Gigamon®

V SERIES

GigaVUE Cloud Suite for AWS Configuration Guide

Version 5.7.00

COPYRIGHT

TRADEMARK ATTRIBUTIONS

DOCUMENT REVISION – 8/9/19

Contents

1 GigaVUE Cloud Suite for AWS

This guide describes how to configure GigaVUE Cloud Suite for AWS using the GigaVUE-FM interface. This guide also describes the procedure for setting up the traffic monitoring sessions for AWS using the GigaVUE-FM. For information about deploying the GigaVUE Cloud on the Amazon Web Services (AWS), refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.

License Information

GigaVUE Cloud is available in both the public AWS cloud and in AWS GovCloud, and supports the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG) model that you can avail from the AWS Marketplace.

Bring Your Own License (BYOL)

The AMI for the BYOL option can be purchased based on the number of TAP points and the term of the license. Gigamon offers the following options for purchasing the license:

- Traffic visibility for up to 100 virtual TAP points (ENIs)
- Traffic visibility for up to 1000 virtual TAP points (ENIs)

NOTE: Make sure you purchase a licensing option that can provide traffic visibility to all the TAP points in the VPC. If the licensing option cannot support all the TAP points, the ENIs are selected randomly for monitoring the traffic.

The minimum term for the license is 3 months.

A free trial is made available in the AWS Marketplace and in the Community AMIs. The trial version provides traffic visibility for up to 10 virtual TAP points for 30 days. When a new license is purchased, the 10 virtual TAP points are replaced with however many TAP points the licensing option supports.

For purchasing licenses with the BYOL option, contact our Gigamon Sales. Refer to *Contacting Sales* on page 103.

Pay-As-You-Go (PAYG)

The AMI for the Pay-As-You-Go (PAYG) option is available in the AWS Marketplace. The hourly PAYG option charges the users for the AWS services availed on an hourly basis. For example, AWS charges the users for the period the GigaVUE-FM instance is running in the EC2 instances. When the instance stops, AWS stops charging the users. The PAYG model has no term contract.

It is a perpetual license that supports up to 100 TAP points. To support additional TAP points, a new license must be purchased from Gigamon.

NOTE: While upgrading GigaVUE-FM, make sure you choose the AMI with the same licensing option as the current AMI. For example, assume that a user has purchased GFM-AWS-100 license with hourly pricing. While upgrading GigaVUE-FM, the user must select the AMI with the same GFM-AWS-100 license associated. Else, there could be discrepancy in the number of instances monitored.

For purchasing licenses with the PAYG option, contact the Gigamon Sales. Refer to *Contacting Sales* on page 103.

Apply Licensing

For instructions on how to generate and apply license refer to the *GigaVUE-OS and GigaVUE-FM Administration Guide*.

Install and Upgrade GigaVUE Fabric Manager

You can install and upgrade the GigaVUE® Fabric Manager (GigaVUE-FM) on cloud or on-premises.

- Cloud—To install and upgrade GigaVUE-FM inside your AWS environment, you can simply launch the GigaVUE-FM instance in your VPC. For installing the GigaVUE-FM instance, . For upgrading the GigaVUE-FM instance, refer to *Upgrade GigaVUE-FM in AWS* on page 85.
- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to *GigaVUE-FM and GigaVUE-VM User’s Guide* available in the Customer Portal.

2 Overview of GigaVUE Cloud Suite - AWS

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

- *About GigaVUE Cloud for AWS* on page 9
- *Supported Architecture* on page 10

About GigaVUE Cloud for AWS

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 that form the GigaVUE Cloud.

GigaVUE-FM integrates with the Amazon Elastic Cloud Compute (EC2) APIs and deploys the components of the GigaVUE Cloud Suite for AWS in the Virtual Private Cloud (VPC).

The GigaVUE-FM is launched by subscribing to the GigaVUE Cloud Suite for AWS in the Community AMIs. Once the GigaVUE Cloud Suite sfor AWS instance is launched, the rest of the AMIs residing in the Community AMIs are automatically launched from GigaVUE-FM.

GigaVUE Cloud Suite for AWS includes the following components:

- **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 that forms the GigaVUE Cloud for AWS.

  GigaVUE-FM can be installed on-premises or launched as an Amazon Machine Image (AMI) in AWS. GigaVUE-FM manages the configuration of the following components in your Amazon Virtual Private Clouds (VPC):

  - GigaVUE V Series nodes
  - G-vTAP Controllers
  - GigaVUE V Series Controllers

  To launch the AMI in AWS, refer to *Obtain AMI* on page 14 and *G-vTAP Agents* on page 15.

To install GigaVUE-FM on premise, refer to *GigaVUE-FM and GigaVUE-VM User's Guide* available in the Customer Portal.

- **G-vTAP agent** is an agent that is deployed in the Elastic Compute Cloud (EC2) instance. This agent mirrors the selected traffic from the instances (virtual machines) to the GigaVUE® V Series node.

  The G-vTAP agent is offered as a Debian (.deb) or Redhat Package Manager (.rpm) package. Refer to *Install G-vTAP Agents* on page 17.
- **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.
- **GigaVUE® V Series node** is a visibility node that aggregates mirrored traffic from multiple G-vTAP agents. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools. GigaVUE Cloud Suite for AWS uses the standard IP GRE or VXLAN tunnels to deliver traffic to tool endpoints.

NOTE: With G-vTAP version 1.6-1 IPSec can be used to establish a secure tunnel between G-vTAP agents and GigaVUE V Series nodes, especially in a centralized controller and GigaVUE V Series node configuration where cross VPC tunneling may be required to be encrypted (refer Table 2-1 on page 10).

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

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

Table 2-1: Configuration options for Controllers and Nodes

Option 1: Standard Configuration	GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in all the VPCs.
Option 2: Centralized Controller and GigaVUE V Series Node Configuration	GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in a centralized VPC. **NOTE:** Peering must be active between VPCs within the same monitoring domain if the centralized controller and V Series option is chosen for configuring the components.

Supported Architecture

GigaVUE Cloud Suite for AWS supports the following cloud deployment models:

- *Hybrid Cloud* on page 11
- *Multi-VPC Cloud* on page 11
- *Centralized Fabric Controllers and Node Configuration* on page 12

Hybrid Cloud

In the hybrid cloud deployment model, you can send the customized traffic to the tools in AWS as well as the tools in the enterprise data center.

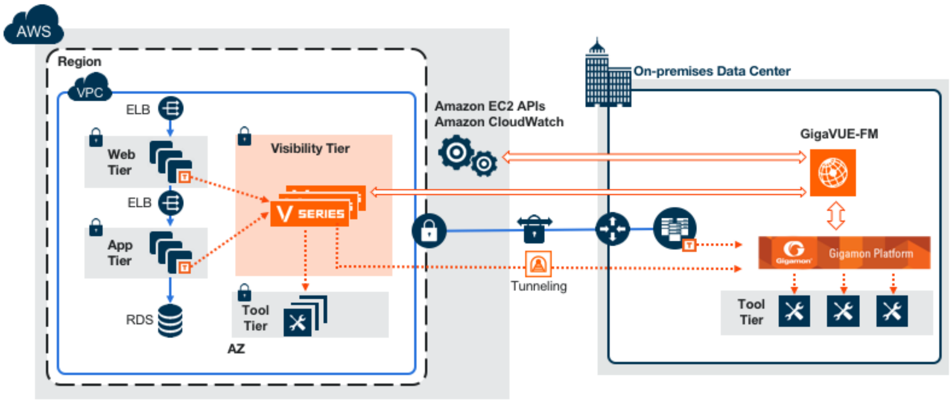


Figure 2-1: Hybrid Cloud Deployment

Multi-VPC Cloud

In the public cloud deployment model, you can send the customized traffic from a single VPC to the tools residing in the same VPC or from multiple VPCs to the tools residing in a different VPC.

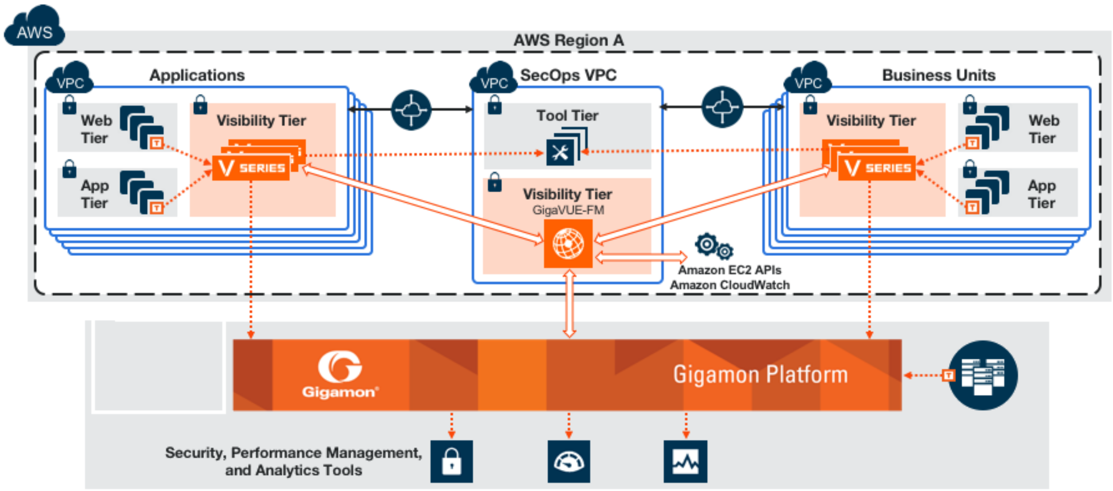


Figure 2-2: Public Cloud Deployment

Centralized Fabric Controllers and Node Configuration

In the centralized fabric controllers and node configuration deployment model, the following Gigamon components are deployed in a shared VPC:

- G-vTAP Controllers
- GigaVUE V Series Controllers
- GigaVUE V Series nodes

With this deployment model, the controllers and nodes are easily manageable as they are launched from a shared VPC. This further reduces the cost involved in the configuration and management of the controllers and nodes in each VPCs.

NOTE: Peering must be active between VPCs within the same monitoring domain if this option is chosen for configuring the components.

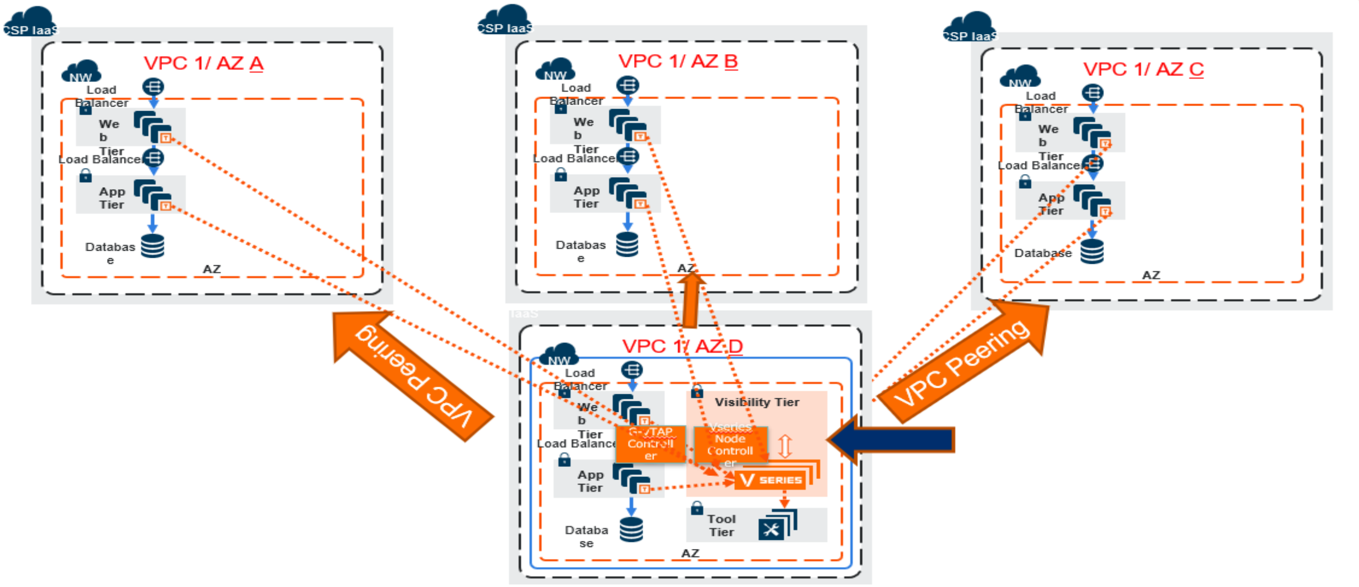


Figure 2-3: Centralized Controller/V Series Node Deployment Model

3 Configure Components in AWS

This chapter describes how to launch a GigaVUE-FM instance and how to configure G-vTAP Controllers, GigaVUE V Series nodes, and GigaVUE V Series Controllers in your VPC.

Refer to the following sections for details:

- *Obtain AMI* on page 14
- *G-vTAP Agents* on page 15

VPN Connectivity

GigaVUE-FM requires Internet access to integrate with the AWS API endpoints and deploy its GigaVUE Cloud Suite for AWS components. For more information about the VPN connectivity options, refer to Amazon Virtual Private Cloud Connectivity Options.

If there is no direct connection from GigaVUE-FM to the AWS public end points, a proxy can be used. Please refer to *Configure Proxy Server* on page 78

At a Glance

You must perform the following steps to configure GigaVUE Cloud Suite for AWS:

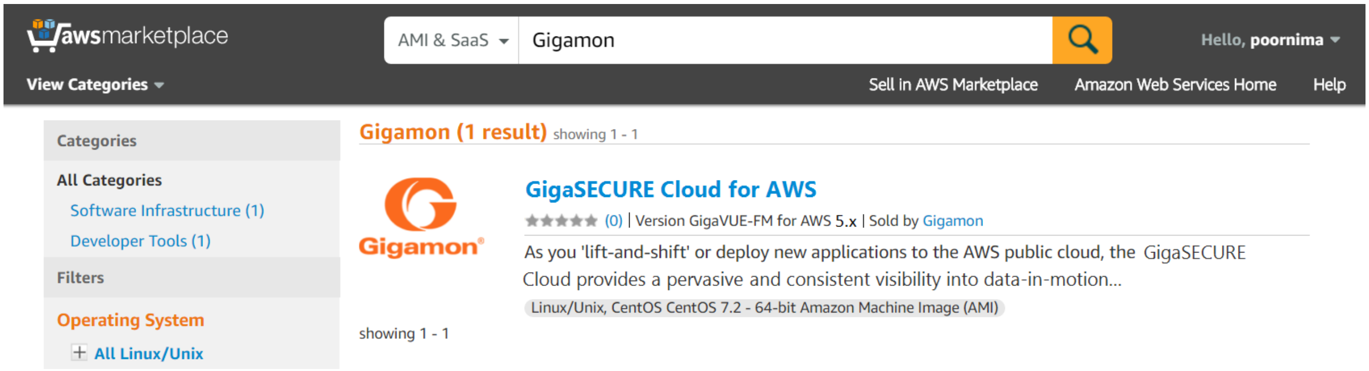
Step 1:	**Launch the GigaVUE-FM AMI**
Step 1.1:	Choose an instance type
Step 1.2:	Configure instance details
Step 1.3:	Add storage
Step 1.4:	Add tag instance
Step 1.5:	Configure security group
Step 1.6:	Review and launch
Step 2:	**Install the G-vTAP agents**
Step 3:	**Launch the visibility components in AWS**
Step 3.1	Connect to AWS
Step 3.2	Launch the G-vTAP controllers
Step 3.3.	Launch the GigaVUE V Series controllers
Step 3.4	Launch the GigaVUE V Series Nodes
Step 4	Configure traffic visibility for AWS

Obtain AMI

The AMI for the GigaVUE Cloud Suite for AWS is available in both the AWS Public Cloud and in AWS GovCloud.

GigaVUE Cloud Suite in AWS Public Cloud

The AMI for the GigaVUE Cloud Suite for AWS is available in the AWS Marketplace for both the Bring Your Own License (BYOL) and the Pay-As-You-Go (PAYG) options. Figure 3-1 on page 15 shows both the licensing models in the AWS Marketplace.



Gigamon (1 result) showing 1 - 1

GigaSECURE Cloud for AWS

(0) | Version GigaVUE-FM for AWS 5.x | Sold by Gigamon

As you 'lift-and-shift' or deploy new applications to the AWS public cloud, the GigaSECURE Cloud provides a pervasive and consistent visibility into data-in-motion...

Linux/Unix, CentOS CentOS 7.2 - 64-bit Amazon Machine Image (AMI)

showing 1 - 1

Figure 3-1: AMI in the AWS Public Cloud

For purchasing licensing with the BYOL option, contact the Gigamon Sales. Refer to *Contacting Sales* on page 103.

GigaVUE Cloud Suite in AWS GovCloud

AWS GovCloud is an isolated AWS region that contains specific regulatory and compliance requirements of the US government agencies. The AWS GovCloud (US) Region adheres to U.S. International Traffic in Arms Regulations (ITAR) requirements.

To monitor the instances that contain all categories of Controlled Unclassified Information (CUI) data and sensitive government data in the AWS GovCloud (US) Region, the AWS GovCloud AMI provides the same robust features in the AWS GovCloud as in the AWS public cloud.

G-vTAP Agents

A G-vTAP agent is a tiny footprint user-space agent (G-vTAP) that is deployed in an EC2 instance. 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. If secure tunnel option is selected, then IPSec is used to establish secure tunnel between G-vTAP agent and GigaVUE V Series nodes.

A G-vTAP agent consists of a source interface and a destination interface. The network packets collected from the source interface are sent to the destination interface. From the destination interface, the packets traverse through the L2 GRE/VXLAN tunnel interface or IPSec tunnel interface to the GigaVUE V Series node.

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

NOTE: For environments with both Windows and Linux agents or just windows agents, VXLAN tunnels in the G-vTAP controller specification is required.

Linux Agent Installation

Refer to the following sections for the Linux agent installation:

- *Single ENI Configuration* on page 16
- *Dual ENI Configuration* on page 16
- *Install G-vTAP Agents* on page 17
- *Install from Ubuntu/Debian Package* on page 17
- *Install from RPM Package* on page 18

Then refer to *Create Images with Agent Installed* on page 21.

Single ENI Configuration

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

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

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

Dual ENI Configuration

A G-vTAP agent lets you configure two ENIs. One ENI can be configured as the source interface and another ENI can be configured as the destination interface.

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 ENI configuration, you may need to modify the network configuration files to make sure that the extra ENI will initialize at boot time.

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

- *Install from Ubuntu/Debian Package*
- *Install from RPM Package*

You can install IPSec on G-vTAP agents either from Debian or RPM packages. Refer to the section *Install IPSec on G-vTAP Agent*.

Install from Ubuntu/Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent Debian (.deb) package.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_1.7-1_amd64.deb
ubuntu@ip-10-0-0-246:~$ sudo dpkg -i
   gvtap-agent_1.7-1_amd64.deb
```

3. Once the G-vTAP package is installed, modify the file /etc/gvtap-agent/gvtap-agent.conf to c onfigure and register the source and destination interfaces.

   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. 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 service gvtap-agent status
G-vTAP Agent is running
```

Install 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 RPM (.rpm) package.
2. Copy this package to your instance. Install the package with root privileges, for example:

   ```
   [ec2-user@ip-10-0-0-214 ~]$ ls
   gvtap-agent_1.7-1_x86_64.rpm
   [ec2-user@ip-10-0-0-214 ~]$ sudo rpm -i
      gvtap-agent_1.7-1_x86_64.rpm
   ```

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

   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. Reboot the instance.

   Check the status with the following command:

   ```
   [ec2-user@ip-10-0-0-214 ~]$ sudo service gvtap-agent status
   G-vTAP Agent is running
   ```

Windows Agent Installation

To install the Windows agent:

1. Download the Windows agent package.
2. Extract the contents of the .zip file into a convenient location.
3. Run ‘WinPcap_4_1_3.exe’ (located in the ‘winpcap’ folder) as **Administrator**.
4. Run ‘install.bat’ as **Administrator**.
5. If you want to start the Windows G-vTAP agent, you may do one of the following:
   - Reboot the VM.
   - Run ‘sc start gvtap’ from the command prompt.
   - Start the G-vTAP Agent from the Task Manager.

Next, refer to *Create Images with Agent Installed* on page 21.

Install IPSec on G-vTAP Agent

If IPSec is used to establish secure connection between G-vTAP agents and GigaVUE V Series nodes, then you must install IPSec on G-vTAP agent instances. To install IPSec on G-vTAP agent you need the following files:

- **StrongSwan binary installer TAR file:** The TAR file contains strongSwan binary installer for different platforms. Each platform has its own TAR file. Refer to https://www.strongswan.org/ for more details.
- **IPSec package file:** The package file includes the following:
  - CA Certificate
  - Private Key and Certificate for G-vTAP Agent
  - IPSec configurations

Refer to the following sections for installing IPSec on G-vTAP Agent:

- *Install from Ubuntu/Debian Package* on page 19
- *Install from Red Hat Enterprise Linux and Centos* on page 19
- *Install from Red Hat Enterprise Linux and Centos with Selinux Enabled* on page 20

Install from Ubuntu/Debian Package

1. Launch the G-vTAP agent AMI.
2. Copy the G-vTAP package files and strongSwan TAR file to the G-vTAP agent:

- strongswan5.3.5-1ubuntu3.8_amd64-deb.tar.gz
- gvtap-agent_1.7-1_amd64.deb
- gvtap-ipsec_1.7-1_amd64.deb

3. Install the G-vTAP agent package file:

```
sudo dpkg -i gvtap-agent_1.7-1_amd64.deb
```

4. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

5. Install strongSwan:

```
tar -xvf strongswan5.3.5-1ubuntu3.8_amd64-deb.tar.gz
    cd strongswan-5.3.5-1ubuntu3.8_amd64/
    sudo sh ./swan-install.sh
```

6. Install IPSec package:

```
sudo dpkg -i gvtap-ipsec_1.7-1_amd64.deb
```

Install from Red Hat Enterprise Linux and Centos

1. Launch RHEL/Centos agent AMI image.
2. Copy the following package files and strongSwan TAR files to the G-vTAP agent:

- strongswan-5.7.1-1.el7.x86_64.tar.gz for rhel7/centos7
- strongswan-5.4.0-2.el6.x86_64.tar.gz for rhel6/centos6
- gvtap-agent_1.7-1_x86_64.rpm
- gvtap-ipsec_1.7-1_x86_64.rpm

3. Install G-vTAP agent package:

```
sudo rpm -ivh gvtap-agent_1.7-1_x86_64.rpm
```

4. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

5. 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
```

6. Install IPSec package:

```
sudo rpm -i gvtap-ipsec_1.7-1_x86_64.rpm
```

NOTE: You must install IPSec package after installing StrongSwan.

Install from Red Hat Enterprise Linux and Centos with Selinux Enabled

1. Launch the RHEL/Centos agent AMI image.
2. Copy package files and strongSwan TAR file to G-vTAP agent.
   - strongswan-5.7.1-1.el7.x86_64.tar.gz for rhel7/centos7
   - strongswan-5.4.0-2.el6.x86_64.tar.gz for rhel6/centos6
   - gvtap-agent_1.7-1_x86_64.rpm
   - gvtap-ipsec_1.7-1_x86_64.rpm

- gvtap.te and gvtap_ipsec.te files (type enforcement files)

3. checkmodule -M -m -o gvtap.mod gvtap.te

   semodule_package -o gvtap.pp -m gvtap.mod

   sudo semodule -i gvtap.pp

4. checkmodule -M -m -o gvtap_ipsec.mod gvtap_ipsec.te

   semodule_package -o gvtap_ipsec.pp -m gvtap_ipsec.mod

   sudo semodule -i gvtap_ipsec.pp

5. Install G-vTAP agent package:

```
sudo rpm -ivh gvtap-agent_1.7-1_x86_64.rpm
```

6. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

```
# 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. Install IPSec package:

```
sudo rpm -i gvtap-ipsec_1.7-1_x86_64.rpm
```

Create Images with Agent Installed

If you want to avoid downloading and installing the G-vTAP agents every time there is a new instance to be monitored, you can save the G-vTAP agent running on an instance as a private AMI. When a new G-vTAP agent is launched in an instance, GigaVUE-FM automatically updates the number of monitoring instances in the monitoring session.

To save the G-vTAP agent as an AMI:

1. From the EC2 console, right click the instance.
2. Click **Image** > **Create Image**.

To launch the G-vTAP agent AMI:

1. Follow steps 1 to 11 as described in *G-vTAP Agents* on page 15 to launch the G-vTAP agent AMI.
2. In that procedure:
   a. Choose **t2 medium** as the instance type.
   b. When you add a device, click **Add Device** and add another ENI which acts as a mirror subnet.

GigaVUE Cloud Suite for AWS Fabric Components

The GigaVUE Cloud Suite for AWS consists of the following fabric components:

- G-vTAP Agents
- G-vTAP Controller
- GigaVUE V Series Nodes
- GigaVUE V Series Controllers

Refer to the following section for details.

G-vTAP Controller

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

NOTE: A single G-vTAP Controller (instance type t2.micro) can manage up to 1000 G-vTAP agents.

A G-vTAP Controller can only manage G-vTAP agents that has the same version. For example, the G-vTAP Controller v1.3 can only manage G-vTAP agents v1.3. So, if you have G-vTAP agents v1.2 still deployed in the EC2 instances, you must configure both G-vTAP Controller v1.2 and v1.3.

While configuring the G-vTAP Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the G-vTAP agents to the GigaVUE V Series nodes. The tunnel type can be L2GRE or VXLAN.

GigaVUE V Series Controllers

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

NOTE: A single GigaVUE V Series Controller can manage up to 100 GigaVUE V Series nodes. The recommended minimum instance type is t2.micro for V Series Controller.

GigaVUE V Series Nodes

GigaVUE® V Series node is a visibility node that aggregates mirrored traffic from multiple G-vTAP agents. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite for AWS using the standard IP GRE or VXLAN tunnels.

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

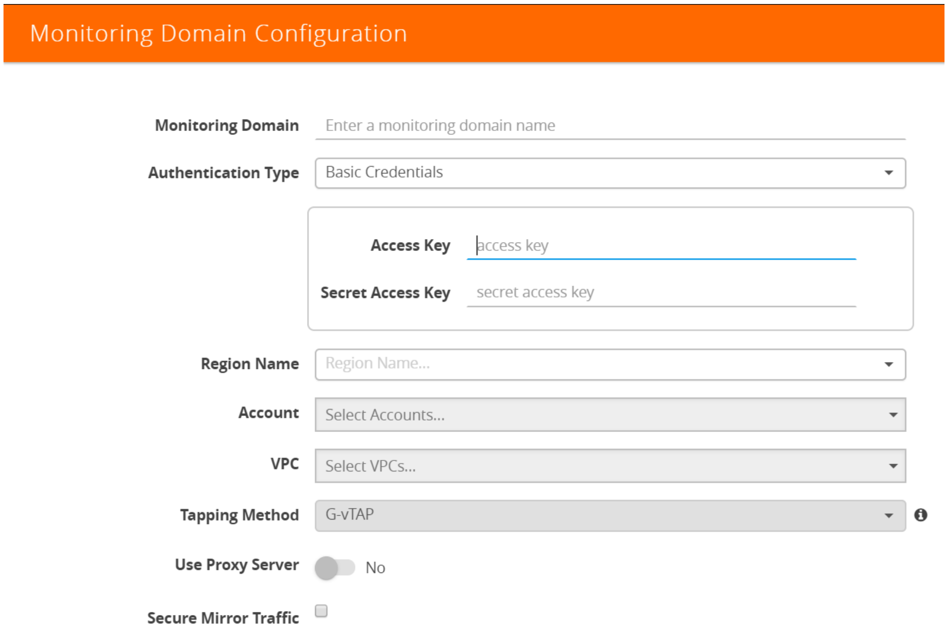
Creating a Monitoring Domain and Launching Visibility Fabric

GigaVUE-FM connects to the VPC through the EC2 API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the EC2 API. For more information about the endpoint and the protocol used, refer to http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region.

