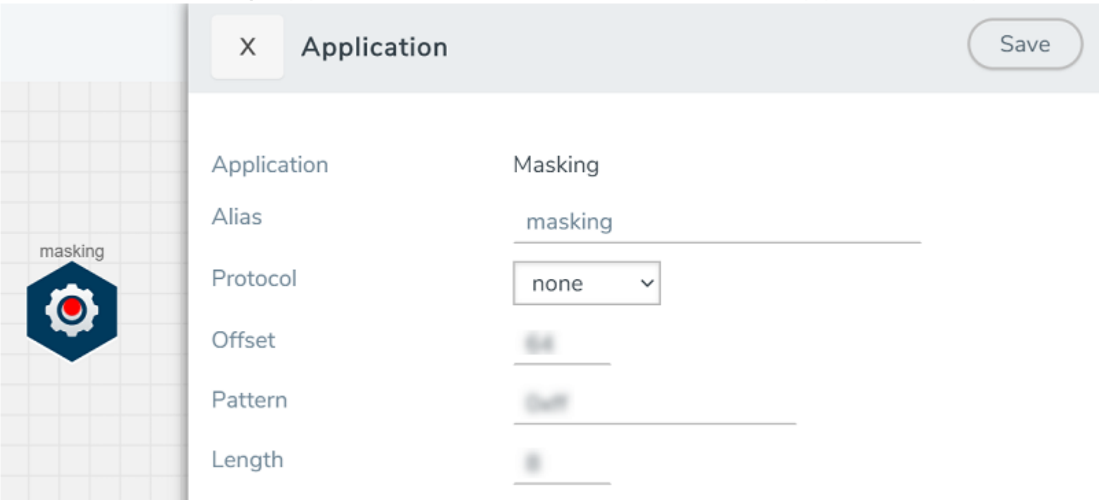
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the slicing.
   - From the **Protocol** drop-down list, specify an optional parameter for slicing the specified length of the protocol.
   - In the **Offset** field, specify the length of the packet that must be sliced.
   - In the **Enhanced Name** field, enter the Enhanced Slicing profile name.
4. Click **Save**.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. For detailed information on masking, refer to GigaSMART Masking"GigaSMART Masking" topic in the *GigaVUE Fabric Management Guide*.

To add a masking application:

1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.
2. Click the Masking application and select **Details**. The Application quick view appears.



Application

Application: Masking

Alias: masking

Protocol: none

Offset: 64

Pattern: 0xff

Length: 8

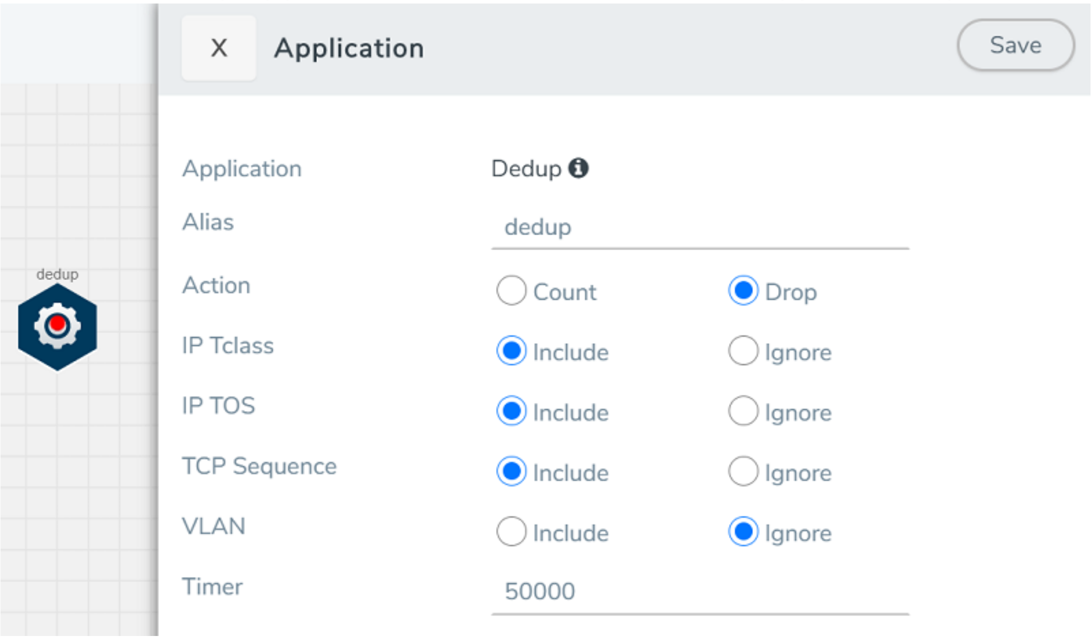
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the masking.
   - From the **Protocol** drop-down list, specify an optional parameter for masking the specified length of the protocol.
   - In the **Offset** field, specify the length of the packet that must be masked.
   - In the **Pattern** field, enter the pattern for masking the packet.
   - In the **Length** field, enter the length of the packet that must be masked.
4. Click **Save**.