GigaVUE-FM provides you the flexibility to connect to multiple VPCs. You can choose the VPC ID and launch the GigaVUE Cloud Suite for AWS components in the desired VPCs.

To create a Monitoring Domain:

1. Click **Cloud** in the top navigation link.
2. On the left navigation pane, select **AWS** > **Monitoring Domain**, and then click the **New** button. The Monitoring Domain Configuration page is displayed.



Monitoring Domain Configuration

Monitoring Domain: Enter a monitoring domain name

Authentication Type: Basic Credentials

Access Key: access key

Secret Access Key: secret access key

Region Name: Region Name...

Account: Select Accounts...

VPC: Select VPCs...

Tapping Method: G-vTAP

Use Proxy Server: No

Secure Mirror Traffic: □

Figure 3-2: Configuring monitoring domain

3. Enter or select the appropriate information as shown in Table 3-1 on page 23.

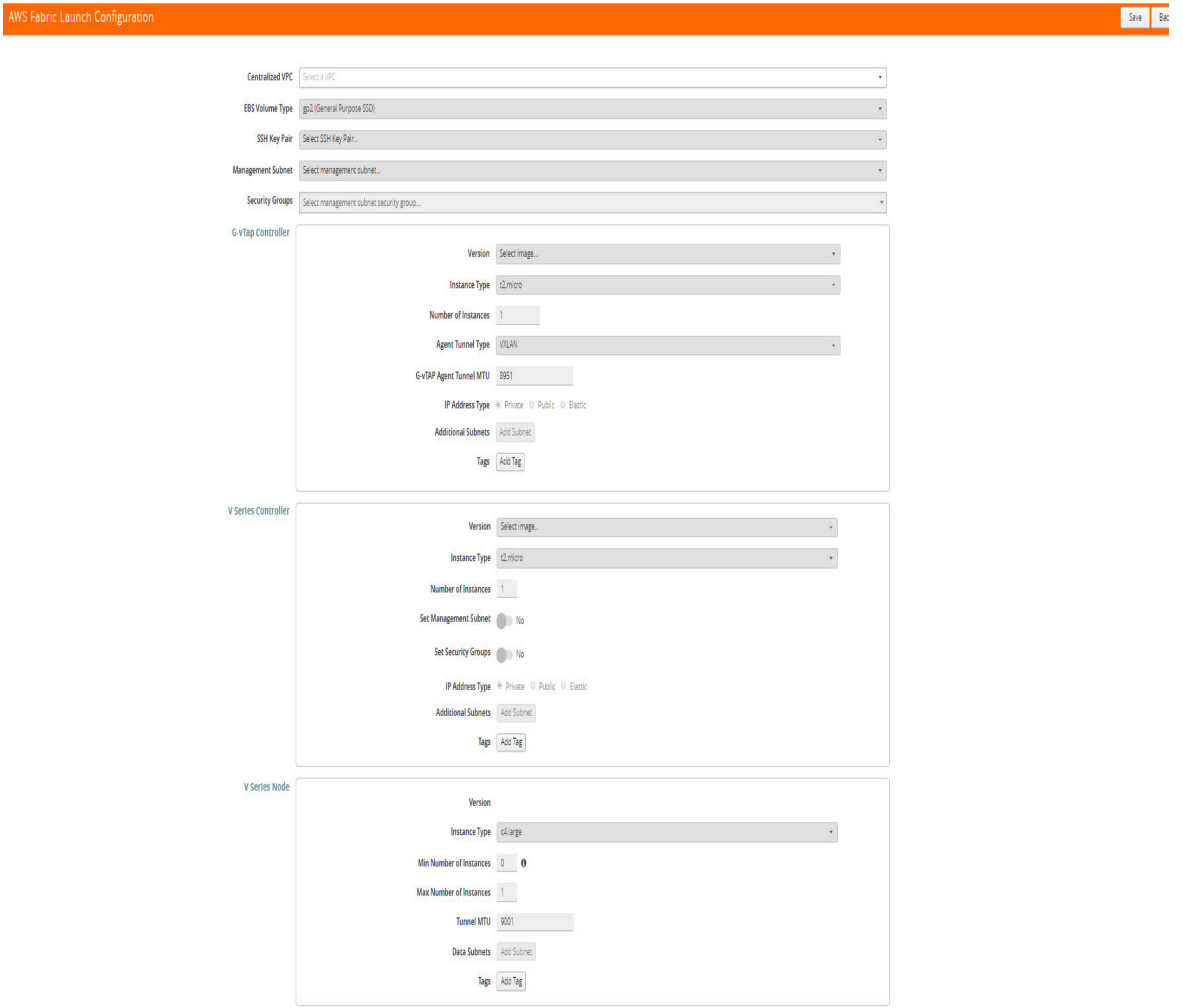
Table 3-1: Creating a Monitoring Domain

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain.
Authentication Type	Authentication type for the connection. Options are: • Basic Credentials • EC2 Instance Role If Basic Credentials is selected, you must enter the Access Key and Secret Access keys.
Region Name	AWS region for the monitoring domain. For example, EU (London).
Account	Select the AWS account
VPC	VPCs belonging to the account.
Tapping Method	Tapping method. Options are: • **G-vTAP**: If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP agents • **AWS VPC Traffic Monitoring Phase1**: If you select this option as tapping method, then you need not configure the G-vTAP Controller **NOTE:** The AWS VPC Traffic Monitoring Phase1 option is available for preview purposes only through Gigamon's Beta Program. If you have interest in exploring this option, please reach out to your Gigamon sales representative and ask to be included in the Beta Program.
Secure Mirror Traffic	Check box to establish secure tunnel between G-vTAP agents and GigaVUE V Series nodes for traffic across VPCs.
Use Proxy Server	Toggle option to add a proxy server. Proxy server enables communication from GigaVUE-FM to the Internet, if GigaVUE-FM is deployed in a private network.

Table 3-1: Creating a Monitoring Domain

Field	Description
Proxy Server	The list of proxy servers already configured in GigaVUE-FM. For more information on adding the proxy servers before configuring the AWS connection, refer to *Configure Proxy Server* on page 78
Add Proxy Server	The proxy sever can be configured from the Settings > Proxy Server page. Click **Add Proxy Server**. For more information, refer to *Configure Proxy Server* on page 78.

4. Click **Save**. The AWS Fabric Launch Configuration page appears. The top half of the page lists the fields that are to be configured in common for the following fabric components:
   - G-vTAP Controller
   - GigaVUE V Series Controller
   - GigaVUE V Series Nodes



AWS Fabric Launch Configuration

Centralized VPC: Select a VPC

EBS Volume Type: gp2 (General Purpose SSD)

SSH Key Pair: Select SSH Key Pair...

Management Subnet: Select management subnet...

Security Groups: Select management subnet security group...

G-vTap Controller

Version: Select image...

Instance Type: t2.micro

Number of Instances: 1

Agent Tunnel Type: VXLAN

G-vTAP Agent Tunnel MTU: 8951

IP Address Type: ● Private ○ Public ○ Elastic

Additional Subnets: Add Subnet

Tags: Add Tag

V Series Controller

Version: Select image...

Instance Type: t2.micro

Number of Instances: 1

Set Management Subnet: No

Set Security Groups: No

IP Address Type: ● Private ○ Public ○ Elastic

Additional Subnets: Add Subnet

Tags: Add Tag

V Series Node

Version

Instance Type: c4.large

Min Number of Instances: 0

Max Number of Instances: 1

Tunnel MTU: 9001

Data Subnets: Add Subnet

Tags: Add Tag

Figure 3-3: Configuring fabric components

5. Enter or select the appropriate information as shown in Table 3-2 on page 26.

Table 3-2: AWS Fabric Launch Configuration - Common fields

Field	Description
Centralized VPC	Alias of the centralized VPC in which the G-vTAP Controllers, GigaVUE V Series Controllers and the GigaVUE V Series nodes are launched.
EBS Volume Type	The Elastic Block Store (EBS) volume that you can attach to the fabric components. The available options are: • gp2 (General Purpose SSD) • io1 (Provisioned IOPS SSD) • Standard (Magnetic).
SSH Key Pair	The SSH key pair for the fabric components. For more information about SSH key pair, refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.
Management Subnet	The subnet that is used for communication between the controllers and the nodes, as well as to communicate with GigaVUE-FM. This is a required field.
Security Groups	The security group created for the fabric components. For more information about security groups, refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.

6. Enter or select appropriate information as shown in Table 3-3 on page 27 for G-vTAP Controller Configuration.

Table 3-3: Fields for G-vTAP Controller Configuration

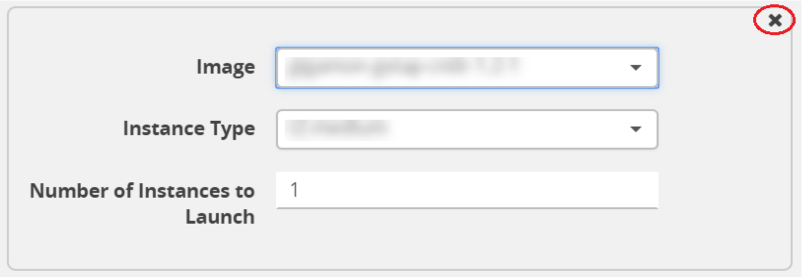
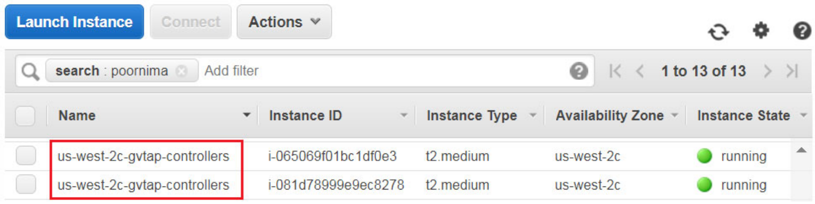
Fields	Description
Version	The G-vTAP Controller version. The G-vTAP Controller version you configure must always be the same as the G-vTAP agents' version number deployed in the EC2 instances. This is because the G-vTAP Controller v1.2 can only manage G-vTAP agents v1.2. Similarly, the G-vTAP Controller v1.3 can only manage G-vTAP agents v1.3. If there are multiple versions of G-vTAP agents deployed in the EC2 instances, then you must configure multiple versions of G-vTAP Controllers that matches the version numbers of the G-vTAP agents. **NOTE:** If there is a version mismatch between G-vTAP controllers and G-vTAP agents, GigaVUE-FM cannot detect the agents in the instances. To add multiple versions of G-vTAP Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP agents installed in the instances. **c.** From the **Instance Type** down-down list, select an instance type for the G-vTAP Controller. The recommended instance type is t2.micro. **NOTE:** The instance type t2.nano is not supported. **d.** In **Number of Instances to Launch**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1. **e.** The Elastic IPs drop-down list appears only if the **Elastic** option is selected in the IP Address Type. From the **Elastic IPs** drop-down list, select an IP. **NOTE:** The Elastic IPs must be allocated in the EC2 management console prior to step e.
	An older version of G-vTAP Controller can be deleted once all the G-vTAP agents are upgraded to the latest version. To delete a specific version of G-vTAP Controller, click **x** (delete) next to its G-vTAP Controller image.  Image Instance Type Number of Instances to Launch 1 *Figure 3-4: Delete a G-vTAP Controller Version* Once you delete a G-vTAP Controller image from the G-vTAP Configuration page, all the G-vTAP Controller instances of that version are deleted from AWS.
Instance Type	The instance type for the G-vTAP controller. The recommended minimum instance type is c4. large.

Table 3-3: Fields for G-vTAP Controller Configuration

Fields	Description
Number of Instances	The number of instances that can be assigned to the G-vTAP Controller.
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. If any Windows agents co-exist with Linux agents, VXLAN must be selected.
G-vTAP Agent 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 V Series node. For GRE, the default value is 9001. For VXLAN, the default value is 8951. However, the G-vTAP agent tunnel MTU should be 50 bytes less than the agent's destination interface MTU size. **NOTE:** If Secure Mirror Traffic option is enabled, then to account for IPSec tunnel overhead and to minimize the occurrence of fragmentation, the following values are recommended to be configured for G-vTAP Agent Tunnel MTU: AWS Platform MTU is 9001 • With agent tunnel type L2GRE and 'Secure Mirror Traffic' option enabled, G-vTAT Agent Tunnel MTU should be set as (9001-42-53) = 8906. • With agent tunnel type L2GRE and 'Secure Mirror Traffic' option disabled, G-vTAP Agent Tunnel MTU should be configured as (9001-42)= 8959 • With agent tunnel type VXLAN and 'Secure Mirror Traffic' option enabled, G-vTAP Agent Tunnel MTU should be (9001-50-53)= 8898. • With agent tunnel type VXLAN And 'Secure Mirror Traffic' option disabled, G-vTAP Agent Tunnel MTU should be 8951.
IP Address Type	The IP address type. Select one of the following: • Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the G-vTAP Controller and GigaVUE-FM. • Select Public if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. • Select Elastic if you want a static public IP address for your instance. Ensure to have the available elastic IP address in your VPC. **NOTE:** The elastic IP address does not change when you stop or start the instance.

Table 3-3: Fields for G-vTAP Controller Configuration

<table>
<tr><th>Fields</th><th>Description</th></tr>
<tr><td><b>Additional Subnet(s)</b></td><td>(Optional) If there are G-vTAP agents on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the G-vTAP Controller can communicate with all the G-vTAP agents.
Click <b>Add</b> to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.</td></tr>
<tr><td><b>Tag(s)</b></td><td>(Optional) The key name and value that helps to identify the G-vTAP Controller instances in your AWS environment. For example, you might have G-vTAP Controllers deployed in a VPC. To identify the G-vTAP Controllers you can provide a name that is easy to identify such as us-west-2-gvtap-controllers.
To add a tag,
<b>a.</b> Click <b>Add tag</b>.
<b>b.</b> In the <b>Key</b> field, enter the key. For example, enter Name.
<b>c.</b> In the <b>Value</b> field, enter the key value. For example, us-west-2-gvtap-controllers.
When the G-vTAP Controllers are launched in the VPC, they appear as shown in Figure 3-5 on page 29:


Launch Instance
Connect
Actions
search : poornima
Add filter
1 to 13 of 13

<table><tr><th>Name</th><th>Instance ID</th><th>Instance Type</th><th>Availability Zone</th><th>Instance State</th></tr><tr><td>us-west-2c-gvtap-controllers</td><td>i-065069f01bc1df0e3</td><td>t2.medium</td><td>us-west-2c</td><td>● running</td></tr><tr><td>us-west-2c-gvtap-controllers</td><td>i-081d78999e9ec8278</td><td>t2.medium</td><td>us-west-2c</td><td>● running</td></tr></table><i>Figure 3-5: G-vTAP Controllers with Custom Tag Name</i></td></tr>
</table>

7. Enter or select appropriate information as shown in Table 3-3 on page 27 for GigaVUE V Series Controller Configuration.

Table 3-4: Fields for GigaVUE V Series Controller Configuration

Fields	Description
Version	GigaVUE V Series Controller version.
Instance Type	Instance type for the GigaVUE V Series Controller
Number of Instances	Number of GigaVUE V Series controllers to be launched in the AWS Account
Set Management Subnet	Toggle option to set the management subnet that is used to communicate with GigaVUE-FM and GigaVUE V Series node.
Set Security Groups	Toggle option to set the security group that is created for the GigaVUE V Series node. Refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide* for more details.

Table 3-4: Fields for GigaVUE V Series Controller Configuration

Fields	Description
IP Address Type	The IP address type. Select one of the following: • Select Private if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Controller and GigaVUE-FM instances in the same network. • Select Public if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. • Select Elastic if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Additional Subnets	(Optional) If there are GigaVUE V Series nodes on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the GigaVUE V Series Controller can communicate with all the GigaVUE V Series nodes. Click Add to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series Controller instances in your AWS environment.

8. Enter or select appropriate information as shown in Table 3-5 on page 30 for GigaVUE V Series Node Configuration.

Table 3-5: Fields for V Series Nodes

Fields	Description
Version	GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series node. The recommended minimum instance type is c4. large.
Min Number of Instances	The minimum number of GigaVUE V Series nodes to be launched in the AWS connection. The minimum number of instances that can be entered is 0. When 0 is entered, no GigaVUE V Series nodes are launched. **NOTE:** If the minimum number of instances is set as '0', then the nodes will be launched when a monitoring session is deployed as long as GigaVUE-FM discovers some targets to monitor.
Max Number of Instances	The maximum number of GigaVUE V Series nodes that can be launched in the monitoring domain.
Tunnel MTU	The Maximum Transmission Unit (MTU) on the outgoing tunnel endpoints of the GigaVUE V Series node when a monitoring session is deployed. The default value is 9001.

Table 3-5: Fields for V Series Nodes

Fields	Description
Data Subnets	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the G-vTAP agents. **NOTE:** Using the Tool Subnet checkbox you can indicate the subnets to be used by the V Series node to egress the aggregated/manipulated traffic to the tools.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series node instances in your AWS environment. For example, you might have GigaVUE V Series node deployed in many regions. To distinguish these GigaVUE V Series node based on the regions, you can provide a name that is easy to identify such as us-west-2-vseries. To add a tag: **a.** Click Add tag. **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-vseries.

9. Click **Save** to save the configuration.

4 Configure Monitoring Sessions in AWS

This chapter describes how to setup the tunnel endpoints to receive and send traffic from the GigaVUE V Series node, and how to filter, manipulate, and send the traffic from the GigaVUE V Series node to the monitoring tools or GigaVUE H Series node.

Refer to the following sections for details:

Overview of GigaVUE Cloud in AWS Components

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

Table 4-1 on page 34 lists the components of the monitoring session:

Table 4-1: Components of Traffic Visibility Sessions

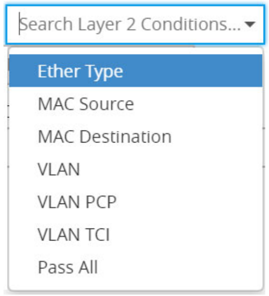
Parameter	Description
Map	A map (M) is used to filter the traffic flowing through the GigaVUE V Series node. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.
Rule	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic. The rules must contain the appropriate Layer 2 (L2) to Layer 4 (L4) filters defined in them. For example, if you want to filter the traffic for HTTP Port 80, you must select the following criteria: • Layer 2—Ethertype IPv4 or IPv6 • Layer 3—Protocol TCP • Layer 4—Port Destination 80 By default, a rule always displays conditions based on the attributes of L2. Refer to Figure 4-1 on page 34.  Search Layer 2 Conditions... Ether Type MAC Source MAC Destination VLAN VLAN PCP VLAN TCI Pass All *Figure 4-1: Layer 2 Rule Conditions* A rule is also associated with priority and action set.
Priority	A priority determines the order in which the rules are executed. The greater the value, the higher the priority. The priority value can range from 0 to 99.

Table 4-1: Components of Traffic Visibility Sessions

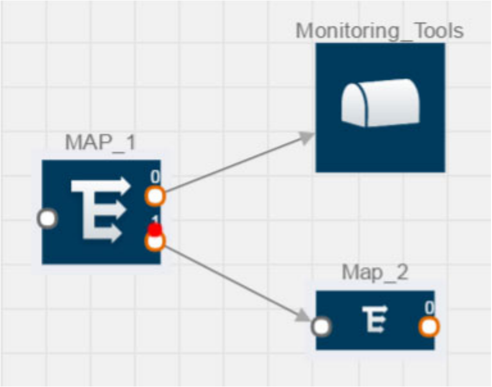
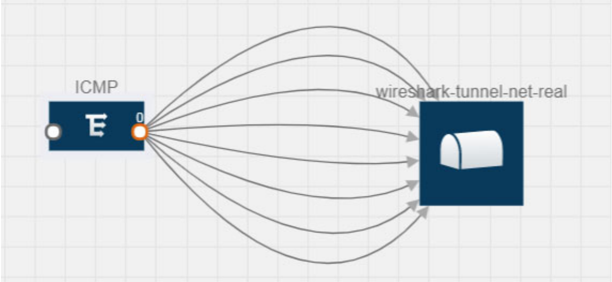
Parameter	Description
Action Set	An action set is an exit point in a map that you can drag and create links to the other maps, applications, and the monitoring tools. A single map can have multiple action sets. A single action set can have multiple links connecting to maps and applications. In the following example (refer to Figure 4-2 on page 35), the packets that match the rules in Action Set 0 are forwarded to a tunnel endpoint. The packets that match the rules in Action Set 1 are forwarded to another map.  *Figure 4-2: Action Set* A single action set can have up to 8 links connecting the same destination point. The same packets from the map are replicated in 8 different links. Refer to Figure 4-3 on page 35.  *Figure 4-3: Action Set with Multiple Links*
Link	A link directs the packets to flow from a map to the destination. The destination could be the other maps, applications, and the monitoring tools. In Figure 4-2 on page 35, the link originating from action set 0 is moving the traffic from MAP_1 to Monitoring_Tools. A link lets you add header transformation to the packets passing through it before they are sent to the destination. For more information about Header Transformation, refer to *Add Header Transformations* on page 70.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.
Application	An application performs operations such as sampling, slicing, and masking on the traffic.
Inclusion Map	An inclusion map determines the instances or ENIs to be included for monitoring. This map is used only for target selection.
Exclusion Map	An exclusion map determines the instances or ENIs to be excluded from monitoring. This map is used only for target selection.

Table 4-1: Components of Traffic Visibility Sessions

Parameter	Description
Target	A target determines the instances that are to be monitored. Targets are determined based on the following formula: Target = (Maps ∩ Inclusion map) – Exclusion map
Automatic Target Selection (ATS)	A built-in feature that automatically selects the EC2 instances and ENIs based on the rules defined in the maps, inclusion maps, and exclusion maps in the monitoring session. For example, if you create a rule determining the MAC source address in a map and a subnet in the inclusion map, the egress traffic from all instances or ENIs matching the MAC address in the specified subnet is selected for tapping the traffic.
Tunnel	A tunnel lists the monitoring tools to which the traffic matching the filtered criteria is routed.

Create Tunnel Endpoints

The customized traffic from the GigaVUE V Series node is distributed to the tunnel endpoints using a standard L2 Generic Routing Encapsulation (GRE) or Virtual Extensible LAN (VXLAN) tunnel.

To create the tunnel endpoints:

1. Select **AWS** > **Settings** > **Tunnel Spec Library**.
2. Click **New**. The Add Tunnel Spec page is displayed as shown in Figure 4-4 on page 36.

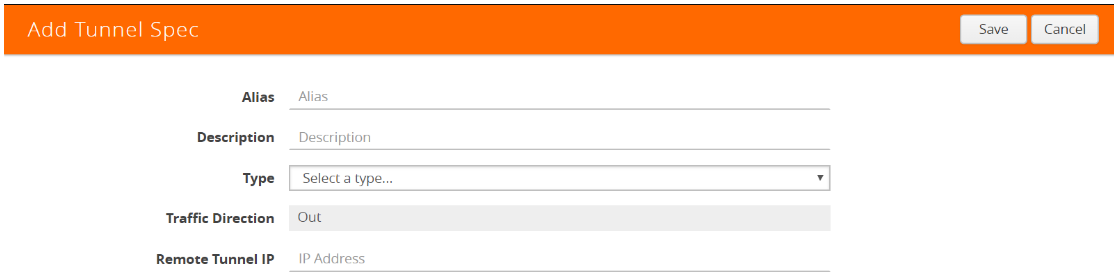


Figure 4-4: Adding a Tunnel Endpoint

3. Select or enter the appropriate information as shown in Table 4-2 on page 36.

Table 4-2: Fields for Tunnel Endpoint

Field	Description
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Type	The type of the tunnel. Select L2GRE or VXLAN to create a tunnel.

Table 4-2: Fields for Tunnel Endpoint

Field	Description
Traffic Direction	The direction of the traffic flowing through the GigaVUE V Series node. Choose **Out** for creating a tunnel from the GigaVUE V Series node to the destination endpoint. **NOTE:** Traffic Direction **In** is not supported in the current release.
Remote Tunnel IP	The IP address of the tunnel destination endpoint.

4. Click **Save**. The tunnel endpoints are added successfully.

Create Monitoring Session

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

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

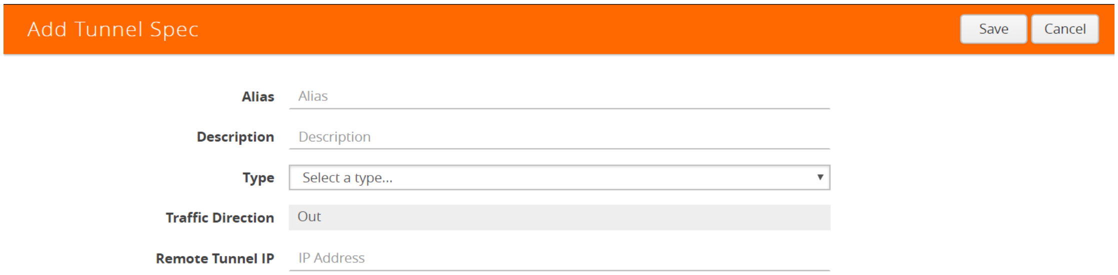
- *Create New Session* on page 38
- *Clone Monitoring Session* on page 38
- *Add Applications to Monitoring Session* on page 47
- *Deploy Monitoring Session* on page 68
- *Add Header Transformations* on page 70
- *View Statistics* on page 73
- *View Topology* on page 74

Create New Session

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

To create a new session:

1. Select **AWS** > **Monitoring Session**. The **Monitoring Sessions** page is displayed.
2. Click **New**. The Create a New Monitoring Session page is displayed as shown in Figure 4-4 on page 36.



Add Tunnel Spec

Alias: Alias

Description: Description

Type: Select a type...

Traffic Direction: Out

Remote Tunnel IP: IP Address

Figure 4-5: Creating Monitoring Session

3. Enter the appropriate information in the **Create a New Monitoring Session** dialog box as shown in Table 4-3 on page 38.

Table 4-3: Fields for Creating Monitoring Session

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain.
Connection	The AWS connection that is to be included as part of the monitoring domain. You can select the required connections.
Agent Pre-filtering	When enabled, traffic is filtered at the G-vTAP agent-level, before mirroring to the V Series Nodes, which reduces the load on the V Series Nodes and the Cloud networks. *Agent Pre-filtering* on page 45.

4. Click **Create.**

Clone Monitoring Session

You can clone an existing monitoring session.

To clone a monitoring session:

1. Select the monitoring session that you need to clone from the **Monitoring Sessions** page.
2. Click **Clone**.

3. Enter the appropriate information in the **Clone Monitoring Session** dialog box as shown in Table 4-4 on page 39.

Table 4-4: Fields for Cloning the Monitoring Session.

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

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

Create Map

Each map can have up to 32 rules associated with it. Table 4-5 on page 39 lists the various conditions that you can select for creating a map, inclusion map, and exclusion map.

Table 4-5: Conditions for the Rules

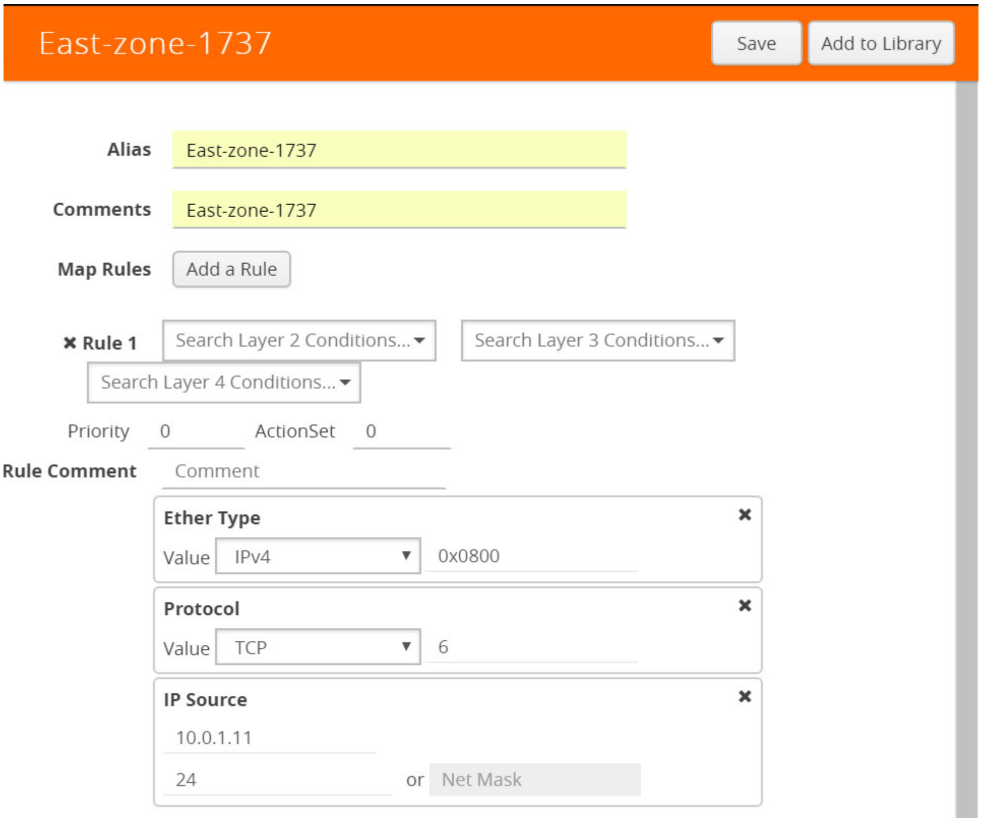
Conditions	Description
L2, L3, and L4 Filters	
Ether Type	The packets are filtered based on the selected ethertype. The following conditions are displayed: • IPv4 • IPv6 • ARP • RARP • Other **L3 Filters** If you choose IPv4 or IPv6, the following L3 filter conditions are displayed: • Protocol • IP Fragmentation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

Table 4-5: Conditions for the Rules

Conditions	Description
MAC Destination	The ingress traffic from the instances or ENIs matching the specified destination MAC address is selected.
VLAN	All the traffic matching the specified IEEE 802.1q Virtual LAN tag is filtered. Specify a number from 0 to 4094.
VLAN Priority Code Point (PCP)	All the traffic matching the specified IEEE 802.1q Priority Code Point (PCP) is filtered. Specify a value between 0 to 7.
VLAN Tag Control Information (TCI)	All the traffic matching the specified VLAN TCI value is filtered. Specify the exact TCI value.
Pass All	All the packets coming from the monitored instances are passed through the filter. When Pass All is selected, the L3 and L4 filters are disabled.

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

When you select a condition with either source or destination specified, it determines the direction based on the selection. For example, if only IP source is selected as shown in Figure 4-6 on page 40, the egress traffic from the instances in the subnet 10.0.1.0/24 is selected for monitoring the traffic.



East-zone-1737

Alias: East-zone-1737

Comments: East-zone-1737

Map Rules

Rule 1

Priority: 0
ActionSet: 0

Rule Comment: Comment

Ether Type
Value: IPv4 — 0x0800

Protocol
Value: TCP — 6

IP Source
10.0.1.11
24 or Net Mask

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

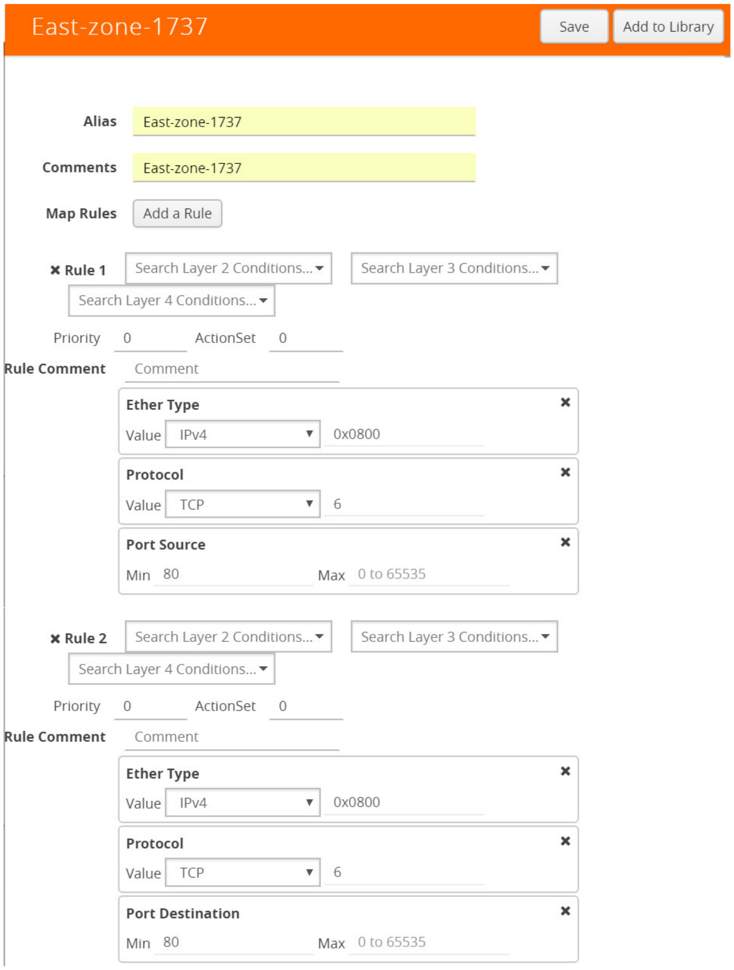
Figure 4-6: Creating a Map for Tapping Egress Traffic

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

To create a new map:

1. Select **AWS > Monitoring Session**.
2. Click **New**. The Monitoring Sessions page is displayed.
3. Create a new session. Refer to *Create New Session* on page 38.
4. From **Maps**, drag and drop a new map template to the workspace. If you are creating an exclusion or inclusion map, drag and drop a new map template to their respective section at the bottom of the workspace.

   The new map page is displayed as shown in Figure 4-7 on page 41.



East-zone-1737

Alias: East-zone-1737

Comments: East-zone-1737

Map Rules

✖ Rule 1

Search Layer 2 Conditions... ▾ | Search Layer 3 Conditions... ▾ | Search Layer 4 Conditions... ▾

Priority: 0 ActionSet: 0

Rule Comment: Comment

Ether Type ✖
Value: IPv4 ▾ 0x0800

Protocol ✖
Value: TCP ▾ 6

Port Source ✖
Min: 80 Max: 0 to 65535

✖ Rule 2

Search Layer 2 Conditions... ▾ | Search Layer 3 Conditions... ▾ | Search Layer 4 Conditions... ▾

Priority: 0 ActionSet: 0

Rule Comment: Comment

Ether Type ✖
Value: IPv4 ▾ 0x0800

Protocol ✖
Value: TCP ▾ 6

Port Destination ✖
Min: 80 Max: 0 to 65535

Figure 4-7: Creating a New Map

5. Enter the appropriate information for creating a new map as shown in Table 4-6 on page 42.

Table 4-6: Fields for Creating a New Map

Parameter	Description
Alias	The name of the new map. **NOTE:** The name can contain alphanumeric characters with no spaces.
Comments	The description of the map.

Table 4-6: Fields for Creating a New Map

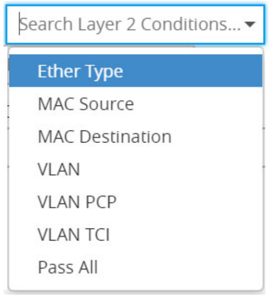
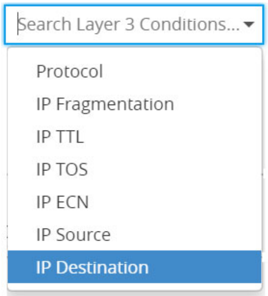
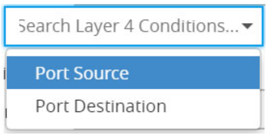
Parameter	Description
Map Rules	The rules for filtering the traffic in the map. To add a map rule: **a.** Click **Add a Rule**. **b.** Select a condition from the **Search L2 Conditions** drop-down list and specify a value. Based on this selection, the Search L3 Conditions drop-down list is automatically updated. Refer to Figure 4-8 on page 43.  Search Layer 2 Conditions... Ether Type MAC Source MAC Destination VLAN VLAN PCP VLAN TCI Pass All *Figure 4-8: L2 Conditions* **c.** Select a condition from the **Search L3 Conditions** drop-down list and specify a value. Refer to Figure 4-9 on page 43.  Search Layer 3 Conditions... Protocol IP Fragmentation IP TTL IP TOS IP ECN IP Source IP Destination *Figure 4-9: L3 Conditions* **d.** (Optional) If you have selected TCP or UDP as the protocol in the L3 conditions, then select Port Source or Port Destination from the Search L4 Conditions drop-down list and specify a value. If you have selected conditions other than TCP or UDP, then the Search L4 Conditions drop-down list is disabled. Refer to Figure 4-10 on page 43.  *Figure 4-10: L4 Conditions*

Table 4-6: Fields for Creating a New Map

Parameter	Description
Map Rules	**e.** (Optional) In the Priority and Action Set box, assign a priority and action set. **f.** (Optional) In the Rule Comment box, enter a comment for the rule. **NOTE:** Repeat steps **b** through **f** to add more conditions. **NOTE:** Repeat steps **a** through **f** to add nested rules.

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

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

   NOTE: The maps saved in the Map Library can be reused in any monitoring session present in the VPC.
7. Click **OK**.

To edit or delete a map, click a map and select **Details** to edit the map or **Delete** to delete the map as shown in Figure 4-11 on page 44.

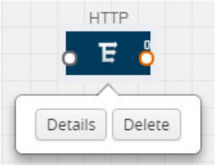


Figure 4-11: Editing or Deleting a Map

Click the **Show Targets** button to view the monitoring targets highlighted in orange. Refer to Figure 4-12 on page 44.

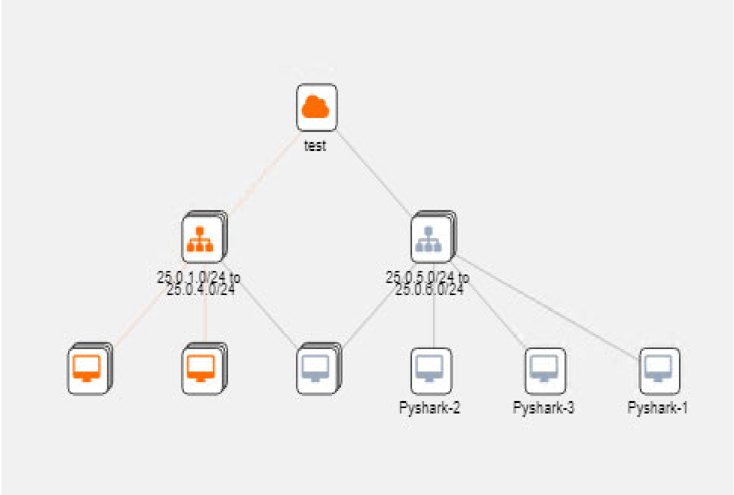
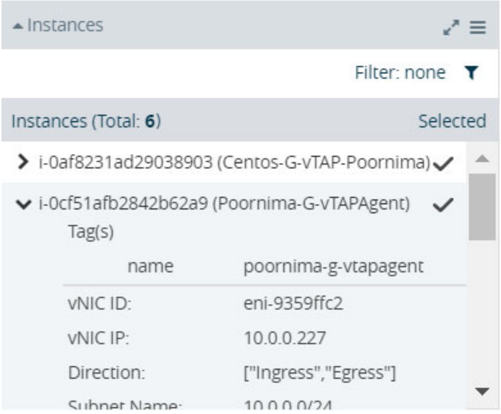


Figure 4-12: Viewing the Topology

Click on ⤢ to expand the **Targets** dialog box. Click on ≡ to change the view from topology to viewing the instance names. To view more details about the instance tag name, direction of tapping, and so on, click the arrow next to the instance name. Refer to Figure 4-13 on page 45.



Instances

Filter: none

Instances (Total: 6) Selected

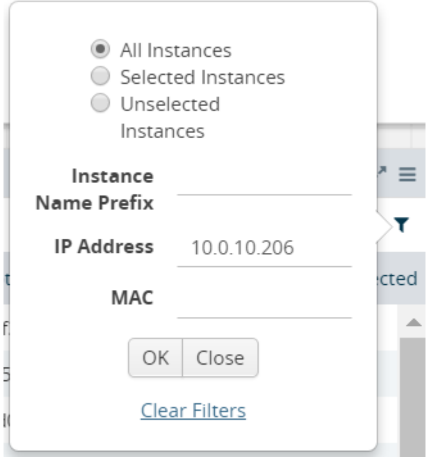
- i-0af8231ad29038903 (Centos-G-vTAP-Poornima) ✓
- i-0cf51afb2842b62a9 (Poornima-G-vTAPAgent) ✓

Tag(s)

name	poornima-g-vtapagent
vNIC ID:	eni-9359ffc2
vNIC IP:	10.0.0.227
Direction:	["Ingress","Egress"]
Subnet Name:	10.0.0.0/24

Figure 4-13: Viewing Instance Details

Filter the instances based on the Instance Name Prefix, IP address, or the MAC address. Refer to Figure 4-14 on page 45.



- ● All Instances
- ○ Selected Instances
- ○ Unselected Instances

Instance Name Prefix	
IP Address	10.0.10.206
MAC	

Figure 4-14: Filtering the instances

Agent Pre-filtering

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

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

Agent Pre-filtering Guidelines

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

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

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

Agent Pre-filtering Capabilities and Benefits

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

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

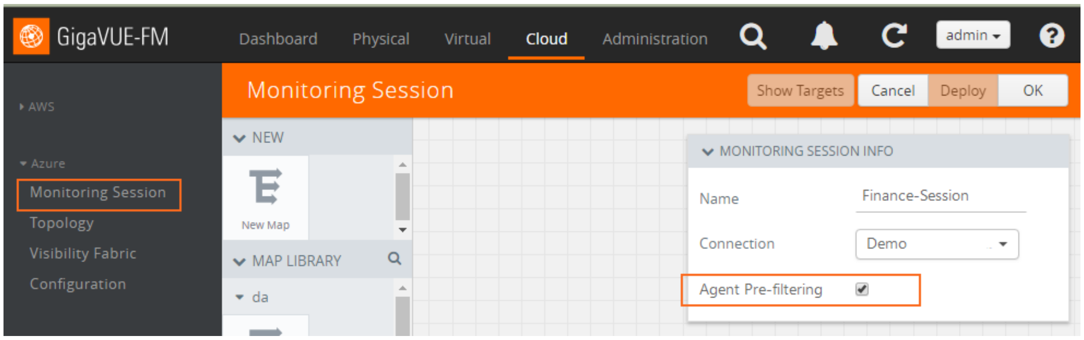
Enable/Disable G-vTAP Agent Pre-filtering

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

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

1. **Cloud > AWS > Monitoring Session**.
2. Open a monitoring session by doing one of the following:
   a. Click **New** to create a new session.

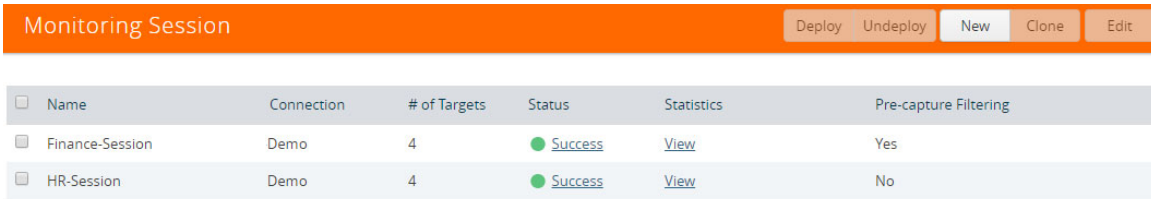
b. Click the check box next to a session and then click **Edit** to edit an existing session.



Name: Finance-Session
Connection: Demo
Agent Pre-filtering ☑

Figure 4-15: Monitoring Session

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



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

Add Applications to Monitoring Session

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

- *Sampling* on page 47
- *Slicing* on page 49
- *Masking* on page 51
- *NetFlow* on page 52

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

Sampling

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

To add a sampling application:

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

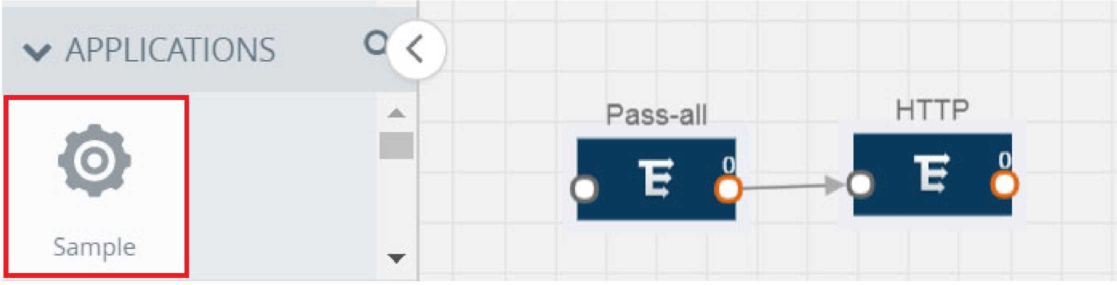


Figure 4-16: Dragging the Sample Application

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

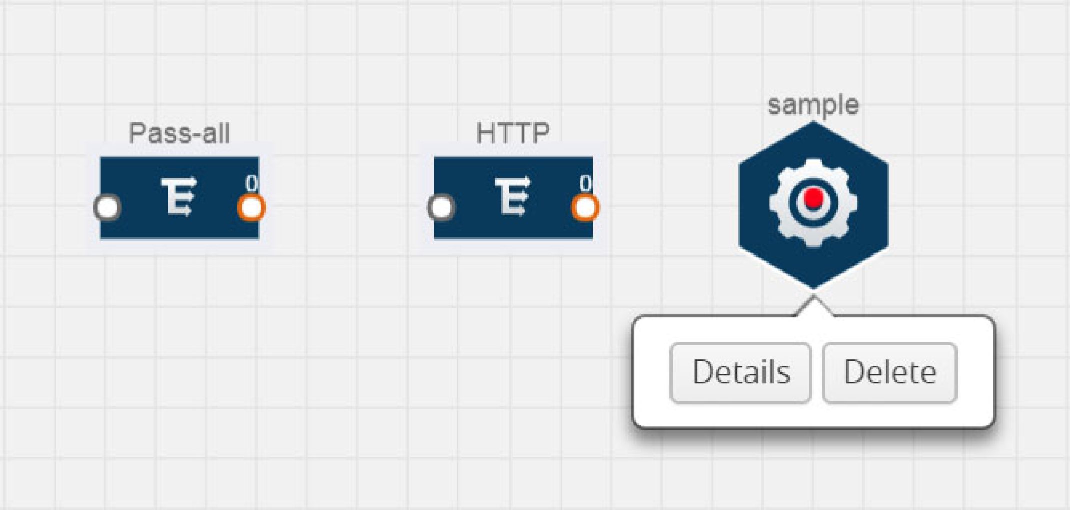
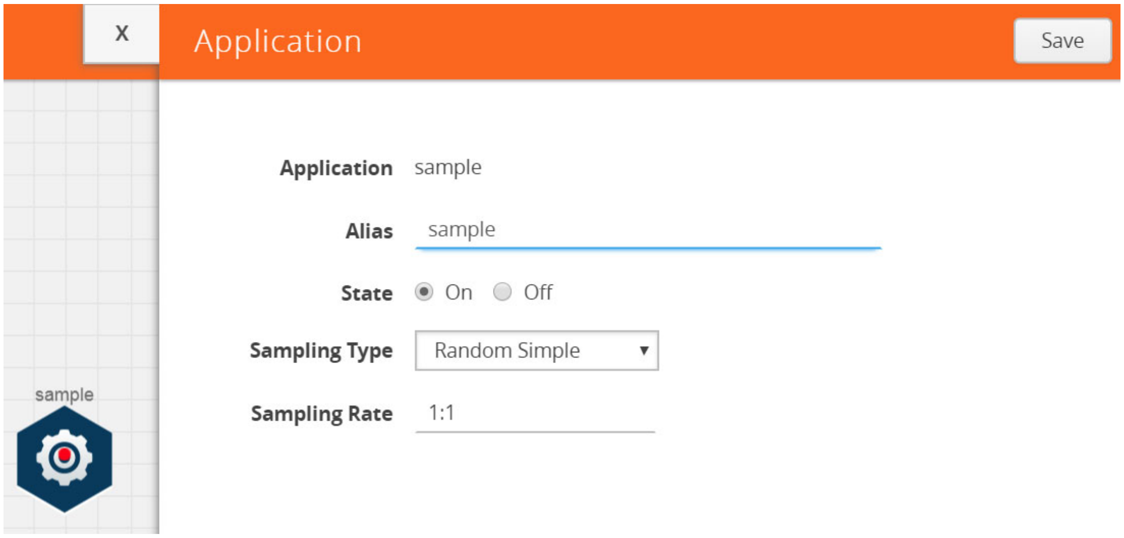


Figure 4-17: Selecting Details

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



Application

Application	sample
Alias	sample
State	● On ○ Off
Sampling Type	Random Simple ▾
Sampling Rate	1:1

Figure 4-18: Viewing Sample Application Quick View

4. For State, select the **On** check box to determine that the application is sampling packets randomly. Select the **Off** check box to determine that the application is not

currently sampling the packets. The state can be changed at anytime whenever required.

5. From the Sampling Type drop-down list, select the type of sampling:
   - **Random Simple** — The first packet is selected randomly. The subsequent packets are also selected randomly based on the rate specified in the **Sampling Rate** field.

     For example, if the first packet selected is 5 and the sampling rate is 1:10, after the 5th packet a random 10 packets are selected for sampling.
   - **Random Systematic** —The first packet is selected randomly. Then, every nth packet is selected, where n is the value specified in the **Sampling Rate** field.

     For example, if the first packet selected is 5 and the sampling rate is 1:10, then every 10th packet is selected for sampling: 15, 25, 35, and so on.
6. In the **Sampling Rate** field, enter the ratio of packets to be selected. The default ratio is 1:1.
7. Click **Save**.