Dedup

De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment. For detailed information on de-duplication, refer to GigaSMART De-Duplication"GigaSMART De-Duplication" topic in the *GigaVUE Fabric Management Guide*.

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.



Application	Dedup	
Alias	dedup	
Action	○ Count	● Drop
IP Tclass	● Include	○ Ignore
IP TOS	● Include	○ Ignore
TCP Sequence	● Include	○ Ignore
VLAN	○ Include	● Ignore
Timer	50000	

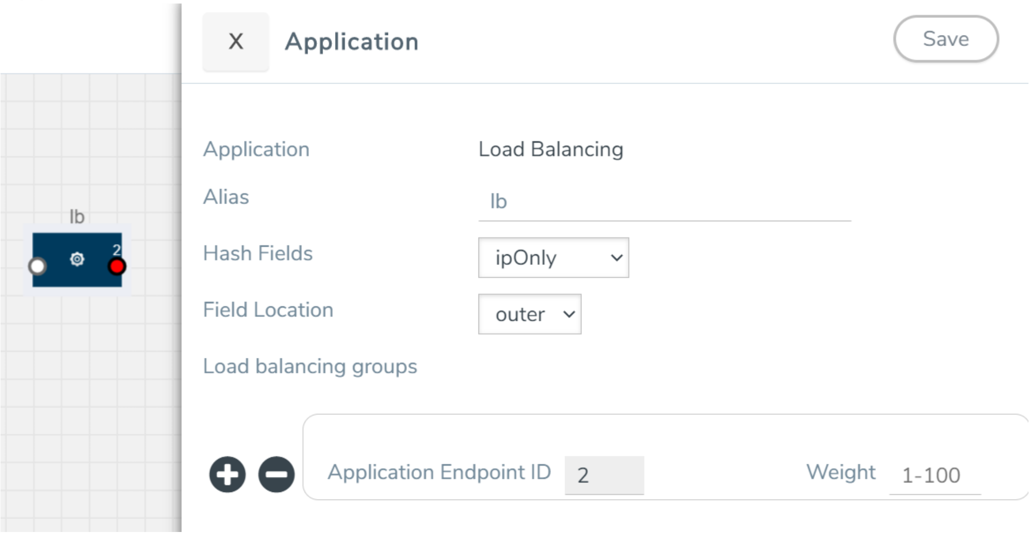
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the de-duplication.
   - In the Action field, select **Count** or **Drop** the detected duplicate packets.
   - For **IP Tclass**, **IP TOS**, **TCP Sequence**, and **VLAN** fields, select **Include** or **Exclude** the packets for de-duplication.
   - In the **Timer** field, enter the time interval (in seconds) for de-duplicating the packet.
4. Click **Save**.

Load Balancing

Load balancing app performs stateless distribution of the packets between different endpoints. For detailed information on load balancing, refer to GigaSMART Load Balancing "GigaSMART Load Balancing" topic in the *GigaVUE Fabric Management Guide*.

To add a load balancing application:

1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
2. Click the load balancing application and select **Details**. The Application quick view appears.



Application: Load Balancing

Alias: lb

Hash Fields: ipOnly

Field Location: outer

Load balancing groups

Application Endpoint ID: 2 — Weight: 1-100

3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the load balancing app.
   - For **Hash Fields** field, select a hash field from the list.
     - **ipOnly**—includes Source IP, and Destination IP.
     - **ipAndPort**—includes Source IP, Destination IP, Source Port , and Destination Ports.
     - **fiveTuple**—includes Source IP, Destination IP, Source Port, Destination Port, and Protocol fields.
     - **gtpuTeid**—includes GTP-U.
   - For **Field location** field, select **Inner** or **Outer** location.

     > NOTE: Field location is not supported for **gtpuTeid**.

   - In the **load balancing groups**, add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.
4. Click **Save**.

PCAPng

The PCAPng application is a GigaSMART parser application that reads the various blocks in the received PCAPng files and validates the blocks to be sent to the destination application or to the tools.

> **NOTE:** The PCAPng application is only applicable for the Ericsson 5G Core vTAP architecture. Refer to "PCAPng Application" topic in the *GigaVUE Fabric Management Guide* for detailed information.

Create Link Between UDP-in-GRE Tunnel and PCAPng Application

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description
Alias	The name of the tunnel endpoint **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint
Type	Select **UDPGRE** as the tunnel type
Traffic Direction	The direction of the traffic flowing through the V Series node • Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6
Remote Tunnel IP	The IP address of the tunnel source
Key	GRE key value
Source L4 Port	Layer 4 source port number
Destination L4 Port	Layer 4 destination port number. You can configure only 4754 or 4755 as the destination UDP ports

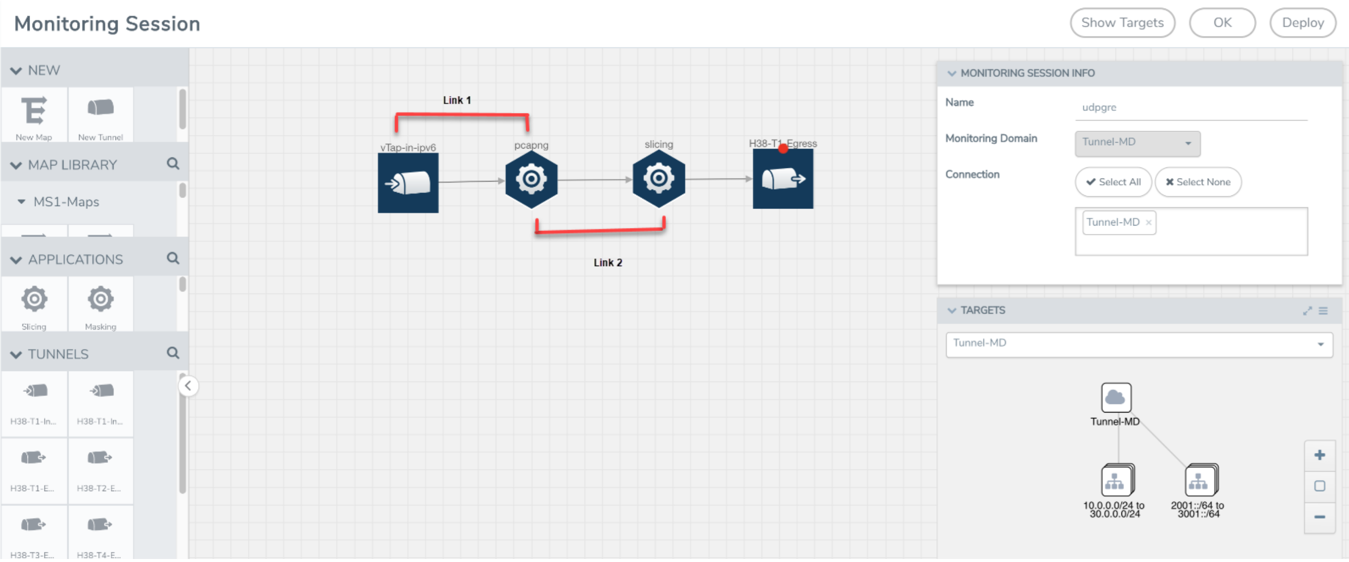
3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

Create a link with source as PCAPng application and destination as one of the following:

- Other GigaSMART applications such as Slicing, Masking, etc.
- Other encapsulation TEPs.
- REP/MAP

Refer to the following image for a sample configuration.