Slicing

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

To add a slicing application:

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

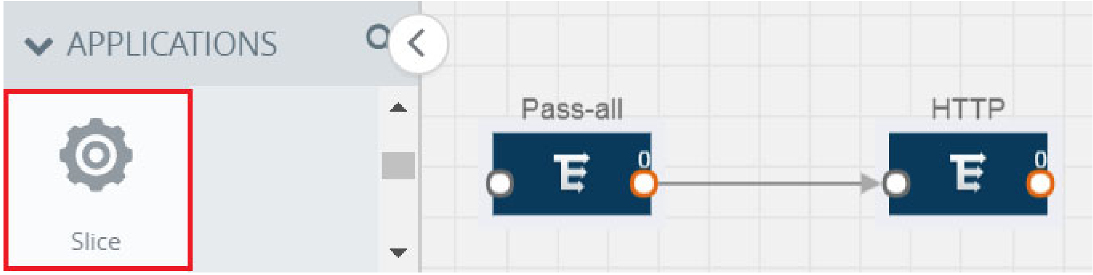


Figure 4-19: Dragging the Slice Application

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

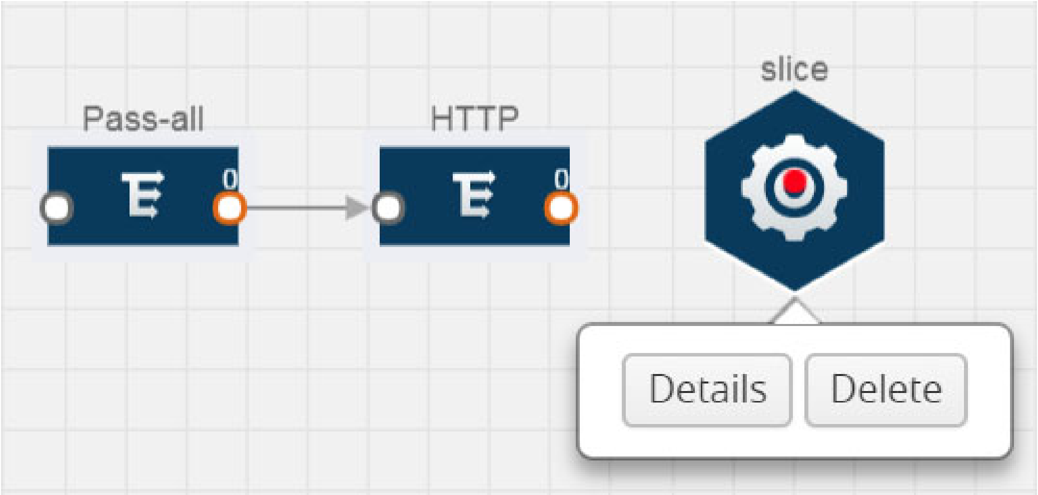
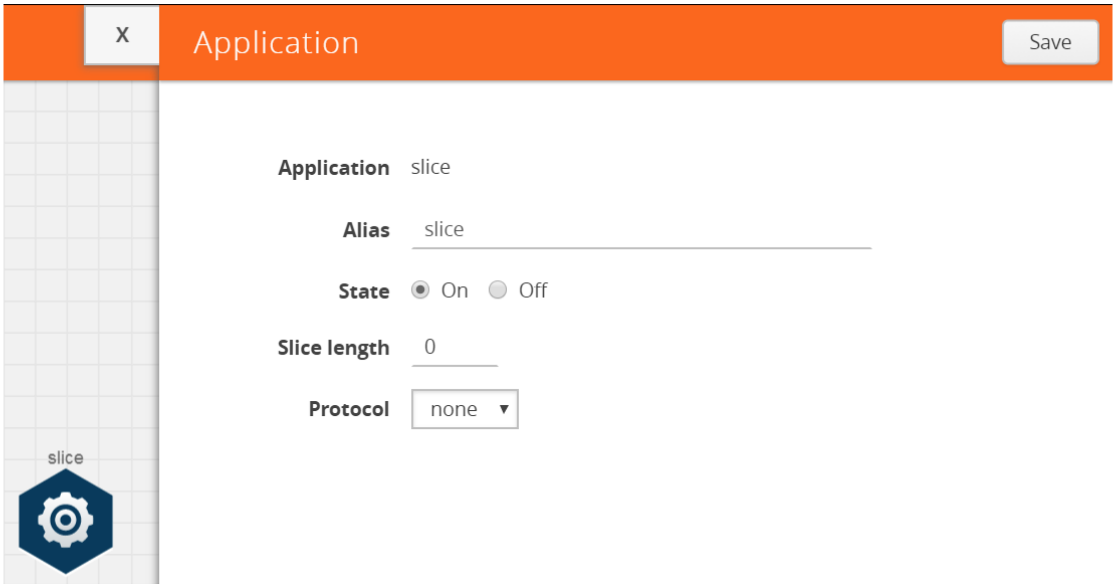


Figure 4-20: Selecting Details

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



Application slice

Alias slice

State ● On ○ Off

Slice length 0

Protocol none ▾

Figure 4-21: Viewing Slice Application Quick View

4. For State, select the **On** check box to determine that the application is slicing packets. Select the **Off** check box to determine that the application is not currently slicing the packets. The state can be changed at a later time whenever required.
5. In the Slice Length field, specify the length of the packet that must be sliced.
6. From the Protocol drop-down list, specify an optional parameter for slicing the specified length of the protocol. The options are as follows:
    - None
    - IPv4
    - IPv6
    - UDP

- TCP

7. Click **Save**.

Masking

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

To add a masking application:

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

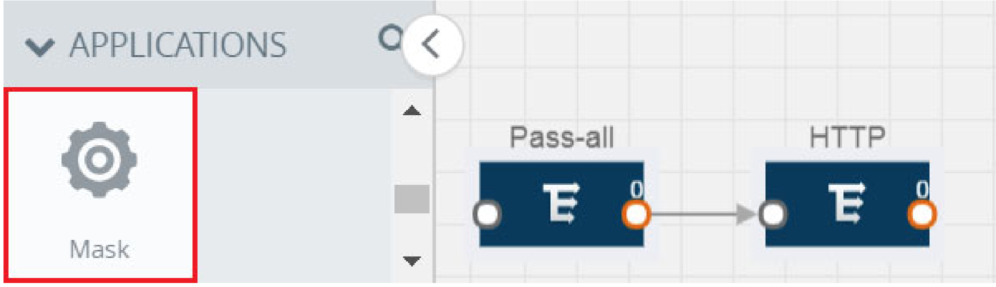


Figure 4-22: Dragging the Mask Application

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

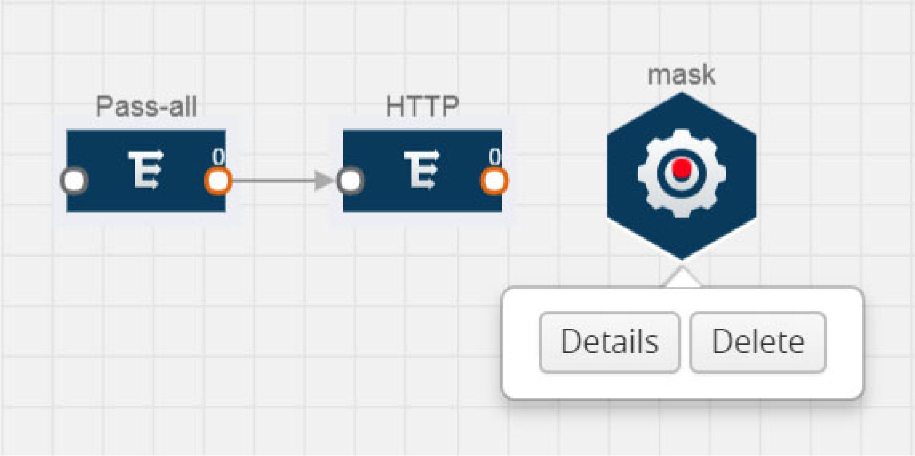
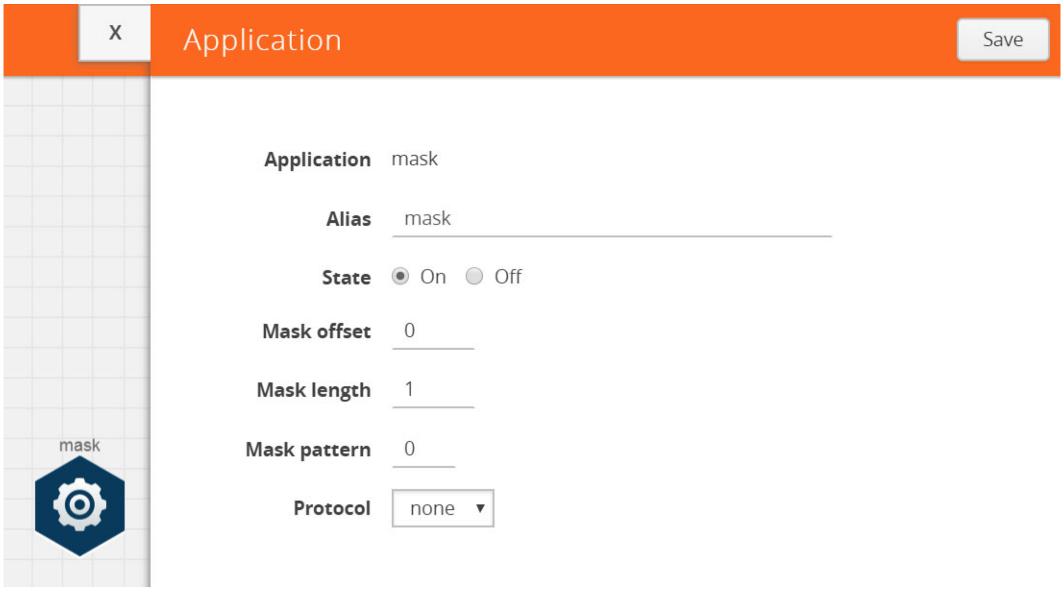


Figure 4-23: Selecting Details

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



Application mask

Alias mask

State ● On ○ Off

Mask offset 0

Mask length 1

Mask pattern 0

Protocol none ▾

Figure 4-24: Viewing Mask Application Quick View

4. For State, select the **On** check box to determine that the application is masking packets. Select the **Off** check box to determine that the application is not currently masking the packets. The state can be changed at anytime whenever required.
5. In the Mask offset field, enter the offset from which the application should start masking data following the pattern specified in the Pattern field.

   The value can be specified in terms of either a static offset, that is, from the start of the packet or a relative offset, that is, from a particular protocol layer as specified in the Protocol field.
6. In the Mask length field, enter the length of the packet that must be masked.
7. In the Mask pattern field, enter the pattern for masking the packet. The value of the pattern is from 0 to 255.
8. From the Protocol drop-down list, specifies an optional parameter for masking packets on the data coming from the selected protocol.
9. Click **Save**.

NetFlow

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

The following are the key benefits of NetFlow application:

- Compresses network information into a single flow record.
- Facilitates up to 99% reduction in data transferred.
- Accelerates the migration of mission-critical workloads to AWS.

- Provides summarized information on traffic source and destination, congestion, and class of service.
- Identifies and classifies DDOS attacks, viruses, and worms in real-time.
- Secures network against internal and external threats.
- Identifies top consumers and analyzes their statistics.
- Reduces the cost of security monitoring.
- Analyzes the network flows based on algorithms and behavior rather than signature matching.
- Analyzes east-west traffic between flows within and across VPCs.

The NetFlow application contains key elements that specify what to match in the flow, such as all packets with the same source and destination port, or the packets that come in on a particular interface. For information about Match/Key fields, refer to *Match/Key Fields* on page 54. A NetFlow record is the output generated by NetFlow. A flow record contains non-key elements that specify what information to collect for the flow, such as when the flow started or the number of bytes in the flow. For information about Match/Key fields, refer to *Collect/Non-Key Fields* on page 56.

Figure 4-25 on page 53 shows an example of a NetFlow application created on a GigaVUE V Series node in the monitoring session.

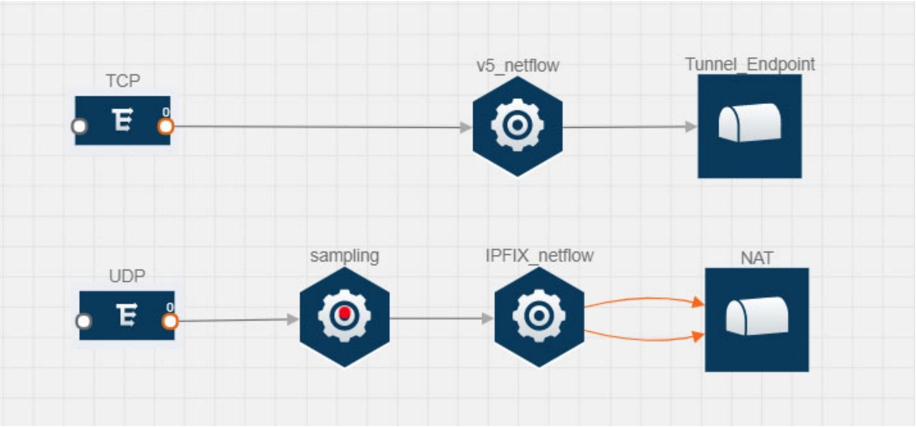


Figure 4-25: NetFlow on GigaVUE V Series Node

The NetFlow record generation is performed on GigaVUE V Series node running the NetFlow application. In Figure 4-25 on page 53, incoming packets from G-vTAP agents are sent to the GigaVUE V Series node. In the GigaVUE V Series node, one map sends the TCP packet to the version 5 NetFlow application. Another map sends the UDP packet to a sampling application. The map rules and applications such as slice, mask, and sample can only be applied prior to sending the data to NetFlow.

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

The flow records can be sent to a tunnel for full packet inspection or to a NAT device for flow inspection. NAT allows the NetFlow records to be directly transmitted to a collector without a tunnel. For more information about NAT, refer to *Network Address Translation (NAT)* on page 62.

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

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

Match/Key Fields

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

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

Table 4-7: Match/Key Elements

Match Type	Description	Supported NetFlow Versions
Data Link		
Destination MAC	Configures the destination MAC address as a key field.	v9 and IPFIX
Egress Dest MAC	Configures the post Source MAC address as a key field.	IPFIX
Ingress Dest MAC	Configures the IEEE 802 destination MAC address as a key field.	IPFIX
Source MAC	Configures the IEEE 802 source MAC address as a key field.	v9 and IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP message as a key field.	v9 and IPFIX
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a key field.	IPFIX
IPv4 ICMP Type	Configures the type and code of the IPv4 ICMP message as a key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a key field.	IPFIX

Table 4-7: Match/Key Elements

Match Type	Description	Supported NetFlow Versions
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9 and IPFIX
IP DSCP	Configures the value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field as a key field.	IPFIX
IP Header Length	Configures the length of the IP header as a key field.	IPFIX
IP Precedence	Configures the value of the IP Precedence as a key field.	IPFIX
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9 and IPFIX
IP Total Length	Configures the total length of the IP packet as a key field.	IPFIX
IP TTL	For IPv4, configures the value of Time to Live (TTL) as a key field. For IPv6, configures the value of the Hop Limit field as a key field.	IPFIX
IP Version	Configures the IP version field in the IP packet header as a key field.	v9 and IPFIX
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9 and IPFIX
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9 and IPFIX
IPv6 ICMP Code	Configures the code of the IPv6 ICMP message as a key field.	IPFIX
IPv6 ICMP Type	Configures the type of the IPv6 ICMP message as a key field.	IPFIX
IPv6 ICMP Type Code	Configures the type and code of the IPv6 ICMP message as a key field.	IPFIX
IPv6 Payload Length	Configures the value of the payload length field in the IPv6 header as a key field.	IPFIX
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9 and IPFIX
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a key field.	v9 and IPFIX

Table 4-7: Match/Key Elements

Match Type	Description	Supported NetFlow Versions
L4 Src Port	Configures the source port identifier in the transport header as a key field.	v9 and IPFIX
TCP AcK Number	Configures the acknowledgment number in the TCP header as a key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP header as a key field.	IPFIX
TCP Src Port	Configures the source port identifier in the TCP header as a key field.	IPFIX
TCP Urgent	Configures the urgent pointer in the TCP header as a key field.	IPFIX
TCP Window Size	Configures the window field in the TCP header as a key field.	IPFIX
UDP Dest Port	Configures the destination port identifier in the UDP header as a key field.	IPFIX
UDP Src Port	Configures the source port identifier in the TCP header as a key field.	IPFIX

Collect/Non-Key Fields

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

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

Table 4-8: Collect/Non-Key Elements

Match Type	Description	Supported NetFlow Versions
Counter		
Byte Count	Configures the number of octets since the previous report in incoming packets for the current flow as a non-key field.	v9 and IPFIX
Packet Count	Configures the number of incoming packets since the previous report for this flow as a non-key field.	v9 and IPFIX
Data Link		
Destination MAC	Configures the destination MAC address as a non-key field.	v9 and IPFIX

Table 4-8: Collect/Non-Key Elements

Match Type	Description	Supported NetFlow Versions
Egress Des MAC	Configures the post source MAC address as a non-key field.	IPFIX
Ingress Des MAC	Configures the IEEE 802 destination MAC address as a non-key field.	IPFIX
Source MAC	Configures the IEEE 802 source MAC address as a non-key field.	v9 and IPFIX
Timestamp		
Flow End Millisec	Configures the absolute timestamp of the last packet of current flow in milliseconds as a non-key field.	IPFIX
Flow End Sec	Configures the flow start SysUp time as a non-key field.	IPFIX
Flow End Time	Configures the flow end SysUp time as a non-key field.	v9 and IPFIX
Flow Start Millisec	Configures the value of the IP Precedence as a non-key field.	IPFIX
Flow Start Sec	Configures the absolute timestamp of the first packet of this flow as a non-key field.	IPFIX
Flow Startup Time	Configures the flow start SysUp time as a non-key field.	v9 and IPFIX
Flow		
Flow End Reason	Configures the reason for Flow termination as a non-key field.	IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP message as a non-key field.	v9 and IPFIX
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 ICMP Type	Configures the type of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a non-key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a non-key field.	IPFIX
Network		

Table 4-8: Collect/Non-Key Elements

Match Type	Description	Supported NetFlow Versions
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9
IP Version	Configures the IP version field in the IP packet header as a key field.	v9
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a non-key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport header as a non-key field.	v9 and IPFIX
TCP AcK Number	Configures the acknowledgment number in the TCP header as a non-key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a non-key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a non-key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a non-key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP header as a non-key field.	IPFIX
TCP Src Port	Configures the source port identifier in the TCP header as a non-key field.	IPFIX
TCP Urgent	Configures the urgent pointer in the TCP header as a non-key field.	IPFIX
TCP Window Size	Configures the window field in the TCP header as a non-key field.	IPFIX
UDP Dest Port	Configures the destination port identifier in the UDP header as a non-key field.	IPFIX
UDP Src Port	Configures the source port identifier in the UDP header as a non-key field.	IPFIX

Add Version 5 NetFlow Application

To add a version 5 NetFlow application:

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

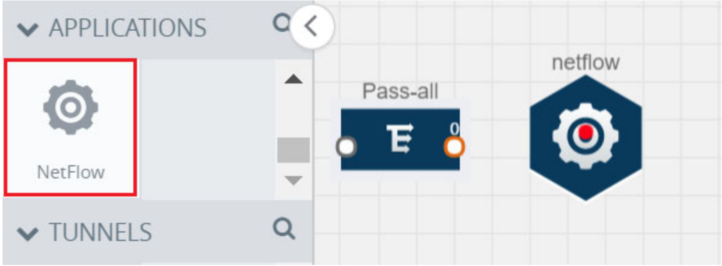


Figure 4-26: Dragging the NetFlow Application

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

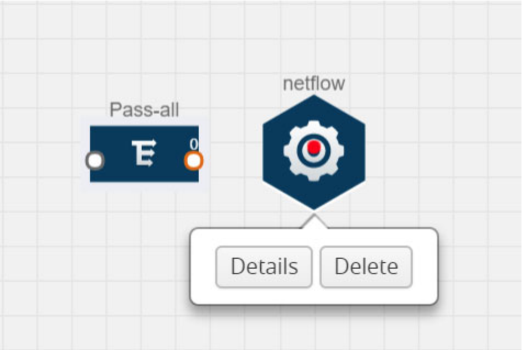
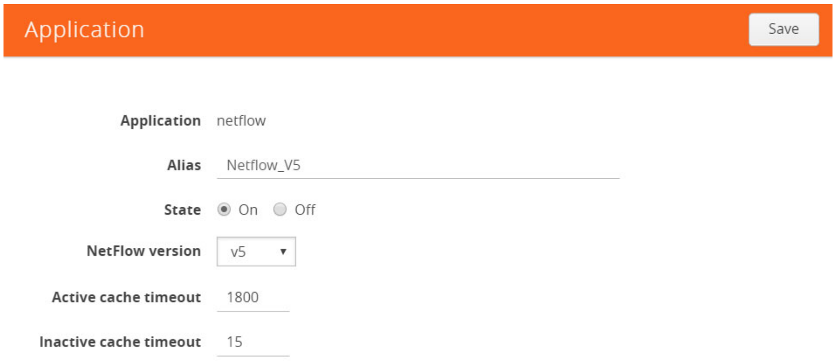


Figure 4-27: Selecting Details

3. In the **Alias** field, enter a name for the v5 NetFlow application.



Application	netflow
Alias	Netflow_V5
State	● On ○ Off
NetFlow version	v5 ▾
Active cache timeout	1800
Inactive cache timeout	15

Figure 4-28: Viewing v5 NetFlow Application Quick View

4. For State, select the **On** check box to determine that the application is currently running. Select the **Off** check box to determine that the application is currently not running. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select v5.

6. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.
7. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.
8. Click **Save**.

For some examples demonstrating the NetFlow application configuration in the GigaVUE V Series nodes, refer to *NetFlow Examples* on page 64.

Add Version 9 and IPFIX NetFlow Application

To add a v9 and IPFIX NetFlow application:

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

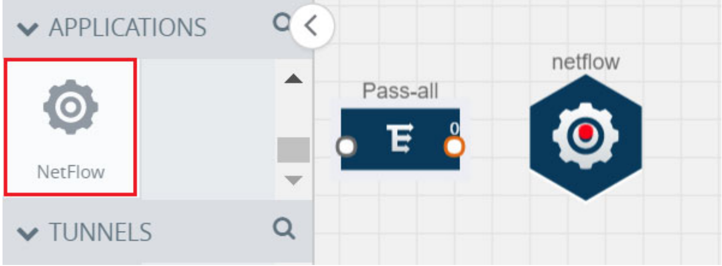


Figure 4-29: Dragging the NetFlow Application

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

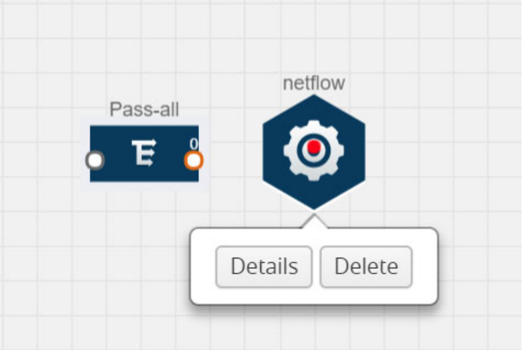
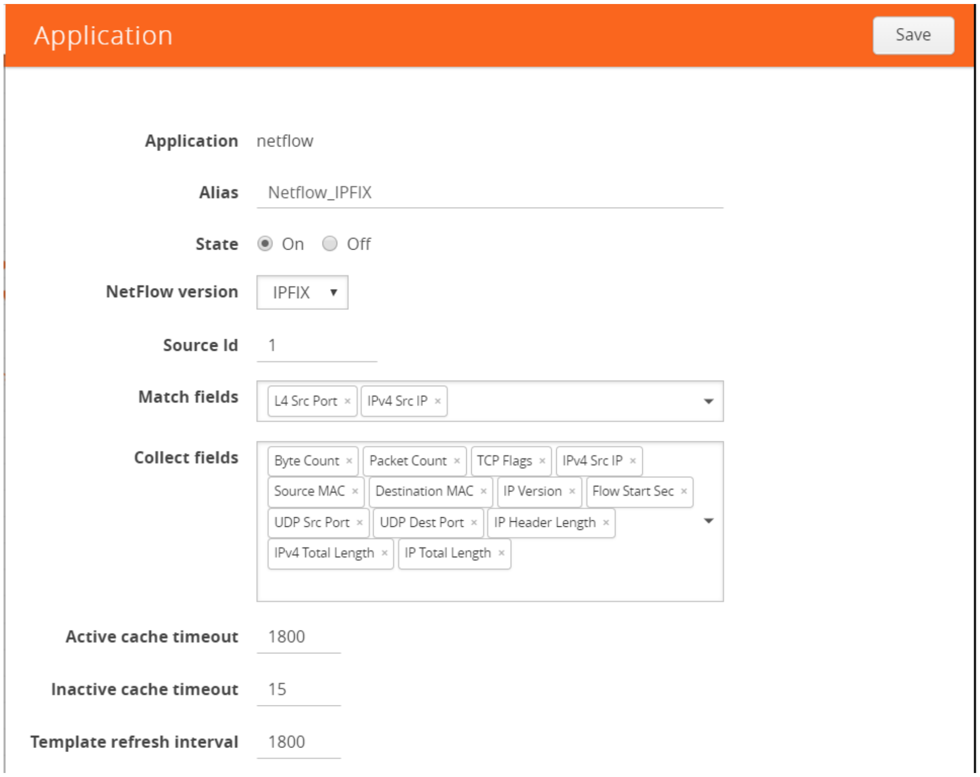


Figure 4-30: Selecting NetFlow Details

3. In the **Alias** field, enter a name for the NetFlow application.



Application	netflow
Alias	Netflow_IPFIX
State	● On ○ Off
NetFlow version	IPFIX ▾
Source Id	1
Match fields	L4 Src Port × IPv4 Src IP ×
Collect fields	Byte Count × Packet Count × TCP Flags × IPv4 Src IP × Source MAC × Destination MAC × IP Version × Flow Start Sec × UDP Src Port × UDP Dest Port × IP Header Length × IPv4 Total Length × IP Total Length ×
Active cache timeout	1800
Inactive cache timeout	15
Template refresh interval	1800

Figure 4-31: Viewing NetFlow Application Quick View

4. For State, select the **On** check box to determine that the application is generating NetFlow records from the packets coming from the G-vTAP agents. Select the **Off** check box to determine that the application is not currently generating NetFlow records. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select the version you want to use to generate the NetFlow records. The default version selected is v5.
6. In the **Source ID** field, enter the observation domain to isolate the traffic. The NetFlow application uses source ID to segregate the records into categories. For example, you can assign source ID 1 for traffic coming over TCP. This results in generating a separate NetFlow record for TCP data. Similarly, you can assign Source ID 2 for traffic coming over UDP. This results in generating a separate NetFlow record for UDP data.
7. From the **Match fields** drop-down list, select the parameters that identify what you want to collect from the incoming packets. The Match fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to *Match/ Key Fields* on page 54.
8. From the **Collect fields** drop-down list, select the parameters that identify what you want to collect from the NetFlow records. The Collect fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to *Collect/Non-Key Fields* on page 56.
9. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.

10. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.
11. In **Template refresh interval**, enter the frequency at which the template must be sent to the tool. The default value is 1800 seconds.
12. Click **Save**.

For some examples demonstrating the NetFlow application configuration in the GigaVUE V Series nodes, refer to *NetFlow Examples* on page 64.

Network Address Translation (NAT)

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

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

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

Add NAT

To add a NAT device:

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

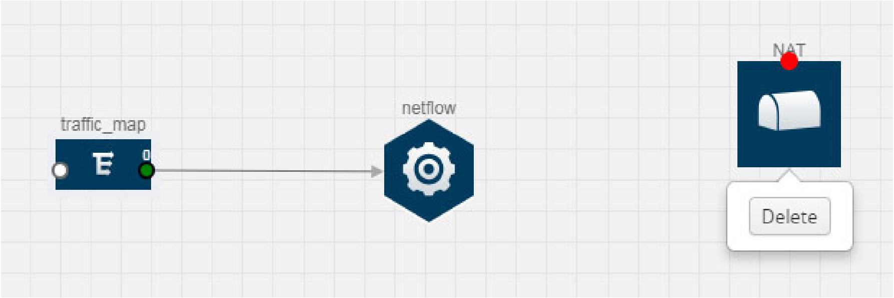
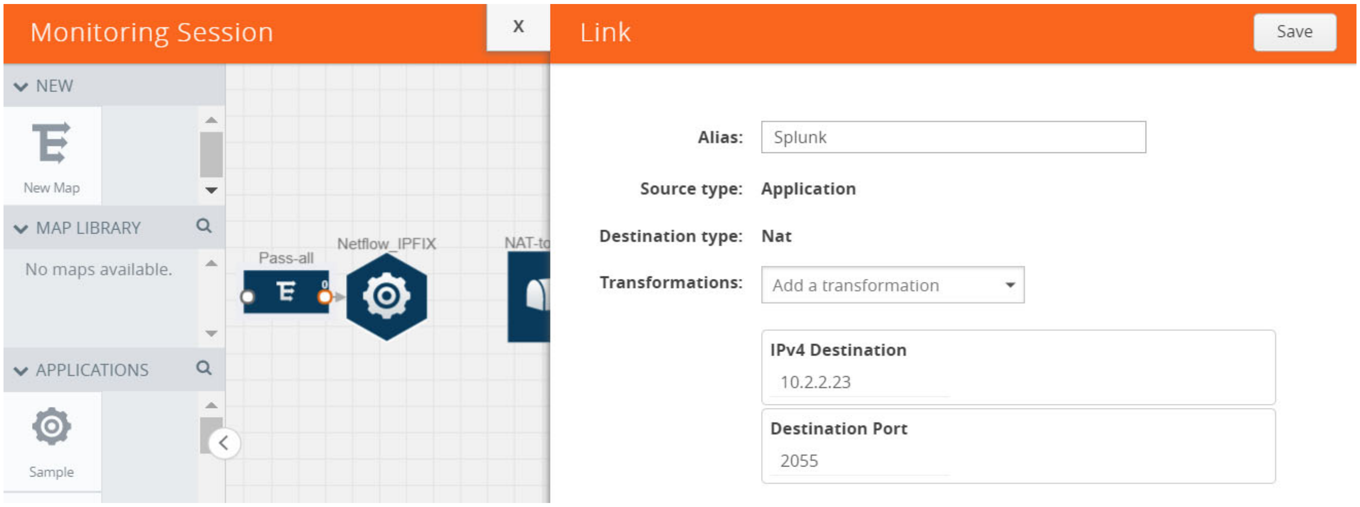


Figure 4-32: Adding NAT

Link NetFlow Application to NAT

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

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



Alias: Splunk

Source type: Application

Destination type: Nat

Transformations: Add a transformation

IPv4 Destination: 10.2.2.23

Destination Port: 2055

Figure 4-33: Creating a Link from NetFlow to NAT

2. In the **Alias** field, enter a name for the link.
3. From the **Transformations** drop-down list, select any one of the header transformations:
   - IPv4 Destination
   - ToS
   - Destination Port

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

4. In **IPv4 Destination**, enter the IP address of the NetFlow collector.
5. (Optional) By default, the Destination Port is 2055. To change the destination port, enter a port number.
6. Click **Save**. The transformed link is displayed in Orange.

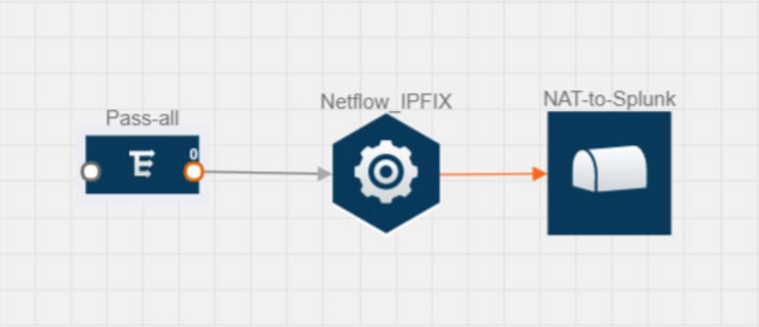


Figure 4-34: Linking NetFlow to NAT

7. Repeat steps 7 to 10 to send additional NetFlow records to NAT.

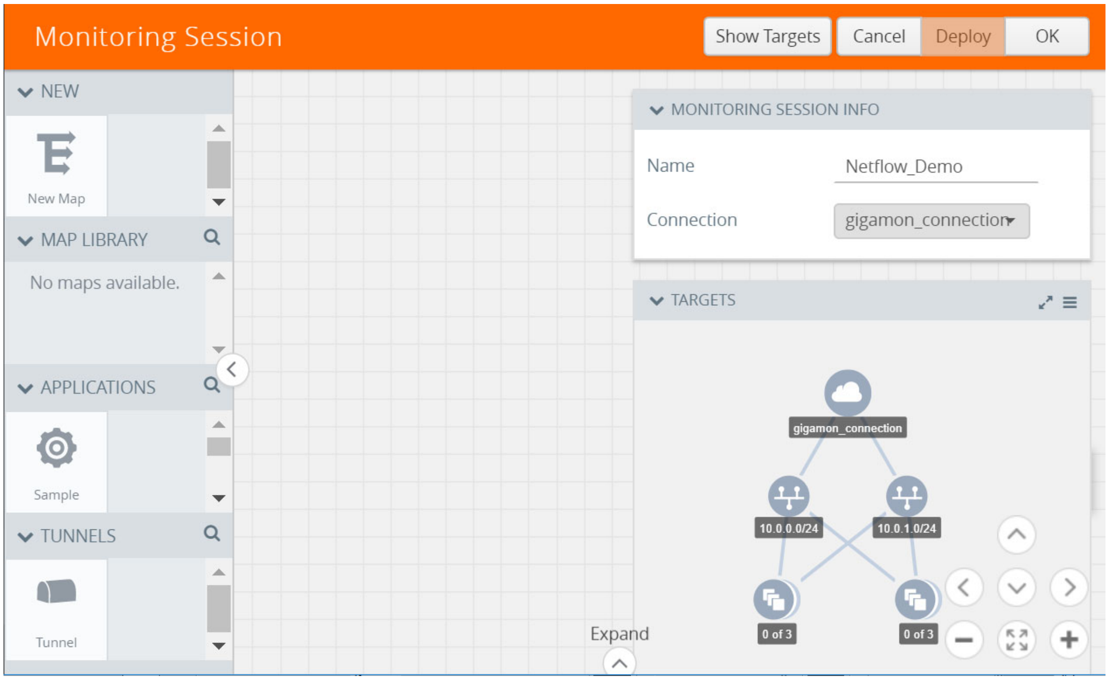
NetFlow Examples

This section provides an example to demonstrate the NetFlow application configuration in the GigaVUE V Series nodes. Refer *Example 1* on page 64 below.

Example 1

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

1. Create a monitoring session. For steps, refer to *Create Monitoring Session* on page 37.



Monitoring Session

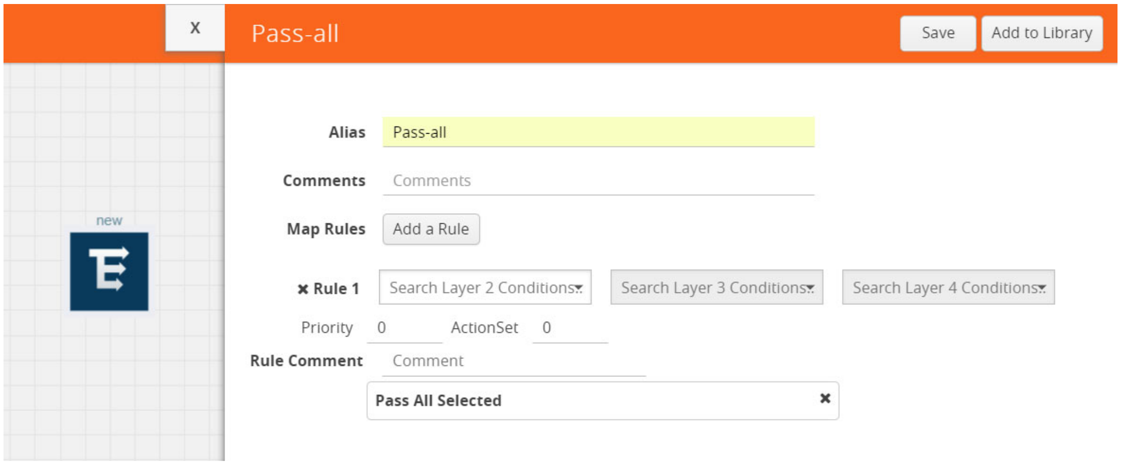
MONITORING SESSION INFO

Name: Netflow_Demo

Connection: gigamon_connection

Figure 4-35: Creating a Monitoring Session

2. In the monitoring session, create a Pass all map. A pass all map sends all the traffic received from the G-vTAP agents to the tunnel endpoint or NAT. For steps, refer to *Clone Monitoring Session* on page 38.



Alias: Pass-all

Comments: Comments

Map Rules: Add a Rule

× Rule 1: Search Layer 2 Conditions | Search Layer 3 Conditions | Search Layer 4 Conditions

Priority 0 ActionSet 0

Rule Comment: Comment

Pass All Selected ×

Figure 4-36: Creating a Pass All Map

3. Drag and drop a tunnel from **Tunnels**. A tunnel encapsulates the flow records and then sends them to the tools for full packet inspection.

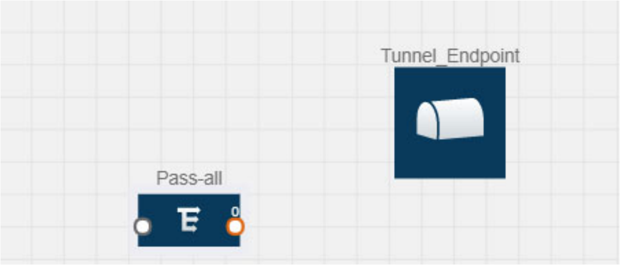


Figure 4-37: Adding a Tunnel

4. Create a link from the Pass-all map to the tunnel endpoint. The traffic from the Pass-all map is forwarded to the tunnel endpoint that is connected to a tool.

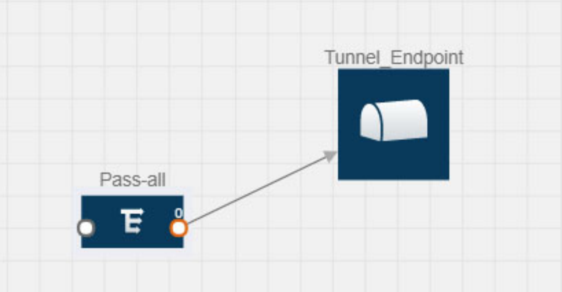


Figure 4-38: Creating a Link from Pass-all Map to Tunnel_Endpoint

5. Drag and drop a v5 NetFlow application.

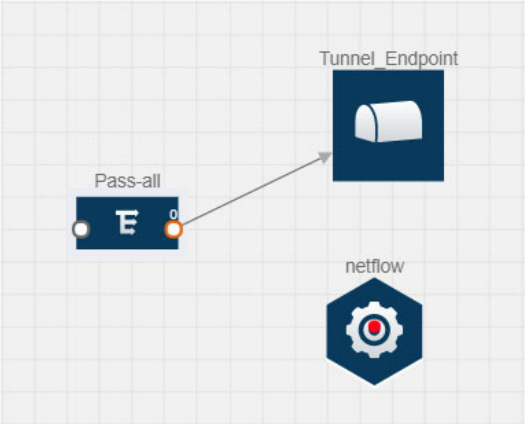
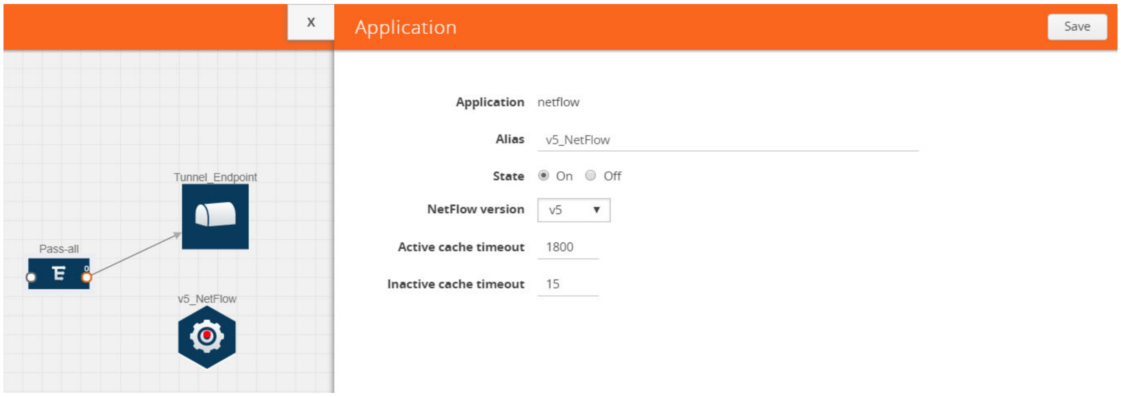


Figure 4-39: Adding a link from Pass-all Map to Tunnel_Endpoint

6. Click the NetFlow application and select **Details**. The Application quick view is displayed. For steps to configure the v5 NetFlow application, refer to *Add Version 5 NetFlow Application* on page 59.



Application netflow

Alias v5_NetFlow

State ● On ○ Off

NetFlow version v5 ▼

Active cache timeout 1800

Inactive cache timeout 15

Figure 4-40: Configuring the NetFlow Application

7. Create a link from the Pass all map to the v5 NetFlow application.

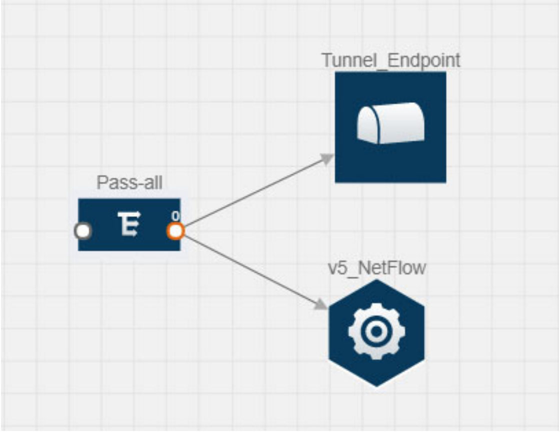


Figure 4-41: Adding a link from Pass-all Map to v5_NetFlow

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

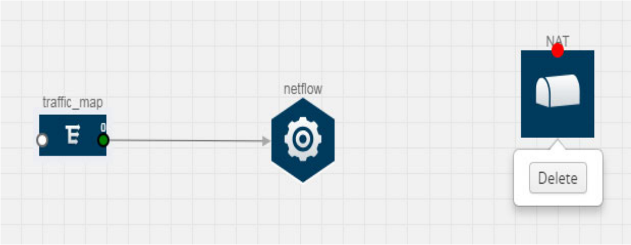
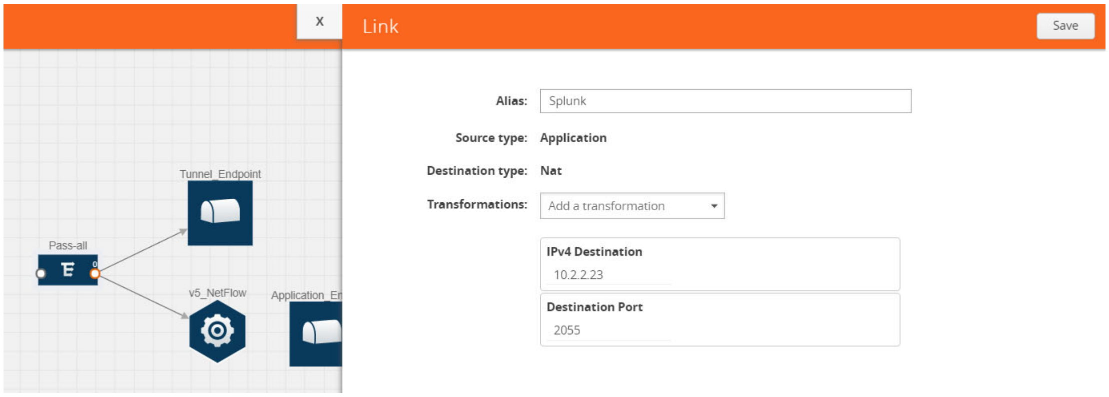


Figure 4-42: Adding a NAT Device

9. Create a link from the v5 NetFlow application to NAT. The link must be configured with the destination IP address of the NetFlow collector and the GigaVUE V Series node interface. For steps to configure the link, refer to *Link NetFlow Application to NAT* on page 63.



Alias: Splunk

Source type: Application

Destination type: Nat

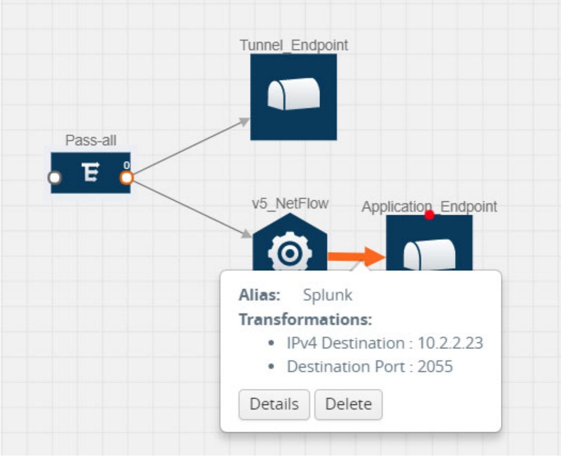
Transformations: Add a transformation

IPv4 Destination
10.2.2.23

Destination Port
2055

Figure 4-43: Adding a Link from v5 NetFlow Application to NAT

10. Click on the link created from the v5 NetFlow application to NAT. The information about the NetFlow collector destination IP and port is displayed.



Alias: Splunk

Transformations:

- IPv4 Destination : 10.2.2.23
- Destination Port : 2055

Figure 4-44: Viewing the Transformation Dialog Box

Deploy Monitoring Session

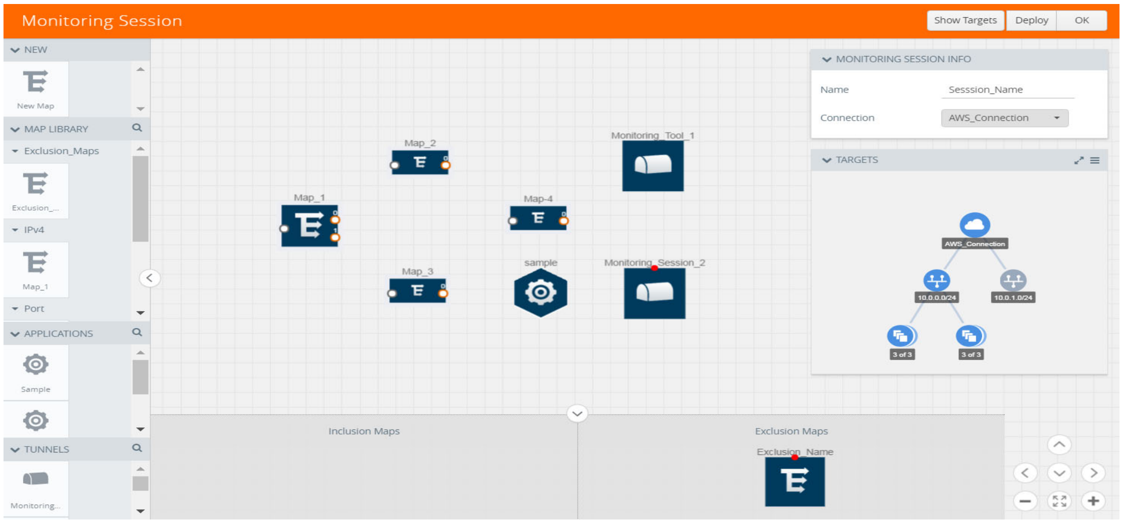
To deploy the monitoring session:

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

   NOTE: For information about adding applications to the workspace, refer to *Add Applications to Monitoring Session* on page 47.

4. Drag and drop one or more tunnels from the TUNNELS section.

   Figure 4-45 on page 68 illustrates three maps, one exclusion map, one application, and two tunnel endpoints dragged and dropped to the workspace.



Name Session_Name

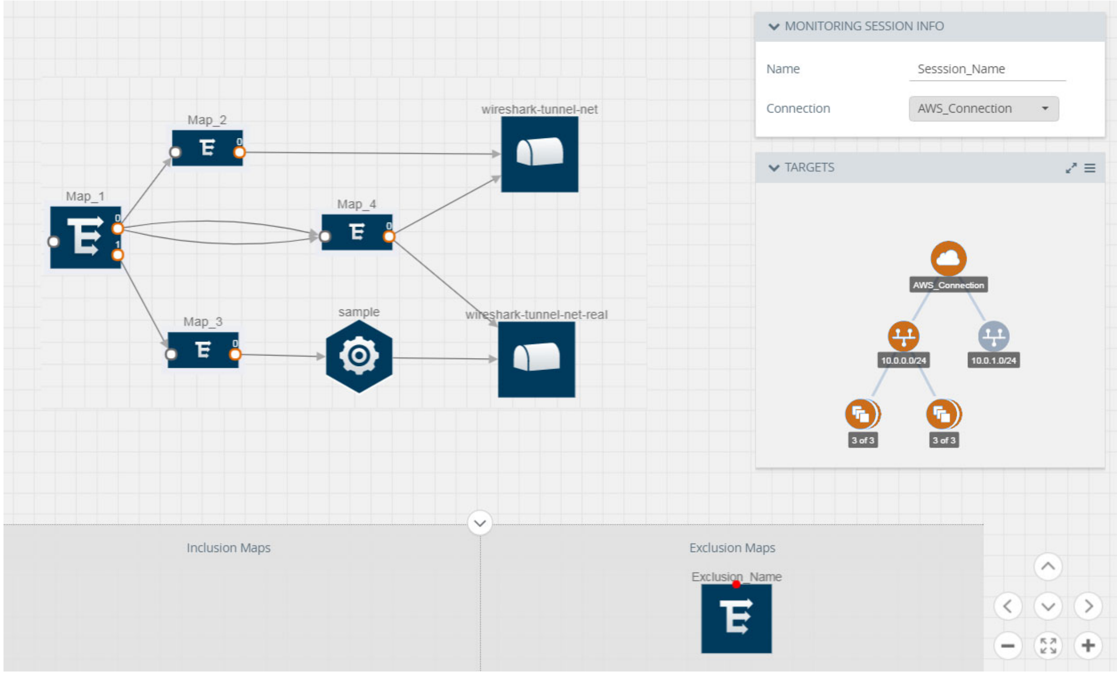
Connection AWS_Connection

Figure 4-45: Dragging and Dropping the Maps, Applications, and Monitoring Tools

NOTE: You can add up to 8 links from a single map to different maps, applications, or monitoring tools.

5. Hover your mouse on the map, click the red dot, and drag the link over to another map, application, or tunnel. You can drag more than one link from a map to the destination. On these links, you can apply link transformation to alter the packets. Refer to Figure 4-46 on page 69. For information about adding link transformation, refer to *Add Header Transformations* on page 70.
6. Hover your mouse on the application, click the red dot, and drag the link (arrow) over to the tunnel endpoints.

In Figure 4-46 on page 69, the traffic matching the rules in each action set is routed to maps, applications, or monitoring tools.



MONITORING SESSION INFO

Name: Sesssion_Name

Connection: AWS_Connection

Figure 4-46: Connecting the Maps, Applications, and Monitoring Tools

7. Click **Show Targets** to view details about the subnets and monitoring instances.

   The instances and the subnets that are being monitored are highlighted in orange.

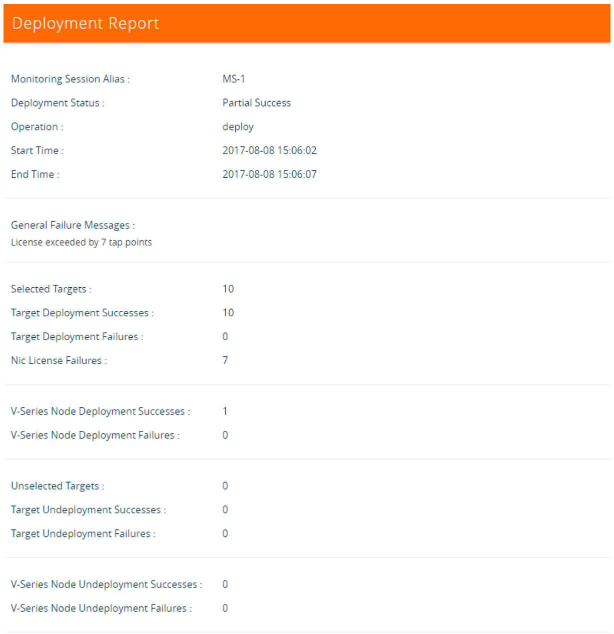
8. Click **Deploy** to deploy the monitoring session.

   The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all GigaVUE V Series nodes and G-vTAP agents.

   If the monitoring session is not deployed properly, then one of the following errors is displayed:

   - Partial Success—The session is not deployed on one or more instances due to G-vTAP or GigaVUE V Series node failure.
   - Failure—The session is not deployed on any of the GigaVUE V Series nodes and G-vTAP agents.

Click on the status link to view the reason for the partial success or failure. Refer to Figure 4-47 on page 70.



Deployment Report

Monitoring Session Alias :	MS-1
Deployment Status :	Partial Success
Operation :	deploy
Start Time :	2017-08-08 15:06:02
End Time :	2017-08-08 15:06:07

General Failure Messages :
License exceeded by 7 tap points

Selected Targets :	10
Target Deployment Successes :	10
Target Deployment Failures :	0
Nic License Failures :	7
V-Series Node Deployment Successes :	1
V-Series Node Deployment Failures :	0
Unselected Targets :	0
Target Undeployment Successes :	0
Target Undeployment Failures :	0
V-Series Node Undeployment Successes :	0
V-Series Node Undeployment Failures :	0

Figure 4-47: Deployment Status

9. Click **View** under Statistics to view and analyze the incoming and outgoing traffic.

You can also do the following in the Monitoring Session page:

- Use the **Redeploy** button to redeploy a monitoring session that is not deployed or partially successful.
- Use the **Undeploy** button to undeploy the selected monitoring session.
- Use the **Clone** button to duplicate the selected monitoring session.
- Use the **Edit** button to edit the selected monitoring session.
- Use the **Delete** button to delete the selected monitoring session.

Add Header Transformations

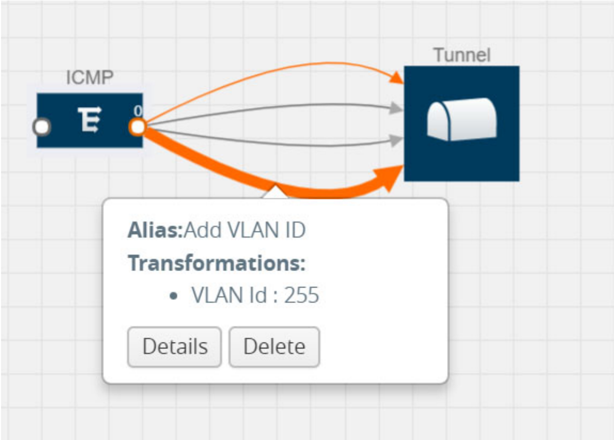
Header transformation is performed on a link in a monitoring session. You can select a link and modify the packet header before they are sent to the destination. The header transformation feature is supported only with GigaVUE V Series node version 1.3-1 and above.

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

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

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

In Figure 4-48 on page 71, the filtered packets from the ICMP map are sent to the same tunnel endpoint in four different links. In each link, you can apply one or more header transformations. A link with the header transformation applied is displayed in orange. When you mouse over the orange link, a detailed information about the alias and the type of transformation is displayed.



Alias: Add VLAN ID
Transformations:
- VLAN Id : 255

Figure 4-48: Action Set with Multiple Links

GigaVUE V Series node supports the following header transformations:

Table 4-9: Header Transformations

Option	Description
MAC Source	Modify the Ethernet source address.
MAC Destination	Modify the Ethernet destination address.
VLAN Id	Specify the VLAN ID.
VLAN PCP	Specify the VLAN priority.
Strip VLAN	Strip the VLAN tag.
IPv4 Source	Specify the IPv4 source address.
IPv4 Destination	Specify the IPv4 destination address.
ToS	Specify the DSCP bits in IPv4 traffic class.
Source Port	Specify the UDP, TCP, or SCTP source port.

Table 4-9: Header Transformations

Option	Description
Destination Port	Specify the UDP, TCP, or SCTP destination port.
Tunnel ID	Specify the tunnel ID. The tunnel ID header transformation can only be applied on the links with the tunnel endpoint destination. Using Tunnel ID header transformation, the filtered packets can be sent to different applications or programs within the same monitoring tool.