Name: udpgre

Monitoring Domain: Tunnel-MD

Connection: Tunnel-MD

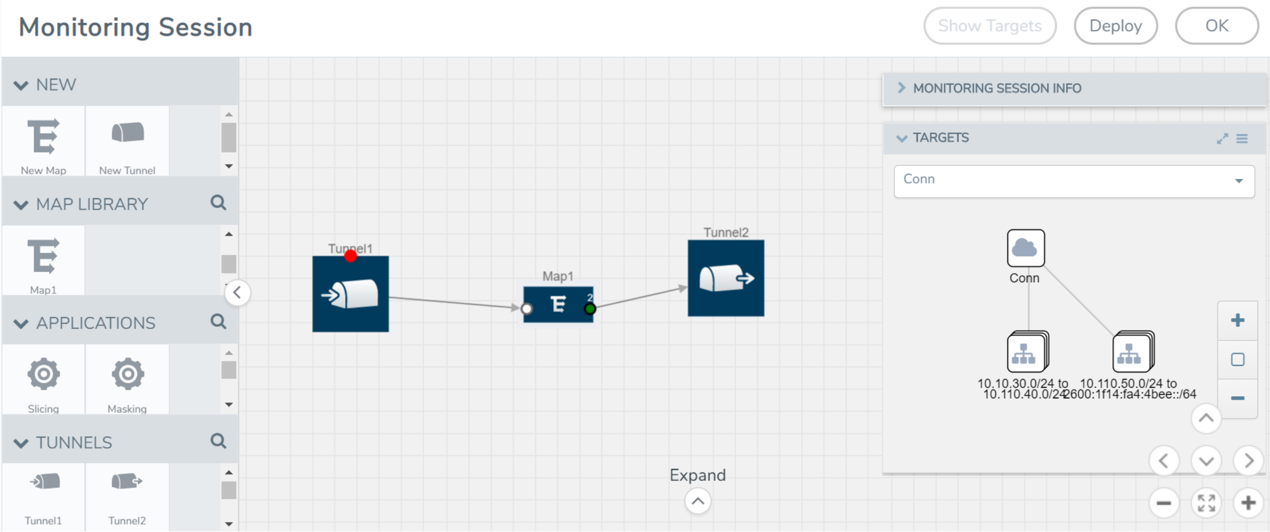
Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
   - Ingress tunnel (as a source) from the **NEW** section
   - Maps from the **MAP LIBRARY** section
   - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART apps from the **APPLICATIONS** section
   - Egress tunnels from the **TUNNELS** section

2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

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



3. (Not applicable for Tunnel traffic acquisition method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
4. 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 the V Series nodes. 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 V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.

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

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

The Monitoring Session page also has the following buttons:

Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected

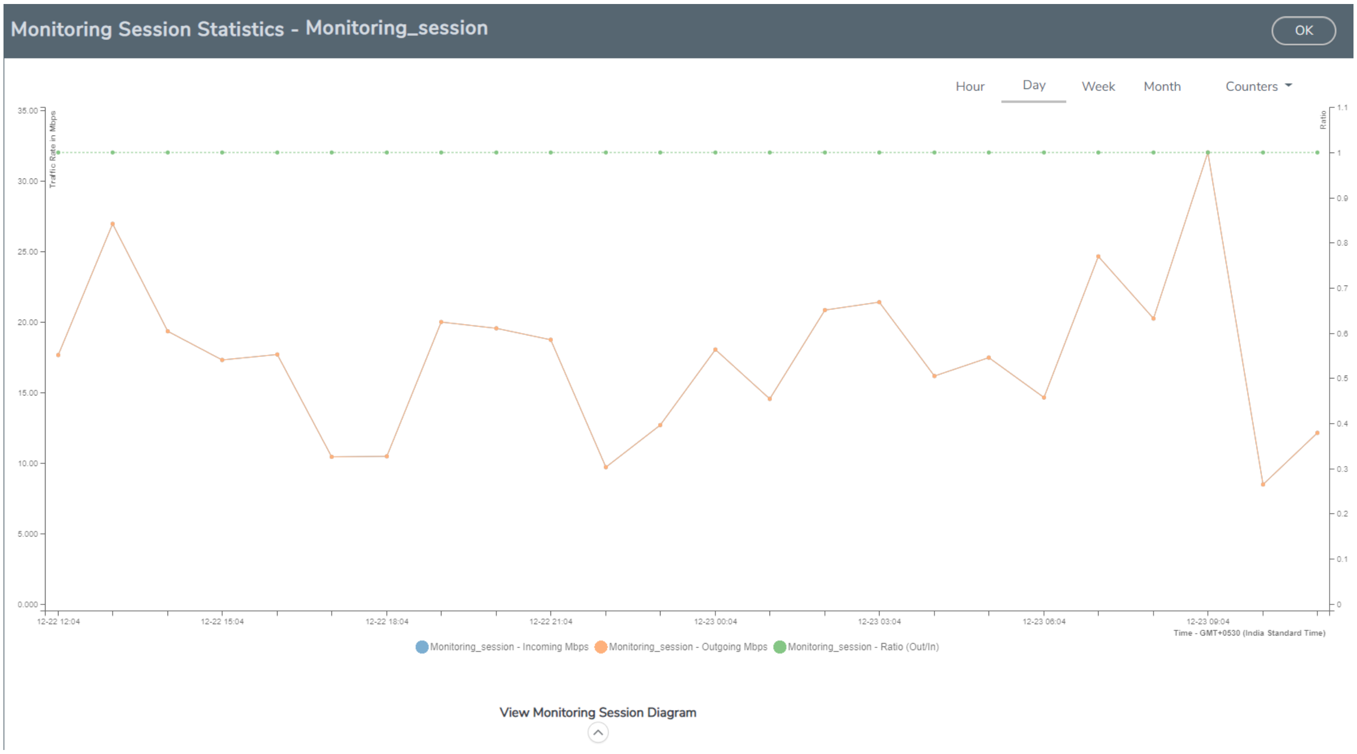
Button	Description
	monitoring session. NOTE: In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again..
Delete	Deletes the selected monitoring session.

View Monitoring Session Statistics

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

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

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


Monitoring Session Statistics - Monitoring_session

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

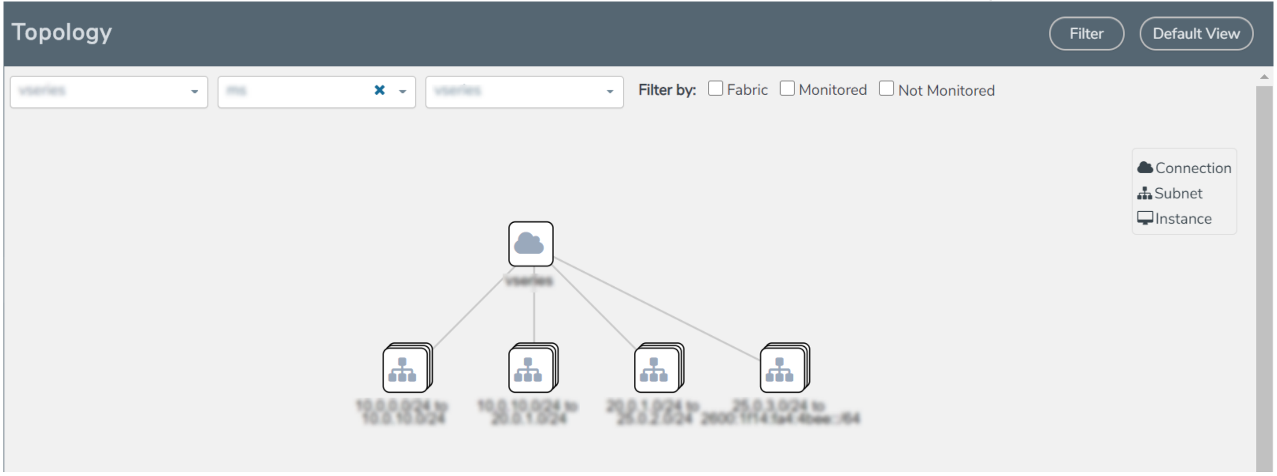
- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.
- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.
4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