To add a header transformation:

1. On the Monitoring Session, click the link and select **Details.** The Link quick view is displayed.

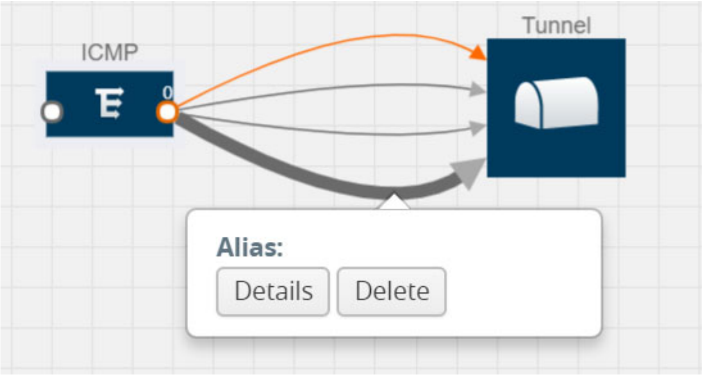
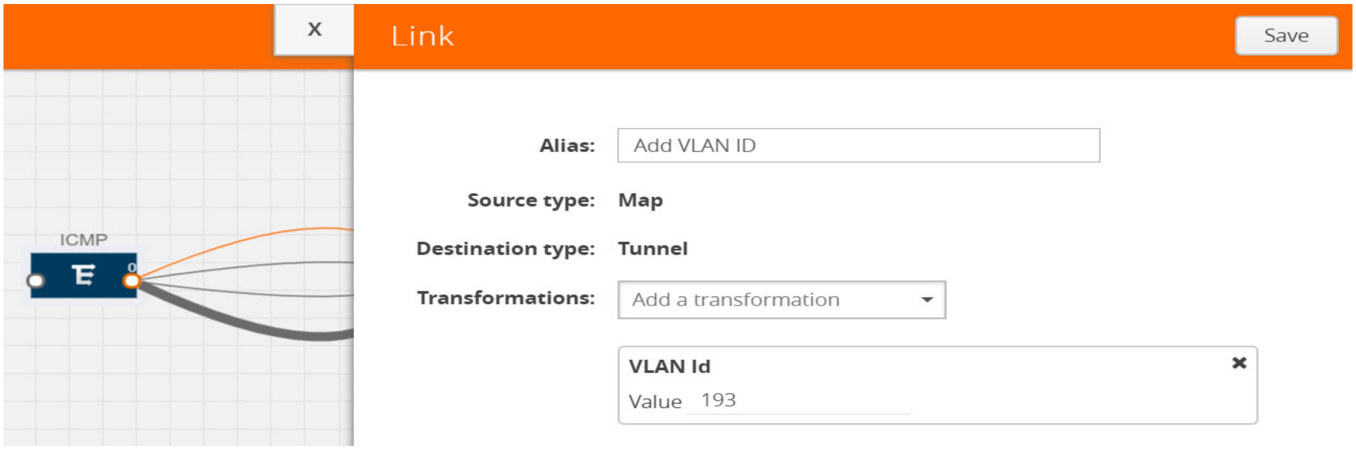


Figure 4-49: Opening the Link Quick View

2. From the **Transformations** drop-down list, select one or more header transformations.

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



Alias: Add VLAN ID

Source type: Map

Destination type: Tunnel

Transformations: Add a transformation

VLAN Id ✖
Value 193

Figure 4-50: Adding Transformation

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

View Statistics

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

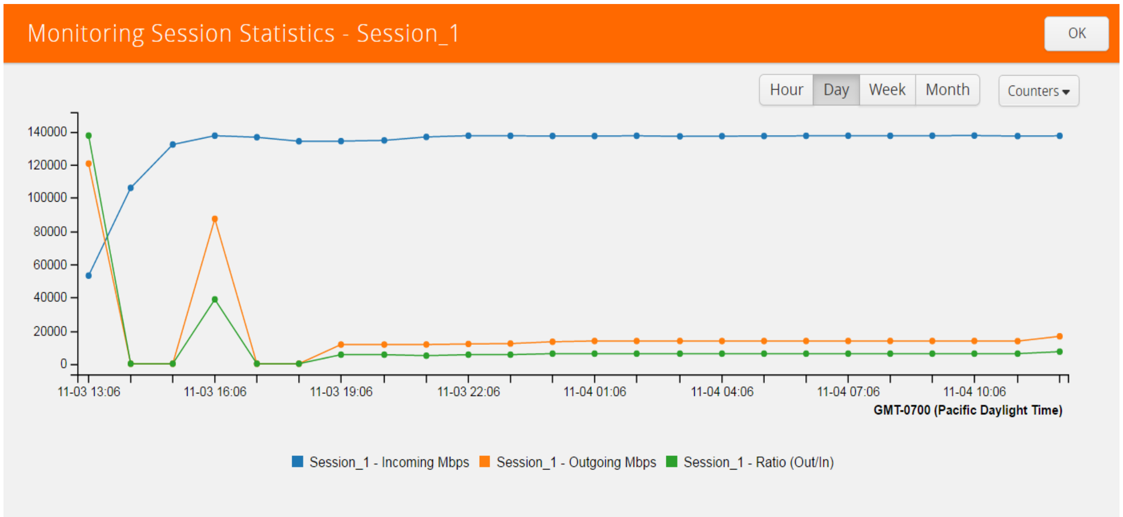
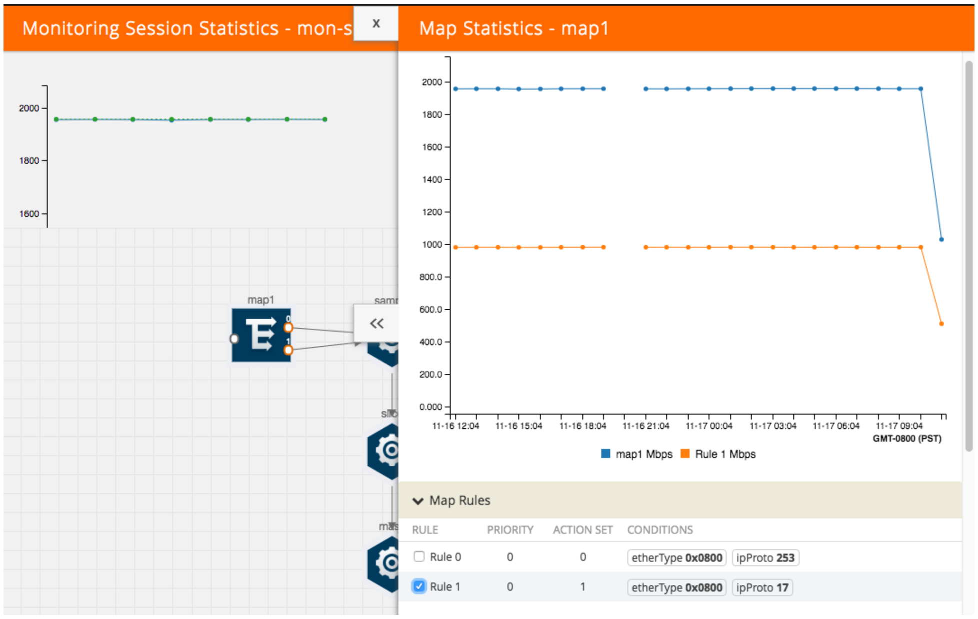


Figure 4-51: Viewing the Monitoring Session Statistics

You can click on Incoming Maps, Outgoing Maps, and Ratio at the bottom of the graph to view the statistics individually.

You can expand the **View Monitoring Session Diagram** and click on each individual map, application, and tunnel to view more details about the incoming and outgoing traffic on the selected statistics page. The Map Statistics page lets you choose the map rules to view the traffic matching the selected rule.



RULE	PRIORITY	ACTION SET	CONDITIONS
□ Rule 0	0	0	etherType **0x0800** ipProto **253**
☑ Rule 1	0	1	etherType **0x0800** ipProto **17**

Figure 4-52: Viewing the Map Statistics

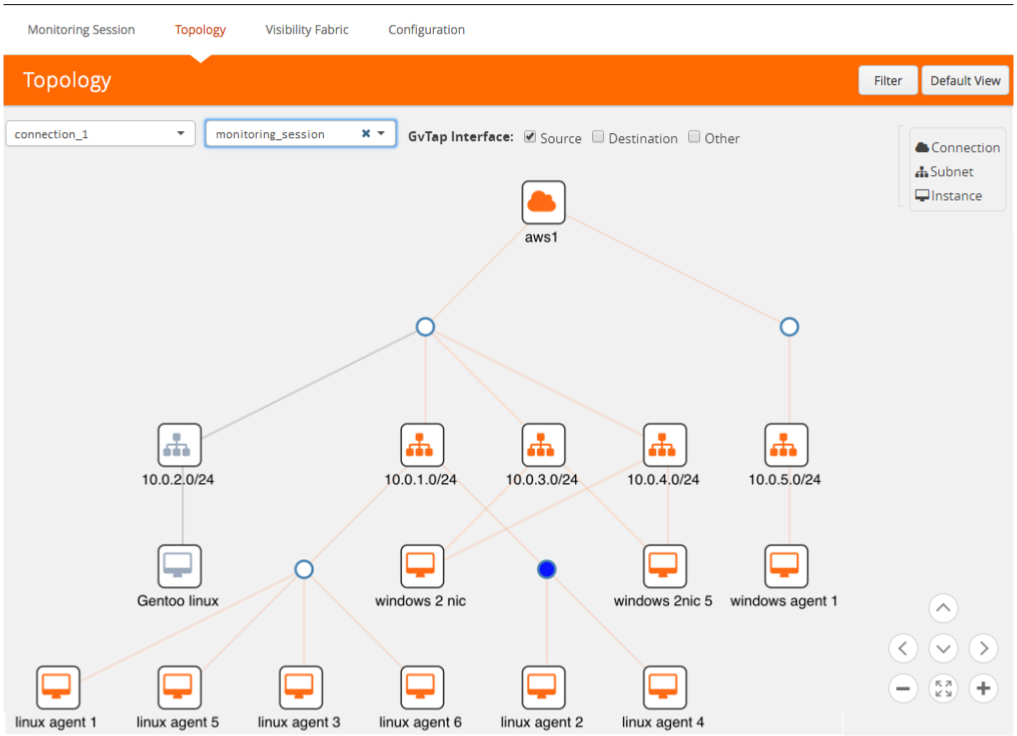
View Topology

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

To view the topology diagram:

1. Select **AWS** > **Topology**.
2. Select a connection from the **Select connection...** list. The topology view of the subnets and instances is displayed.
3. (Optional) Select a monitoring session from the **Select Monitoring Session...**list. The topology view of the monitored subnets and instances in the selected session are displayed.
4. Select one of the following check boxes:
   - **Source**— Displays the topology view of the source target interfaces that are being monitored.
   - **Destination**—Displays the topology view of the destination target interfaces where the traffic is being mirrored.

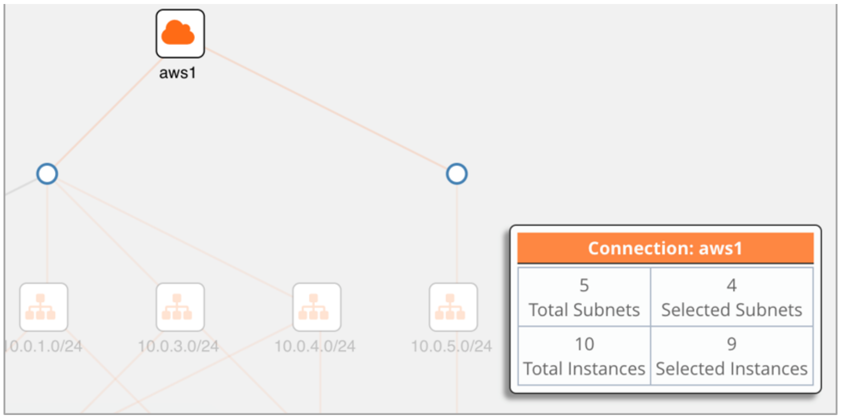
- **Other**—Displays the topology view of the non-G-vTAP agents such as GigaVUE V Series Controllers, G-vTAP Controllers, monitoring tools, and instances that are being used in the connection.



connection_1 ▾ | monitoring_session ✕ ▾ | **GvTap Interface:** ☑ Source ☐ Destination ☐ Other

Figure 4-53: Viewing the Topology

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



Connection: aws1

5 Total Subnets	4 Selected Subnets
10 Total Instances	9 Selected Instances

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

- 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.
- 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. Refer to Figure 4-54 on page 76.

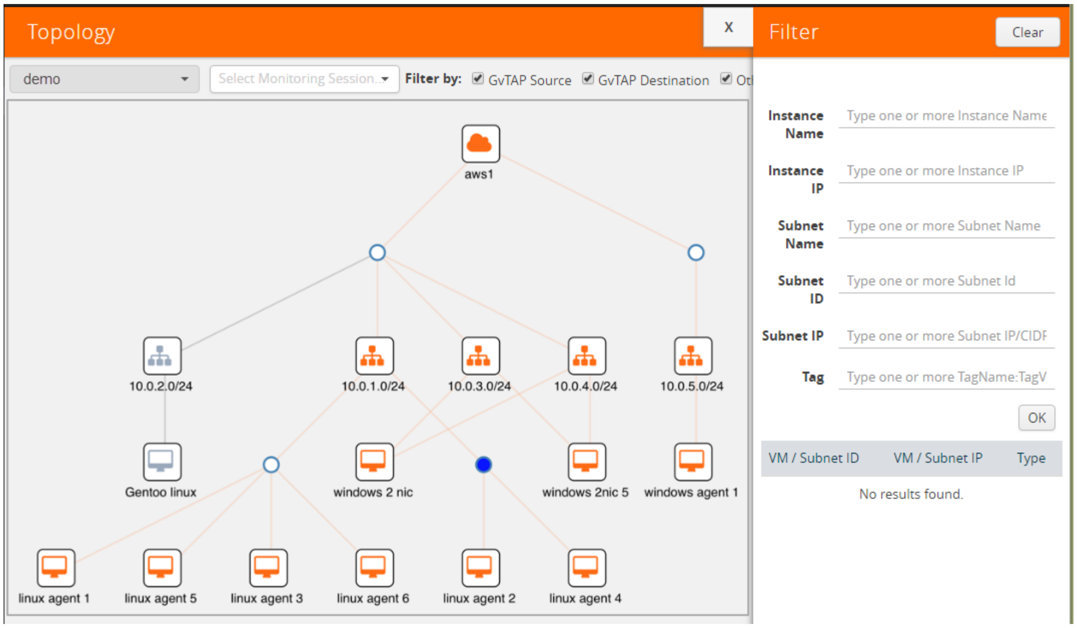


Figure 4-54: Filtering in Topology View

Configure AWS Settings

This section provides information on how to configure the maximum number of connections, refresh intervals for instance and non-instance inventory, and maximum batch size for monitoring session updates. It also provides information on how to enable CloudWatch events.

Use the **AWS** > **Settings** > **Advanced** to edit these AWS settings. Refer to Table 4-10 on page 77 for more information about the settings:

Table 4-10: AWS Settings

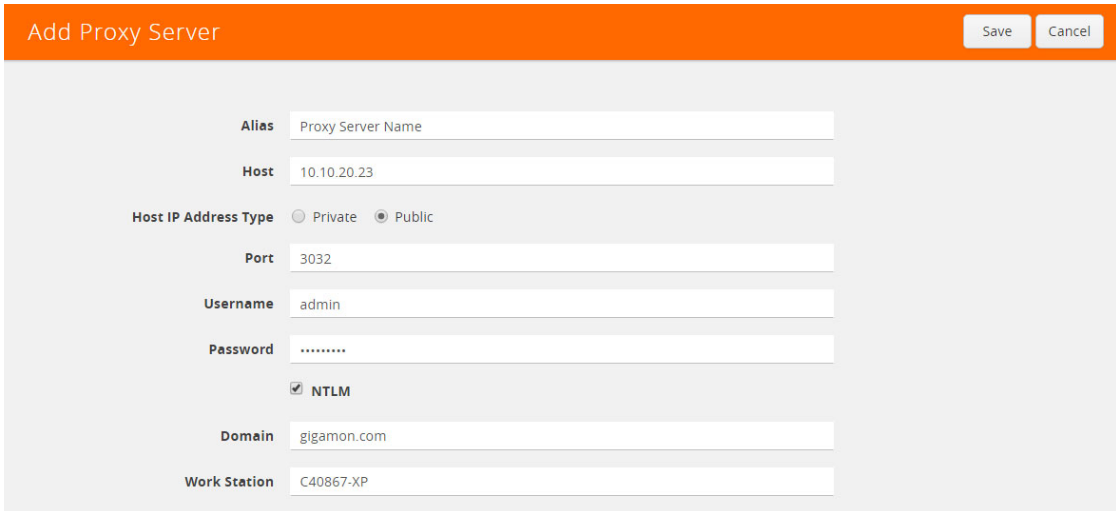
Settings	Description
Maximum number of connections allowed	Specifies the maximum number of VPC connections you can establish in GigaVUE-FM.
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of EC2 instances in AWS.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric nodes
Number of instances per GigaVUE V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node.
Refresh interval for G-vTAP agent inventory (secs)	Specifies the frequency for discovering the G-vTAP agents available in the VPC.
AWS CloudWatch event-based inventory refresh	Enables or disables the AWS CloudWatch event-based inventory refresh. If enabled, CloudWatch event rules updates GigaVUE-FM with EC2 instance state changes.
G-vTAP Agent Tunnel Type	Specifies the G-vTAP Agent Tunnel Type

Configure Proxy Server

Sometimes, the VPC in which the GigaVUE-FM is launched may not have access to the Internet. Without Internet access, GigaVUE-FM cannot connect to the AWS API endpoints. For GigaVUE-FM to connect to AWS, a proxy server must be configured.

To create a proxy server:

1. Select **AWS** > **Settings** > **Proxy Server**.
2. Click **Add**. The Add Proxy Server page is displayed as shown in Figure 4-55 on page 78.



Add Proxy Server

Alias: Proxy Server Name
Host: 10.10.20.23
Host IP Address Type: ○ Private ● Public
Port: 3032
Username: admin
Password: ·········
☑ NTLM
Domain: gigamon.com
Work Station: C40867-XP

Figure 4-55: Adding a Proxy Server

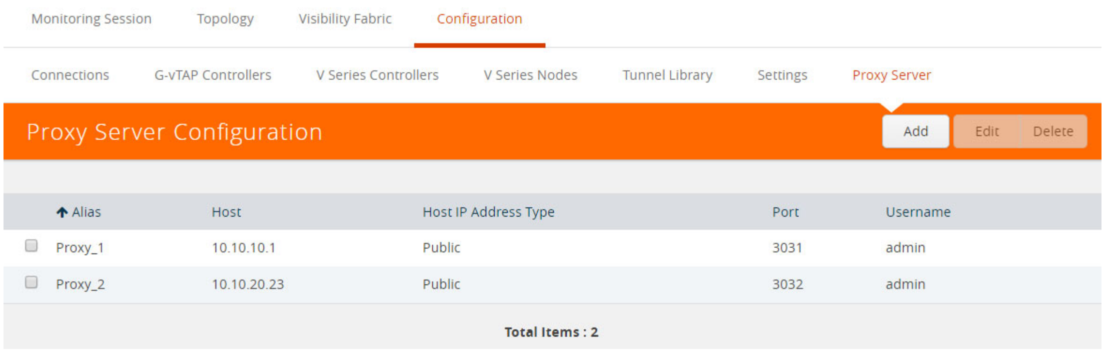
3. Select or enter the appropriate information as shown in Table 4-11 on page 78.

Table 4-11: Fields for Proxy Sever Configuration

Field	Description
Alias	The name of the proxy server.
Host	The host name or the IP address of the proxy server.
Host IP Address Type	The type of the Host IP address that indicate whether the proxy server IP address is private or public to the VPC.
Port	The port number used by the proxy server for connecting to the Internet.
Username	(Optional) The username of the proxy server.
Password	The password of the proxy server.
NTLM	(Optional) The type of the proxy server used to connect to the VPC.
Domain	The domain name of the client accessing the proxy server.
Workstation	(Optional) The name of the workstation or the computer accessing the proxy server.

4. Click **Save**.

   The new proxy server configuration is added to the Proxy Server Configuration page. Refer to Figure 4-56. The proxy server is also listed in the AWS Connection page. Refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.



Proxy Server Configuration

	↑ Alias	Host	Host IP Address Type	Port	Username
□	Proxy_1	10.10.10.1	Public	3031	admin
□	Proxy_2	10.10.20.23	Public	3032	admin

Total Items : 2

Figure 4-56: Proxy Server Configuration Page

Events

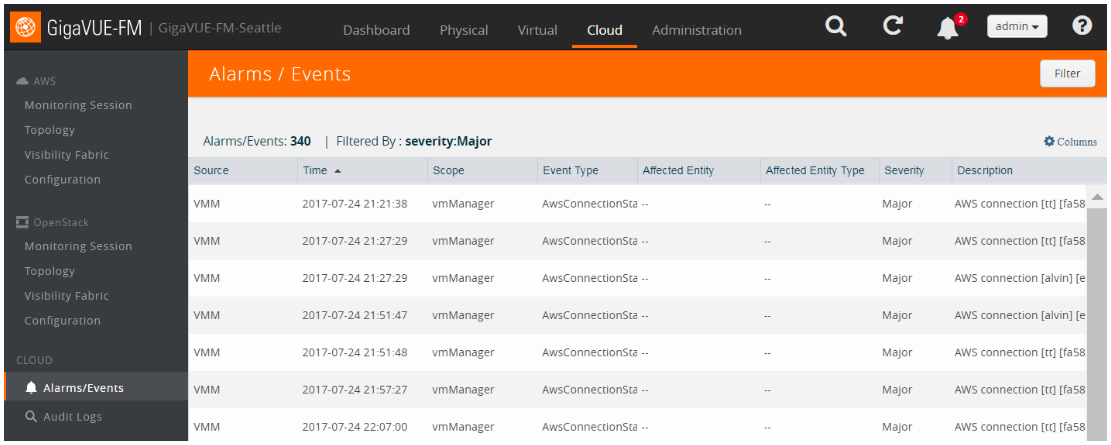
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- AWS License Expire
- G-vTAP Agent Inventory Update Completed
- AWS 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 AWS license expiry.

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

Click **Cloud** on the top navigation link. On the left navigation pane, click **Events**.



Alarms / Events

Alarms/Events: **340** | Filtered By : **severity:Major**

Source	Time ▲	Scope	Event Type	Affected Entity	Affected Entity Type	Severity	Description
VMM	2017-07-24 21:21:38	vmManager	AwsConnectionSta	--	--	Major	AWS connection [tt] [fa58
VMM	2017-07-24 21:27:29	vmManager	AwsConnectionSta	--	--	Major	AWS connection [tt] [fa58
VMM	2017-07-24 21:27:29	vmManager	AwsConnectionSta	--	--	Major	AWS connection [alvin] [e
VMM	2017-07-24 21:51:47	vmManager	AwsConnectionSta	--	--	Major	AWS connection [alvin] [e
VMM	2017-07-24 21:51:48	vmManager	AwsConnectionSta	--	--	Major	AWS connection [tt] [fa58
VMM	2017-07-24 21:57:27	vmManager	AwsConnectionSta	--	--	Major	AWS connection [tt] [fa58
VMM	2017-07-24 22:07:00	vmManager	AwsConnectionSta	--	--	Major	AWS connection [tt] [fa58

Figure 4-57: Alarms

Table 4-12 describes the parameters recording for each event. You can also use filters to narrow down the results. Refer to *Filter Events* on page 80.

Table 4-12: Event Parameters

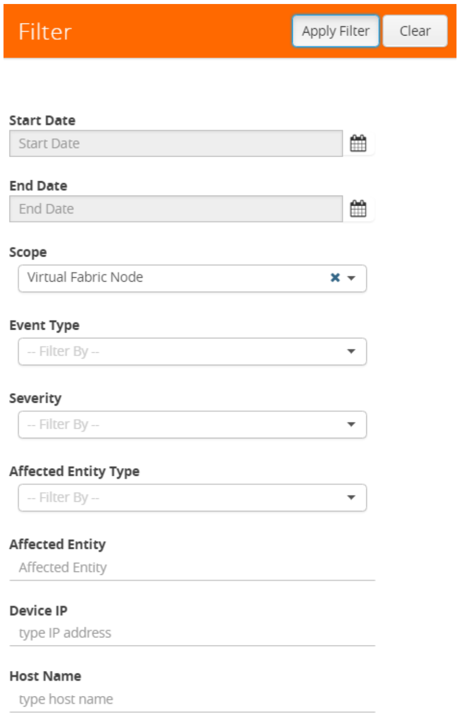
Controls/ Parameters	Description
Source	The source from where the alarms and events are generated.
Time	The timestamp when the event occurred. **IMPORTANT:** Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node reporting the event. The timestamp is based 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.

Filter Events

To filter the event:

1. Click **Filter**.

The Filter quick view is displayed.



Filter | Apply Filter | Clear

Start Date
Start Date

End Date
End Date

Scope
Virtual Fabric Node

Event Type
-- Filter By --

Severity
-- Filter By --

Affected Entity Type
-- Filter By --

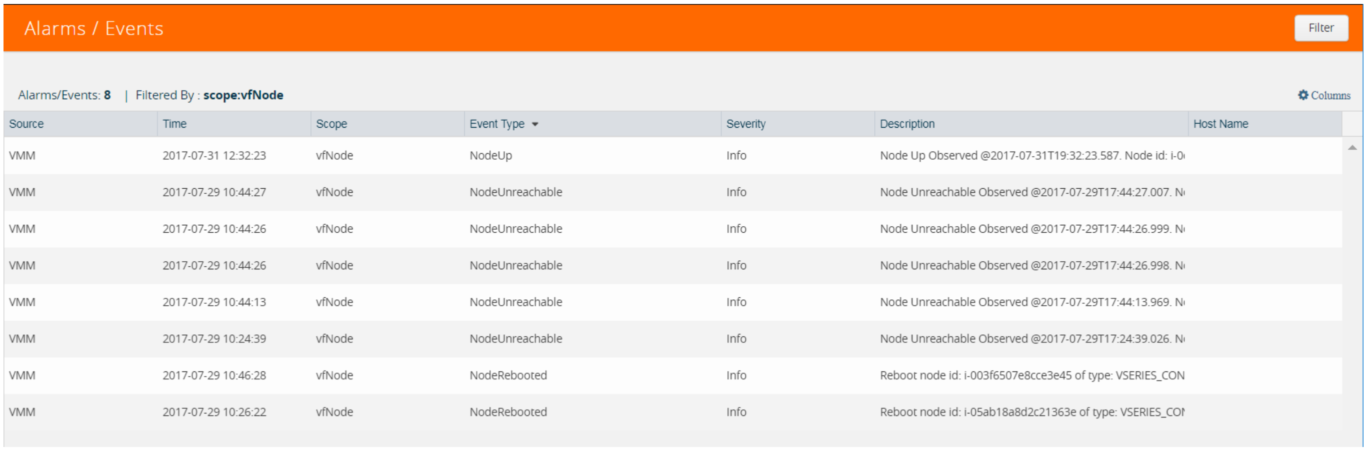
Affected Entity
Affected Entity

Device IP
type IP address

Host Name
type host name

Figure 4-58: Filtering Alarms/Events

2. Select the filtering criteria, then click **Apply Filter**. The results are displayed in the Events page.



Alarms / Events | Filter

Alarms/Events: **8** | Filtered By : **scope:vfNode**

Columns

Source	Time	Scope	Event Type	Severity	Description	Host Name
VMM	2017-07-31 12:32:23	vfNode	NodeUp	Info	Node Up Observed @2017-07-31T19:32:23.587. Node id: i-0	
VMM	2017-07-29 10:44:27	vfNode	NodeUnreachable	Info	Node Unreachable Observed @2017-07-29T17:44:27.007. N	
VMM	2017-07-29 10:44:26	vfNode	NodeUnreachable	Info	Node Unreachable Observed @2017-07-29T17:44:26.999. N	
VMM	2017-07-29 10:44:26	vfNode	NodeUnreachable	Info	Node Unreachable Observed @2017-07-29T17:44:26.998. N	
VMM	2017-07-29 10:44:13	vfNode	NodeUnreachable	Info	Node Unreachable Observed @2017-07-29T17:44:13.969. N	
VMM	2017-07-29 10:24:39	vfNode	NodeUnreachable	Info	Node Unreachable Observed @2017-07-29T17:24:39.026. N	
VMM	2017-07-29 10:46:28	vfNode	NodeRebooted	Info	Reboot node id: i-003f6507e8cce3e45 of type: VSERIES_CON	
VMM	2017-07-29 10:26:22	vfNode	NodeRebooted	Info	Reboot node id: i-05ab18a8d2c21363e of type: VSERIES_CO	

Figure 4-59: Events Filter Results

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.

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.

Filter Audit Logs

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.

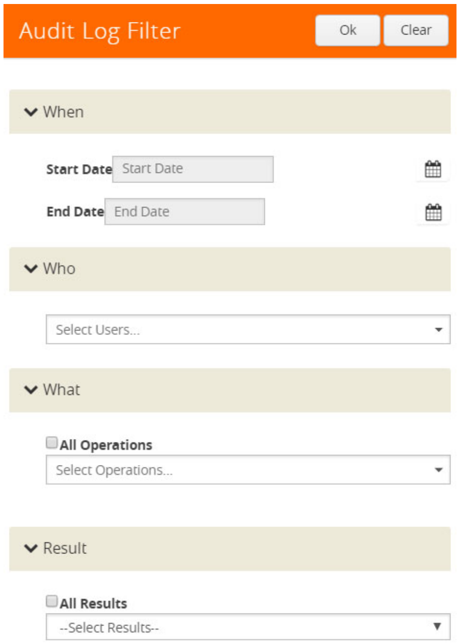


Figure 4-60: Audit Logs Filter

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.

5 Upgrade GigaVUE-FM in AWS

This chapter describes how to upgrade the GigaVUE-FM instance on AWS.

Refer to the following sections for details:

- *At a Glance* on page 85
- *Stop GigaVUE FM Instance* on page 85
- *Create Snapshot of the GigaVUE-FM Instance* on page 86
- *Upgrade GigaVUE-FM Instance* on page 90

At a Glance

To upgrade the GigaVUE-FM instance successfully, you must perform the following steps:

Step 1: Stop the existing version of the GigaVUE-FM instance.

Step 2: Create a snapshot of the second disk (dev/sdb) of the FM instance.

Step 3: Make a note of the snapshot ID.

Step 4: Launch the latest version of the GigaVUE-FM instance. While launching the latest version, enter the snapshot ID of the old version of the GigaVUE-FM instance in **Add Storage** > **Add New Volume**.

Step 5: Complete the launch.

Step 6: Verify if the data from the previous GigaVUE-FM instance is restored in the new instance.

Step 7: Terminate the old FM instance.

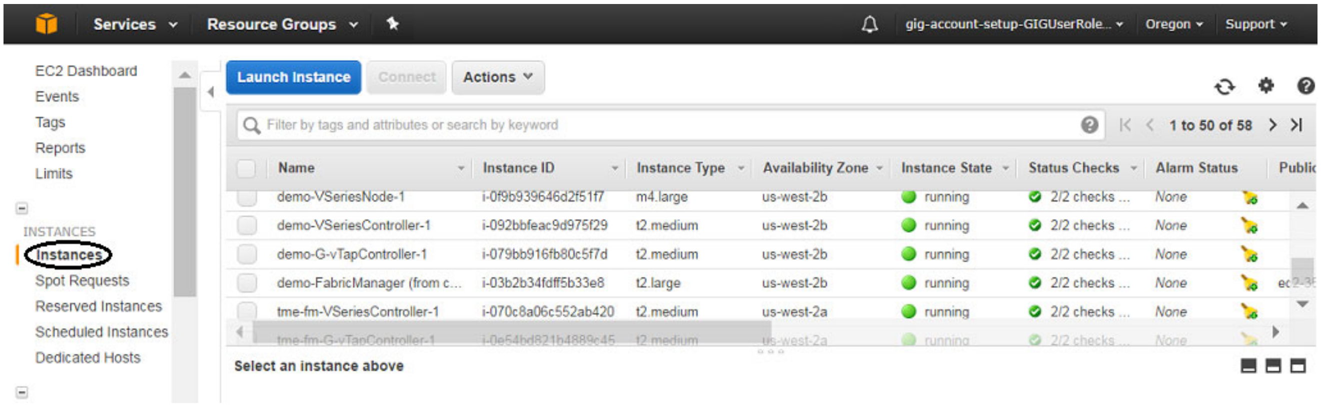
Stop GigaVUE FM Instance

Before upgrading the GigaVUE-FM instance, the existing version of the GigaVUE-FM instance must be stopped.

NOTE: Do not terminate the GigaVUE-FM instance.

To stop the GigaVUE-FM instance:

1. Login to the AWS account and select **Services** > **EC2**.
2. In the left navigation pane, select **Instances**. Refer to Figure 5-1 on page 86.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public
demo-VSeriesNode-1	i-0f9b939646d2f51f7	m4.large	us-west-2b	running	2/2 checks ...	None	
demo-VSeriesController-1	i-092bbfeac9d975f29	t2.medium	us-west-2b	running	2/2 checks ...	None	
demo-G-vTapController-1	i-079bb916fb80c5f7d	t2.medium	us-west-2b	running	2/2 checks ...	None	
demo-FabricManager (from c...	i-03b2b34fdff5b33e8	t2.large	us-west-2b	running	2/2 checks ...	None	ec2-3
tme-fm-VSeriesController-1	i-070c8a06c552ab420	t2.medium	us-west-2a	running	2/2 checks ...	None	
tme-fm-G-vTapController-1	i-0e54bd821b4889c45	t2.medium	us-west-2a	running	2/2 checks ...	None	

Figure 5-1: Selecting Instances

3. In the search field, enter the name of the existing GigaVUE-FM instance and select the Instance ID.

NOTE: If the instance ID is the password for logging in to the existing GigaVUE-FM, make note of this instance ID. This instance ID will be used as the password for logging in to the upgraded GigaVUE-FM as well. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

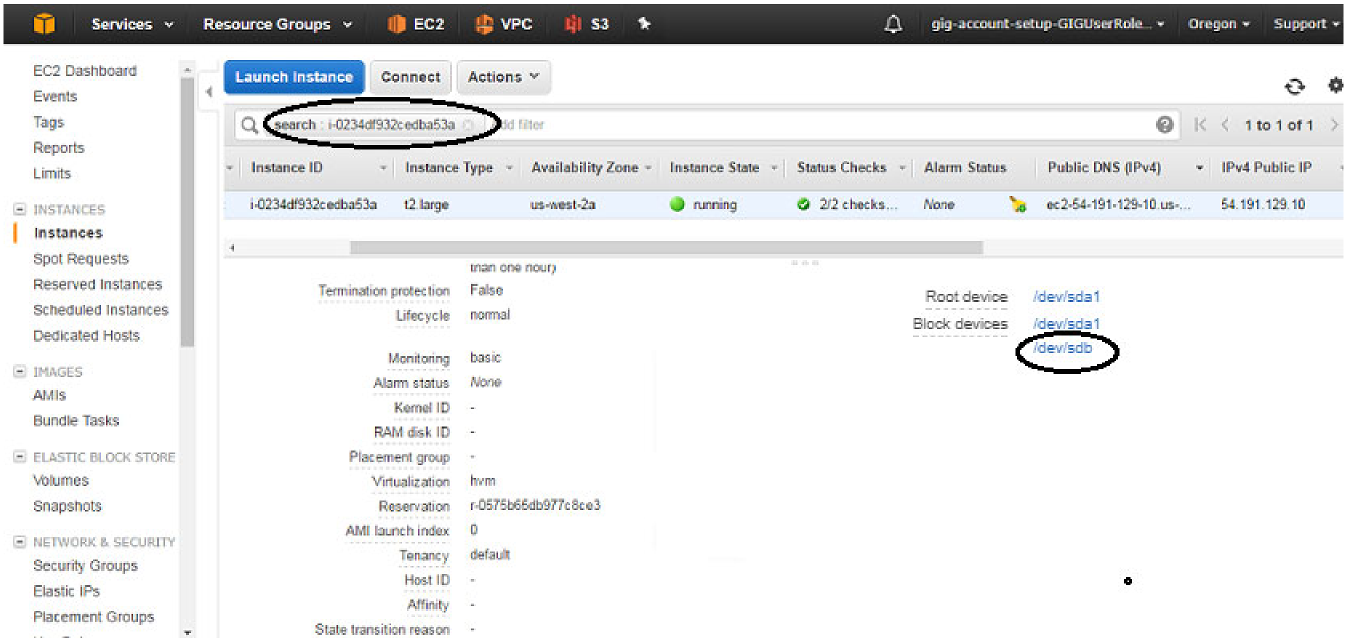
4. Go to **Actions** > **Instance State** > **Stop**.

Create Snapshot of the GigaVUE-FM Instance

You must create a snapshot of the volume of the existing version (dev/sdb) of the GigaVUE-FM instance. Snapshots capture data that are written to your Amazon EBS volume at the time the snapshot is taken. This excludes any data that are cached by any applications or the operating system.

To create a snapshot:

1. Select the GigaVUE-FM instance and click the **Description** tab. Refer to Figure 5-2 on page 87.



search : i-0234df932cedba53a   Add filter

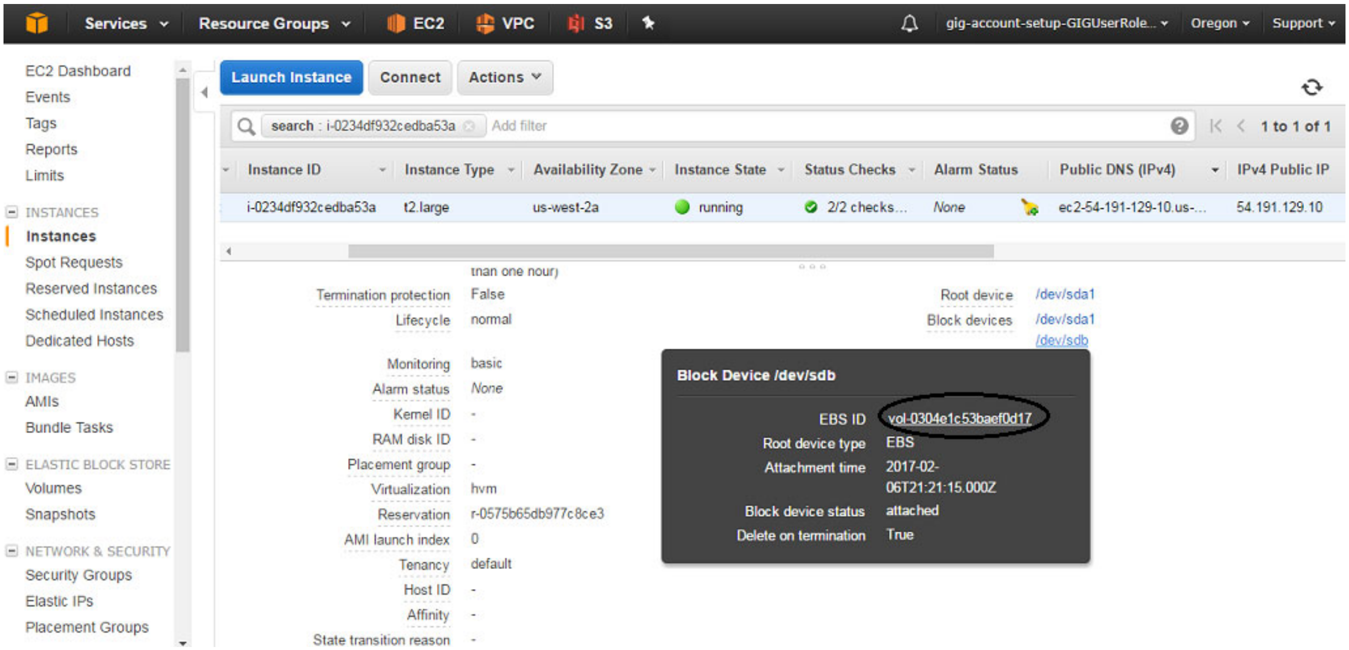
Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
i-0234df932cedba53a	t2.large	us-west-2a	running	2/2 checks...	None	ec2-54-191-129-10.us-...	54.191.129.10

than one hour)

Termination protection	False
Lifecycle	normal
Monitoring	basic
Alarm status	None
Kernel ID	-
RAM disk ID	-
Placement group	-
Virtualization	hvm
Reservation	r-0575b65db977c8ce3
AMI launch index	0
Tenancy	default
Host ID	-
Affinity	-
State transition reason	-
Root device	/dev/sda1
Block devices	/dev/sda1 /dev/sdb

Figure 5-2: Searching for the GigaVUE-FM Instance

2. Scroll down and locate Block Devices. Refer to Figure 5-2 on page 87.
3. Click the **/dev/sdb** link. The Block Device dialog box is displayed with the volume ID link. Refer to Figure 5-3 on page 87.



search : i-0234df932cedba53a   Add filter

Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
i-0234df932cedba53a	t2.large	us-west-2a	running	2/2 checks...	None	ec2-54-191-129-10.us-...	54.191.129.10

than one hour)

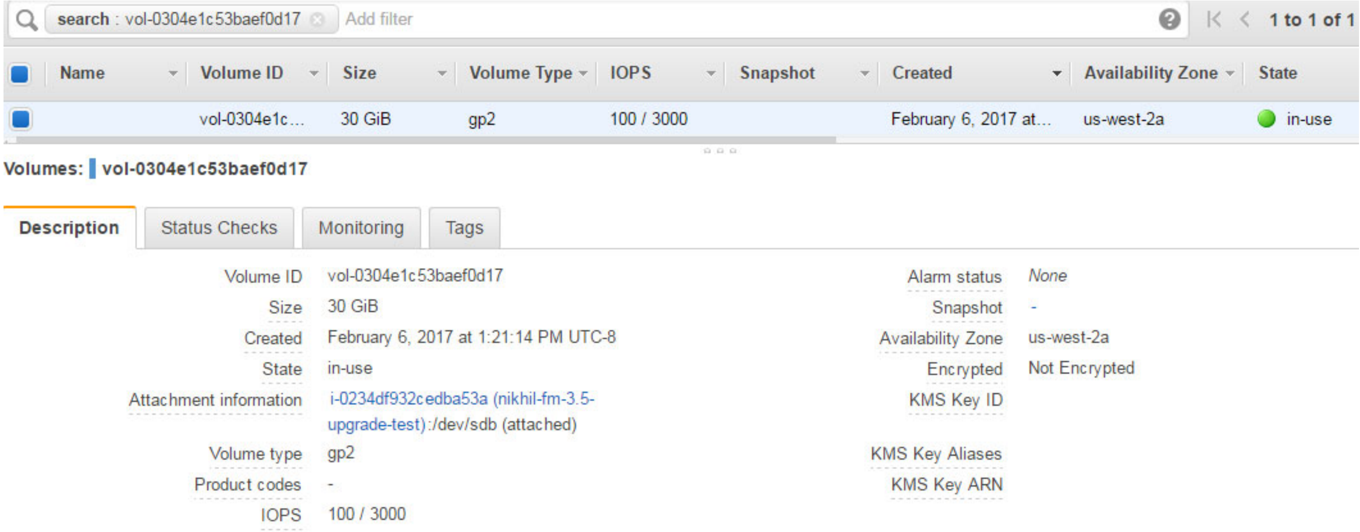
Termination protection	False
Lifecycle	normal
Monitoring	basic
Alarm status	None
Kernel ID	-
RAM disk ID	-
Placement group	-
Virtualization	hvm
Reservation	r-0575b65db977c8ce3
AMI launch index	0
Tenancy	default
Host ID	-
Affinity	-
State transition reason	-
Root device	/dev/sda1
Block devices	/dev/sda1 /dev/sdb

Block Device /dev/sdb

EBS ID	vol-0304e1c53baef0d17
Root device type	EBS
Attachment time	2017-02-06T21:21:15.000Z
Block device status	attached
Delete on termination	True

Figure 5-3: Opening Block Device Dialog Box

4. In the Block Device dialog box, click the volume ID link. The Volumes page is displayed. Refer to Figure 5-4 on page 88.



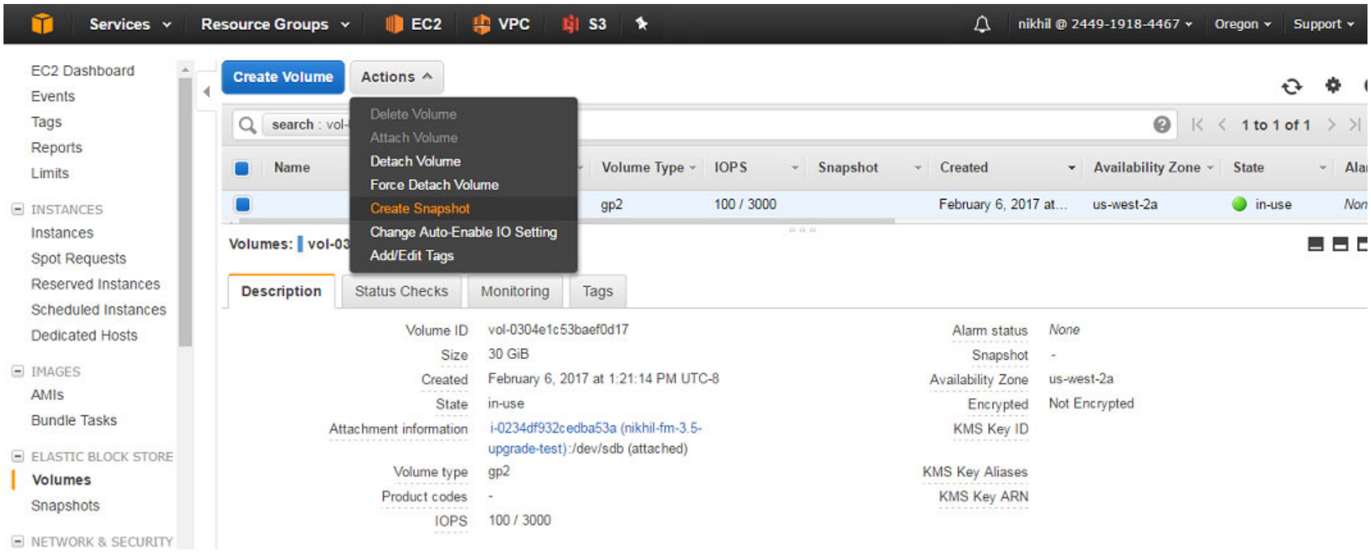
Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
	vol-0304e1c...	30 GiB	gp2	100 / 3000		February 6, 2017 at...	us-west-2a	● in-use

Volumes: vol-0304e1c53baef0d17

Volume ID	vol-0304e1c53baef0d17	Alarm status	None
Size	30 GiB	Snapshot	-
Created	February 6, 2017 at 1:21:14 PM UTC-8	Availability Zone	us-west-2a
State	in-use	Encrypted	Not Encrypted
Attachment information	i-0234df932cedba53a (nikhil-fm-3.5-upgrade-test):/dev/sdb (attached)	KMS Key ID	
Volume type	gp2	KMS Key Aliases	
Product codes	-	KMS Key ARN	
IOPS	100 / 3000		

Figure 5-4: Viewing the Volumes Page

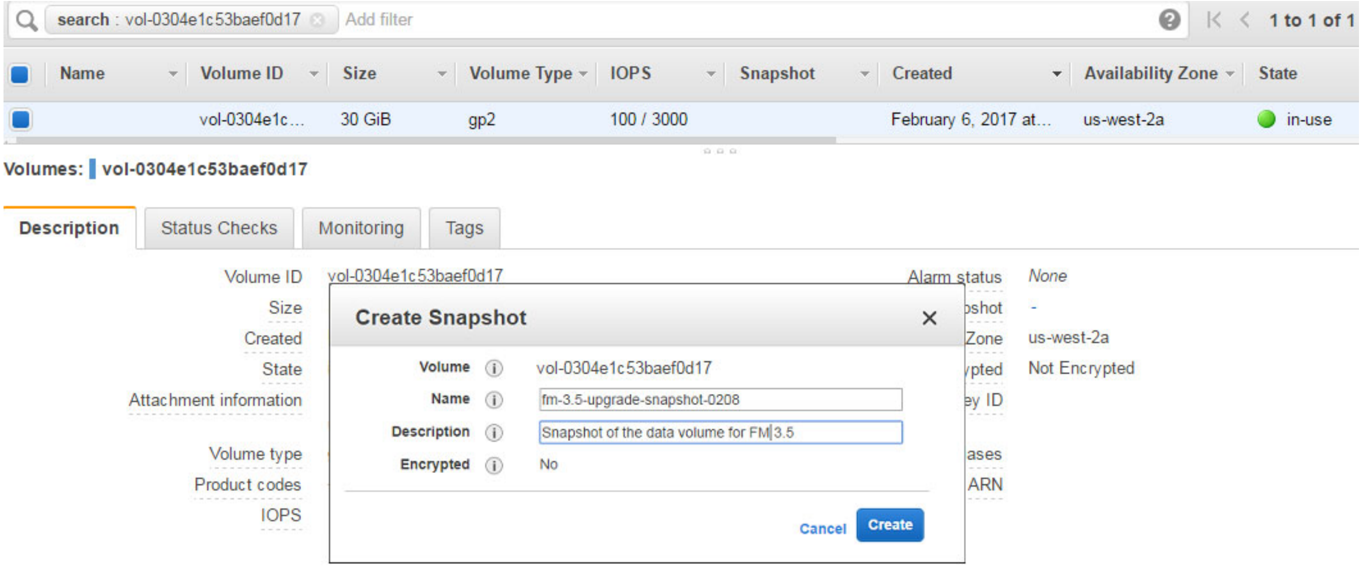
5. Click **Actions** and select **Create Snapshot.** Refer to Figure 5-5 on page 88.



Volume ID	vol-0304e1c53baef0d17	Alarm status	None
Size	30 GiB	Snapshot	-
Created	February 6, 2017 at 1:21:14 PM UTC-8	Availability Zone	us-west-2a
State	in-use	Encrypted	Not Encrypted
Attachment information	i-0234df932cedba53a (nikhil-fm-3.5-upgrade-test):/dev/sdb (attached)	KMS Key ID	
Volume type	gp2	KMS Key Aliases	
Product codes	-	KMS Key ARN	
IOPS	100 / 3000		

Figure 5-5: Selecting Create Snapshot

The Create Snapshot dialog box is displayed. Refer to Figure 5-6 on page 89.



search : vol-0304e1c53baef0d17 | Add filter | 1 to 1 of 1

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State
	vol-0304e1c...	30 GiB	gp2	100 / 3000		February 6, 2017 at...	us-west-2a	● in-use

Volumes: vol-0304e1c53baef0d17

Volume ID vol-0304e1c53baef0d17
Size
Created
State
Attachment information
Volume type
Product codes
IOPS

Alarm status None
...pshot -
...Zone us-west-2a
...ypted Not Encrypted
...ey ID
...ases
...ARN

Create Snapshot

Volume vol-0304e1c53baef0d17
Name fm-3.5-upgrade-snapshot-0208
Description Snapshot of the data volume for FM 3.5
Encrypted No

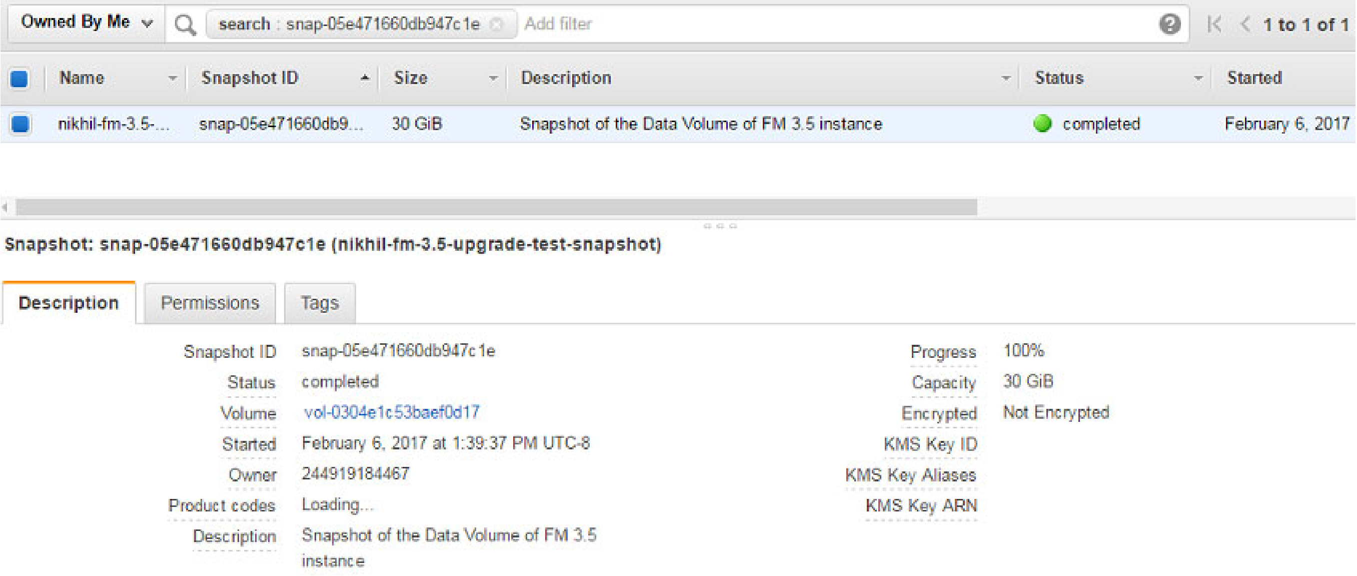
Figure 5-6: Creating a Snapshot

6. In the Create Snapshot dialog box, enter the following information:

Table 5-1: Fields for Creating a Snapshot

Field	Description
Name	The name of the snapshot.
Description	The description of the snapshot.