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

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

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

Administer GigaVUE Cloud Suite for OpenStack

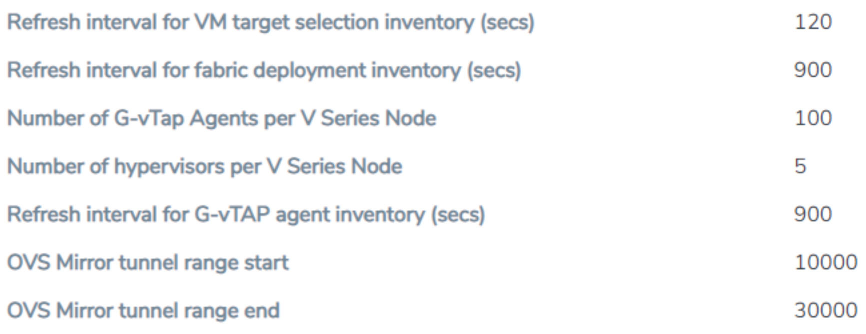
You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for OpenStack:

- Configure the OpenStack Settings
- Role Based Access Control
- About Audit Logs
- About Events

Configure the OpenStack Settings

To configure the OpenStack Settings:

1. From the left navigation pane, select **Inventory > VIRTUAL > OpenStack > Settings**. The Settings page appears.
2. In the OpenStack Settings page, select **Advanced** tab.
3. Click **Edit** to edit the Advanced Settings fields.



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

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

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

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

Role Based Access Control

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

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

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

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

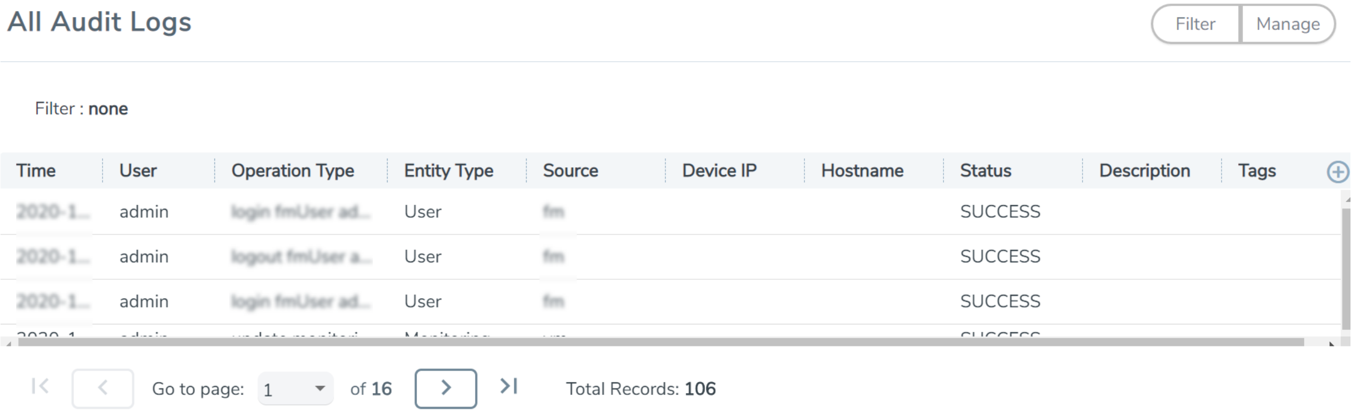
NOTE: Cloud APIs are also RBAC enabled.

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

About Audit Logs

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

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



All Audit Logs

Filter : **none**

Time	User	Operation Type	Entity Type	Source	Device IP	Hostname	Status	Description	Tags
[redacted]	admin	[redacted]	User	[redacted]			SUCCESS		
[redacted]	admin	[redacted]	User	[redacted]			SUCCESS		
[redacted]	admin	[redacted]	User	[redacted]			SUCCESS		

Go to page: 1 of **16**

Total Records: **106**

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

About Events

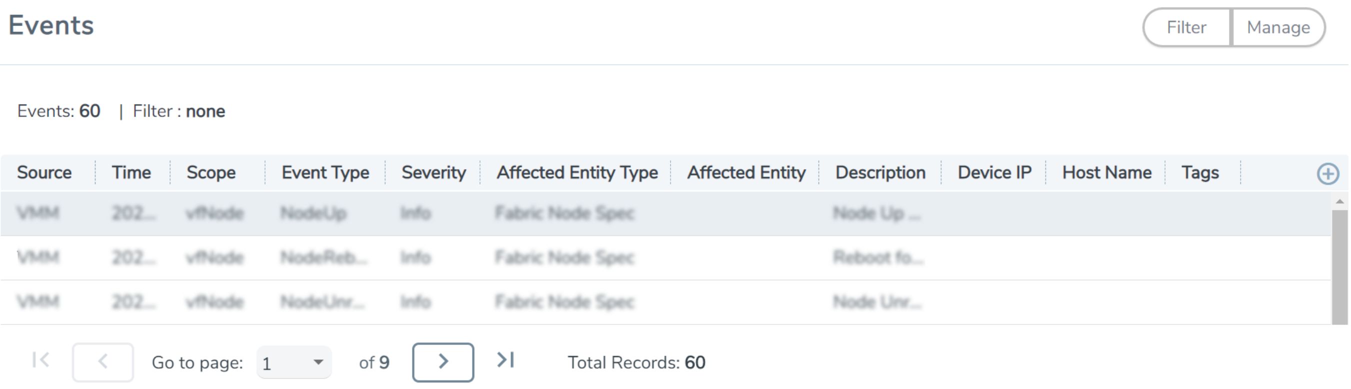
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- Cloud provider License Expiry
- G-vTAP Agent Inventory Update Completed
- Cloud provider Connection Status Changed

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. An example of alarm could be your cloud provider license expiry.

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

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



Events: **60** | Filter : **none**

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

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

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

To filter the alarms and event:

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

GigaVUE-FM Version Compatibility Matrix

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

GigaVUE-FM	G-vTAP Agent	G-vTAP OVS Agent	G-vTAP Controller	GigaVUE V Series Proxy	GigaVUE V Series 2 Node
5.16.00	v1.8-5	v1.8-2	v1.8-5	v2.6.0	v2.6.0
5.15.00	v1.8-5	v1.8-1	v1.8-5	v2.5.0	v2.5.0
5.14.00	v1.8-4	v1.8-1	v1.8-4	v2.4.0	v2.4.0
5.13.01	v1.8-3	v1.8-1	v1.8-3	v2.3.3	v2.3.3
5.13.00	v1.8-2	v1.8-0	v1.8-2	v2.3.0	v2.3.0
5.12.00	v1.7-1	v1	v1.7-1	v2.1.0	v2.1.0

Troubleshooting

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

OpenStack Connection Failed

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

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

Handshake Alert: unrecognized_name

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

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

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

GigaVUE V Series Node or G-vTAP Controller is Unreachable

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

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

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 5.16 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
G-TAP A Series 2 Installation Guide
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010

GigaVUE Cloud Suite 5.16 Hardware and Software Guides
GigaVUE-OS Installation Guide for DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
Administration
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
Fabric Management
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Configuration and Monitoring how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide
GigaVUE Cloud Suite for AnyCloud Guide
GigaVUE Cloud Suite for Kubernetes Guide
GigaVUE Cloud Suite for Nutanix Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
GigaVUE Cloud Suite for AWS Secret Regions Guide
Reference
GigaVUE-OS CLI Reference Guide

GigaVUE Cloud Suite 5.16 Hardware and Software Guides
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-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release NOTE: Release Notes are not included in the online documentation. NOTE: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The 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.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)