7. Click **Create**. It will take several minutes for the snapshot to be created. Refer to Figure 5-7 on page 89.



Owned By Me | search : snap-05e471660db947c1e | Add filter | 1 to 1 of 1

Name	Snapshot ID	Size	Description	Status	Started
nikhil-fm-3.5-...	snap-05e471660db9...	30 GiB	Snapshot of the Data Volume of FM 3.5 instance	● completed	February 6, 2017

Snapshot: snap-05e471660db947c1e (nikhil-fm-3.5-upgrade-test-snapshot)

Snapshot ID snap-05e471660db947c1e
Status completed
Volume vol-0304e1c53baef0d17
Started February 6, 2017 at 1:39:37 PM UTC-8
Owner 244919184467
Product codes Loading...
Description Snapshot of the Data Volume of FM 3.5 instance

Progress 100%
Capacity 30 GiB
Encrypted Not Encrypted
KMS Key ID
KMS Key Aliases
KMS Key ARN

Figure 5-7: Viewing the Snapshot Page

NOTE: Make a note of the snapshot ID. This snapshot ID will be used to find the snapshot and add the volume while upgrading the GigaVUE-FM instance.

Upgrade GigaVUE-FM Instance

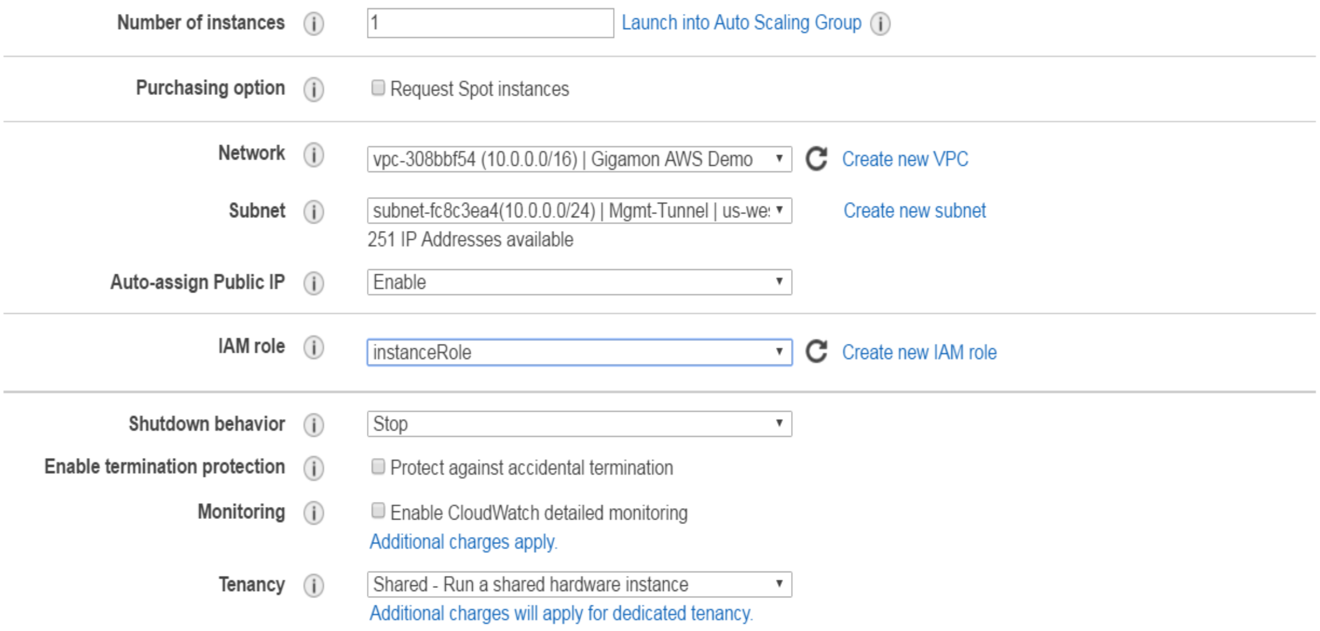
While upgrading the GigaVUE-FM instance, the Amazon EBS volume must be restored with the data from the snapshot that is created in *Create Snapshot of the GigaVUE-FM Instance* on page 86.

To upgrade the GigaVUE-FM instance:

1. Select **Services** > **EC2**.
2. Click **Launch Instance** and go to **AWS Marketplace** or **Community AMIs**.
3. Search for **Gigamon**, locate the latest version of the GigaVUE-FM AMI, and click **Select**.
4. Choose the Instance Type. The recommended instance type is **m4.xlarge**.

NOTE: Do not select the t2 instance types as they are not supported.

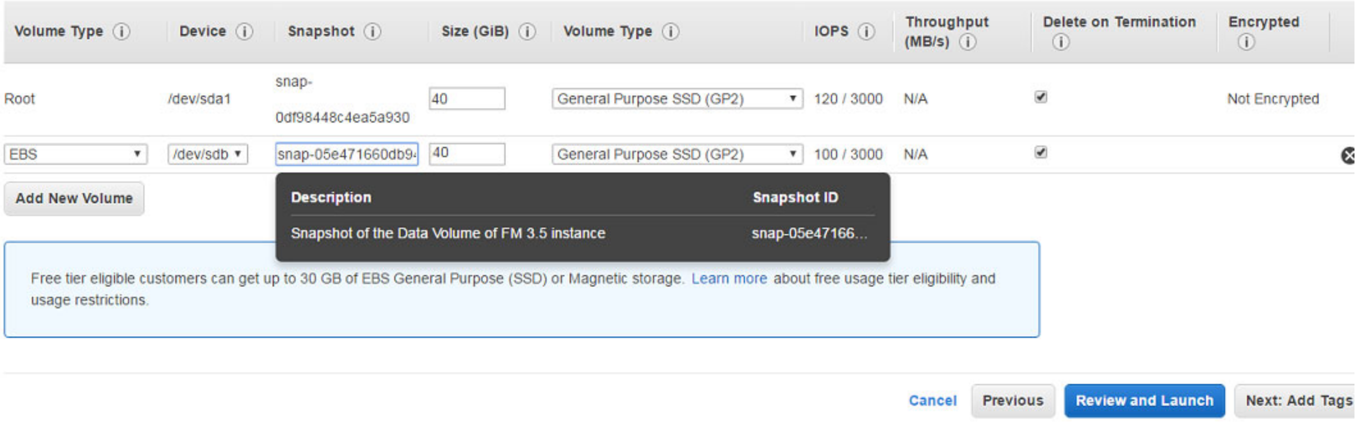
5. Click **Next: Configure Instance Details.** Refer to Figure 5-8 on page 90.



Number of instances	1	Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances	
Network	vpc-308bbf54 (10.0.0.0/16) | Gigamon AWS Demo	Create new VPC
Subnet	subnet-fc8c3ea4(10.0.0.0/24) | Mgmt-Tunnel | us-we: 251 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	
IAM role	instanceRole	Create new IAM role
Shutdown behavior	Stop	
Enable termination protection	□ Protect against accidental termination	
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	

Figure 5-8: Configuring an Instance

6. Enter the following information.
   - **Network**— Select the VPC where you want to launch the AMI.
   - **Subnet**— Select the management subnet that the instance will use after launch. (Required)
   - **Auto-assign Public IP**— Select **Enable**.
   - **IAM role**—Select an existing IAM role to associate with the instance. Refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.
7. Click **Next: Add Storage** and click **Add New Volume**. Refer to Figure 5-9 on page 91.



Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ	
Root	/dev/sda1	snap-0df98448c4ea5a930	40	General Purpose SSD (GP2)	120 / 3000	N/A	☑	Not Encrypted	
EBS	/dev/sdb	snap-05e471660db9	40	General Purpose SSD (GP2)	100 / 3000	N/A	☑		⊗

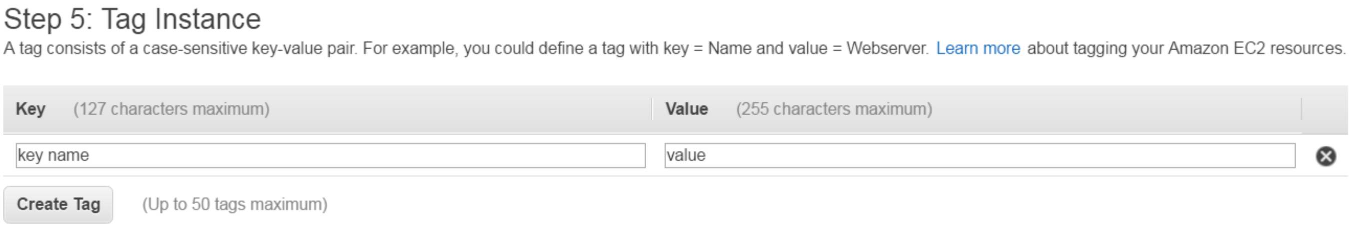
Add New Volume

Description	Snapshot ID
Snapshot of the Data Volume of FM 3.5 instance	snap-05e47166...

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Figure 5-9: Adding New Volume

8. Enter the following storage device settings as shown in Figure 5-9 on page 91:
   - **Snapshot**—Enter the name of the snapshot that is created in step 9 in the section *Create Snapshot of the GigaVUE-FM Instance* on page 86.
   - **Size (GiB)**— Enter a minimum of 40Gb of storage. The size of the volume must be same as the volume selected while launching the previous version of the GigaVUE-FM instance.
   - **Volume Type**— Select a volume type. The recommended volume is General Purpose SSD (GP2).
   - **Delete on Termination**— Select this check box to make sure the volumes are cleaned up when the GigaVUE-FM instance is removed.
9. Click **Next: Tag Instance,** and then add a key-value pair to identify the instance. Refer to Figure 5-10 on page 91.



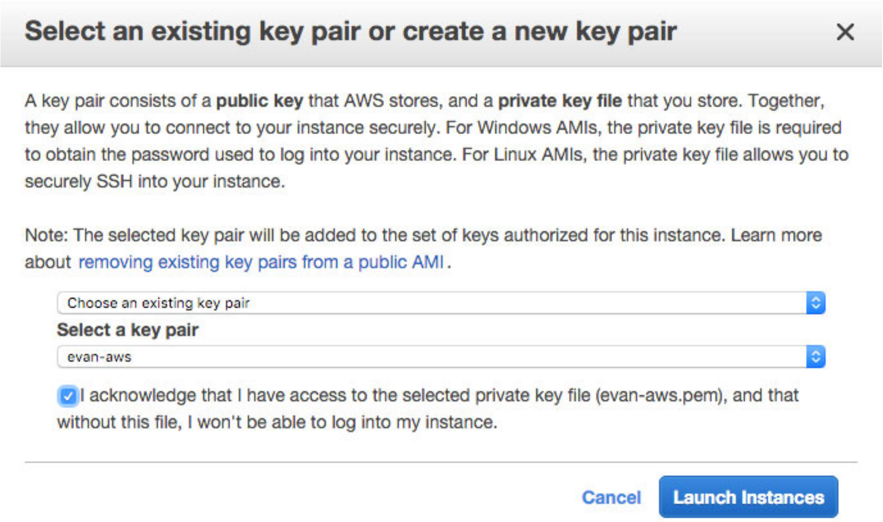
Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	
key name	value	⊗

Figure 5-10: Adding a Tag to an Instance

10. Click **Next: Add Security Group**. Click the **Select an existing security group** check box if the security group is already created. Otherwise, select the **Create a new security group** check box and click **Add Rule**. For more information on creating a security group, refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.
11. Click **Review and Launch**. Review the instance launch details and click **Launch**.
12. Select the SSH key pair, check the acknowledgment check box, and click **Launch Instances** as shown in Figure 5-11 on page 92.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Choose an existing key pair

Select a key pair

evan-aws

☑ I acknowledge that I have access to the selected private key file (evan-aws.pem), and that without this file, I won't be able to log into my instance.

Figure 5-11: Selecting an SSH Key Pair

13. It will take several minutes for the instance to initialize. After the initialization is completed, verify the instance through the Web interface as follows:
    a. Find the instance and expand the page in the **Descriptions** tab to view the instance information, if necessary.
    b. Copy the Public DNS value and paste the value into a new browser window or tab.
    c. Copy the Instance ID of the previous version of the GigaVUE-FM. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

NOTE: Do not have multiple versions of GigaVUE-FM instances monitoring the same AWS connection.

Launch the new version of the GigaVUE-FM instance. Verify if the data from the previous GigaVUE-FM instance is restored in the new instance. Once the data is verified, terminate the old version of the GigaVUE-FM instance.

6 Upgrade Virtual Fabric in AWS

This chapter describes how to upgrade GigaVUE V Series Controllers and GigaVUE V Series nodes.

NOTE: G-vTAP Controllers cannot be upgraded. Only a new version that is compatible with the G-vTAP agents' version can be added during the G-vTAP configuration.

Prerequisite

Before you upgrade the GigaVUE V Series Controllers and GigaVUE V Series nodes, you must upgrade GigaVUE-FM to software version 5.1 or above. For information about upgrading the GigaVUE-FM instance, refer to *Upgrade GigaVUE-FM in AWS* on page 85.

NOTE: The older version of virtual fabric is compatible with GigaVUE-FM 5.1. For better performance, Gigamon recommends you to upgrade to the latest version.

Upgrade GigaVUE V Series Controllers and Nodes

GigaVUE-FM lets you upgrade GigaVUE V Series Controllers and GigaVUE V Series nodes at a time.

There are multiple ways to upgrade the GigaVUE V Series Controllers and nodes. You can:

- Launch and replace the complete set of nodes and controllers at a time.

  For example, if you have 1 GigaVUE V Series Controller and 10 GigaVUE V Series nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series controller is launched. Next, the new version of GigaVUE V Series nodes are launched. Then, the old version of V Series controller and nodes are deleted from the VPC.

  NOTES:

  - When the new version of nodes and controllers are launched, the old version still exists in the VPC until they are deleted. Make sure the instance type determined during the configuration can accommodate the total number of new and old instances present in the VPC. If the instance type cannot support so many instances, you can choose to upgrade in multiple batches.

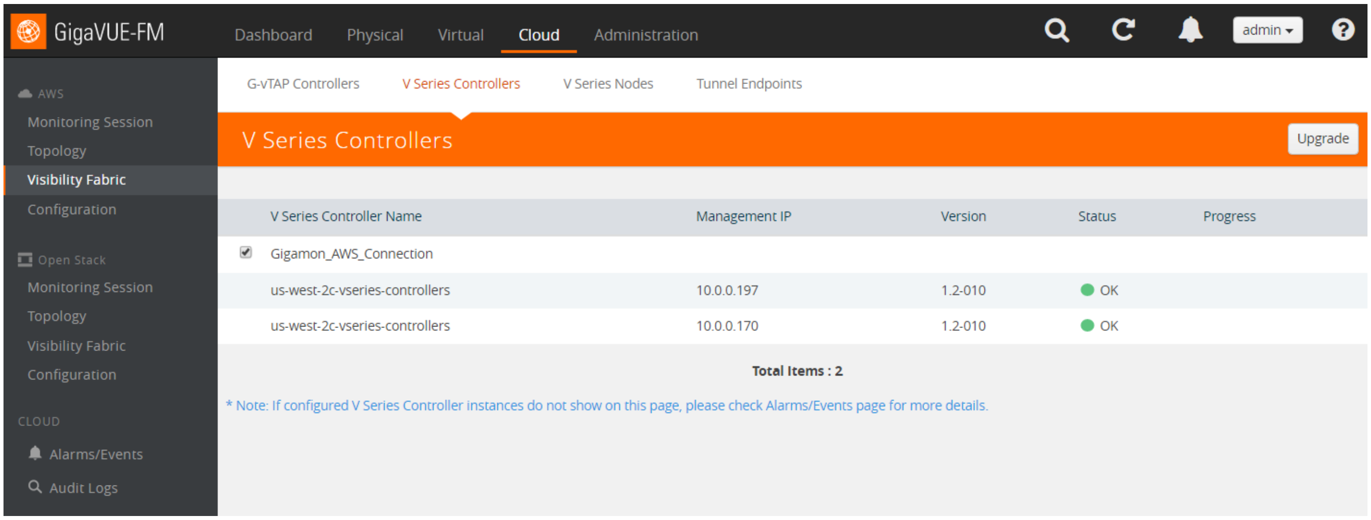
  - If there is an error while upgrading the complete set of controllers and nodes present in the VPC, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
  - Prior to upgrading the GigaVUE V Series Controllers and nodes, you must ensure that the required number of free addresses are available in the respective subnets. Otherwise, the upgrade will fail.

- Launch and replace the nodes and controllers in multiple batches.

  For example, if there are 18 GigaVUE V Series nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Controllers and GigaVUE V Series Nodes:

1. Click **Cloud** in the top navigation link.
2. In the left navigation pane, select **Visibility Fabric** > **V Series Controllers**. Refer to Figure 6-1 on page 94.



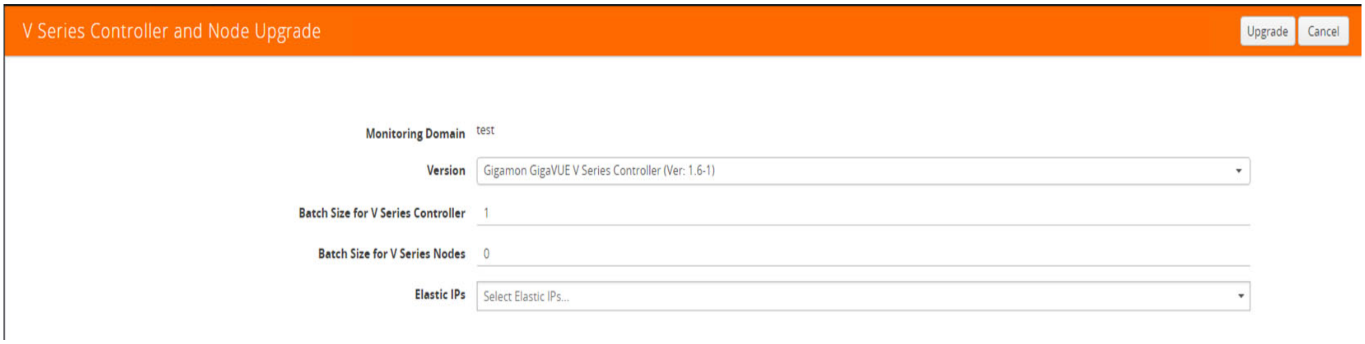
	V Series Controller Name	Management IP	Version	Status	Progress
☑	Gigamon_AWS_Connection				
	us-west-2c-vseries-controllers	10.0.0.197	1.2-010	● OK	
	us-west-2c-vseries-controllers	10.0.0.170	1.2-010	● OK	

Total Items : 2

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

Figure 6-1: Gigamon Virtual Fabric Upgrade

3. Select the connection name check box and click **Upgrade**. The V Series Controller and Node Upgrade page is displayed. Refer to Figure 6-2 on page 94.



Monitoring Domain test

Version Gigamon GigaVUE V Series Controller (Ver: 1.6-1)

Batch Size for V Series Controller 1

Batch Size for V Series Nodes 0

Elastic IPs Select Elastic IPs...

Figure 6-2: GigaVUE V Series Controller and Node Upgrade

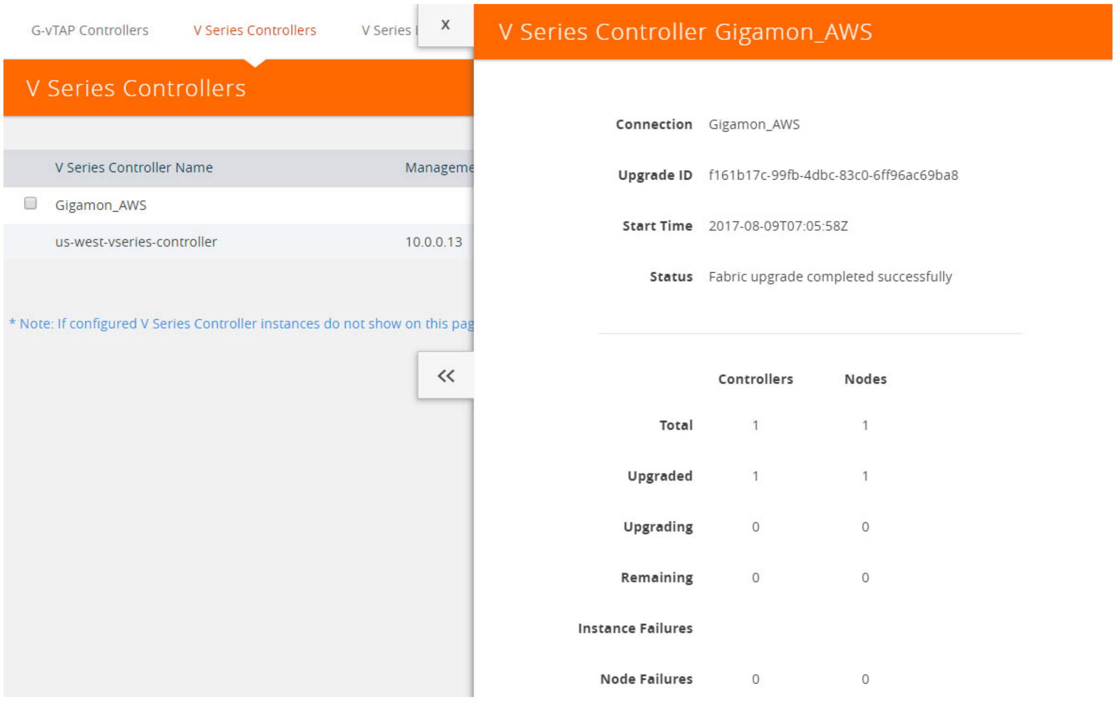
4. From the **Version** drop-down list, select the latest version of the GigaVUE V Series Controller.
5. To upgrade the GigaVUE V Series Controllers, specify the batch size in the **Batch Size for V Series Controller** box.

   For example, if there are 4 GigaVUE V Series Controllers in your VPC, you can specify 4 as the batch size and upgrade all of them at once or specify 2 as the batch size and upgrade 2 GigaVUE V Series Controllers in each batch.
6. To upgrade the GigaVUE V Series nodes, specify the batch size in the **Batch Size for V Series Nodes** box.

   For example, if there are 7 GigaVUE V Series nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series nodes in each batch. In the last batch, the remaining 1 V Series node is launched.
7. Click **Upgrade**.

   The upgrade process takes a while depending on the number of GigaVUE V Series controllers and nodes upgrading in your AWS environment. First, the new version of the GigaVUE V Series Controllers is launched. Next, the new version of GigaVUE V Series nodes is launched. Then, the older version of both is deleted from the VPC. In the V Series Controllers page, click the link under Progress to view the upgrade status. Refer to Figure 6-3 on page 95.

   The monitoring session is deployed automatically



V Series Controllers

	V Series Controller Name	Manageme
□	Gigamon_AWS	
	us-west-vseries-controller	10.0.0.13

* Note: If configured V Series Controller instances do not show on this pag

V Series Controller Gigamon_AWS

Connection Gigamon_AWS

Upgrade ID f161b17c-99fb-4dbc-83c0-6ff96ac69ba8

Start Time 2017-08-09T07:05:58Z

Status Fabric upgrade completed successfully

	Controllers	Nodes
Total	1	1
Upgraded	1	1
Upgrading	0	0
Remaining	0	0
Instance Failures		
Node Failures	0	0

Figure 6-3: GigaVUE Fabric Upgrade Status

7 Glossary

This appendix lists the AWS terminologies used in this document. To find a brief definition of these terms, refer to AWS Glossary.

- Access Key
- Access key ID
- Amazon API Gateway
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon VPC
- AMI
- AWS
- AWS Identity and Access Management (IAM)
- CIDR block
- EC2 Instances
- Elastic IP address
- Endpoint
- Instance
- Instance type
- Internet gateway
- Key pair
- Secret access key
- Subnet
- Tag
- Target Instance
- Tunnel

8 Compatibility Matrix for AWS

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

Refer to the following sections for details:

GigaVUE-FM Version Compatibility

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

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Controller	GigaVUE-V Series Nodes
5.3.01	v1.4-1	v1.4-1	v1.4-1	v1.4-1
5.4.00	v1.4-1	v1.4-1	v1.4-1	v1.4-1
5.5.00	v1.5-1	v1.5-1	v1.5-1	v1.5-1
5.6.00	v1.6-1	v1.6-1	v1.6-1	v1.6-1
5.7.00	v1.7-1	v1.7-1	v1.7-1	v1.7-1

Supported Features in GigaVUE V Series Nodes

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

Features	GigaVUE V Series v1.0	GigaVUE V Series v1.2	GigaVUE V Series v1.3
Header Transformation	No	No	Yes
Multi-link Support	No	No	Yes
NetFlow Application	No	No	Yes

Features	GigaVUE V Series v1.0	GigaVUE V Series v1.2	GigaVUE V Series v1.3
NAT Support	No	No	Yes

Supported Features in G-vTAP Agents

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

Features	G-vTAP Agent v1.2	G-vTAP Agent v1.3	G-vTAP Agent v1.4/ v1.5/v1.6/v1.7
Dual ENI Support	Yes	Yes	Yes
Single ENI Support	No	Yes	Yes
VXLAN Support	No	Yes	Yes
Agent Pre-filtering			Yes

9 Additional Sources of Information - AWS

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

- *Documentation* on page 101
- *Documentation Feedback* on page 103
- *Contacting Technical Support* on page 103
- *Contacting Sales* on page 103
- *The Gigamon Community* on page 103

Documentation

Table 9-1 lists the documents that are provided for the various Gigamon products. You can download the PDF versions of these documents from the Gigamon Customer Portal.

Table 9-1: Documentation Suite for Gigamon Products

Document	Summary
Hardware Installation Guides	
GigaVUE-HC1 Hardware Installation Guide	Describes how to unpack, assemble, rack-mount, connect, and perform the initial configuration of the various GigaVUE nodes. Also provides reference information for the respective GigaVUE nodes, including specifications.
GigaVUE-HC2 Hardware Installation Guide	
GigaVUE-HC3 Hardware Installation Guide	
GigaVUE TA Series Hardware Installation Guide	
GigaVUE-OS Installation Guide on a White Box	Describes how to install the GigaVUE-OS on a white box.
Software Installation and Upgrade Guides	
GigaVUE-FM Installation and Upgrade Guide	Provides instructions for installing GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM. Also, provides instructions to upgrade GigaVUE-FM.
GigaVUE-OS Upgrade Guide	Describes how to upgrade a GigaVUE H Series node or a GigaVUE TA Series node to the latest GigaVUE-OS.

Document	Summary
Administration Guide	
GigaVUE-OS and GigaVUE-FM Administration Guide	Describes how to use the GigaVUE-FM interface to administer the GigaVUE H Series and GigaVUE TA Series software.
Configuration and Monitoring Guides	
GigaVUE-FM User's Guide	Provides instructions for installing, deploying, and operating the GigaVUE® Fabric Manager (GigaVUE-FM).
GigaVUE Cloud Suite for VMware Configuration Guide	Provides instructions for installing, deploying, and operating the GigaVUE® Virtual Machine (GigaVUE-VM).
GigaVUE Cloud Suite for AWS Configuration Guide	Provides instructions on configuring the GigaVUE Cloud components and setting up traffic monitoring sessions for the respective Cloud platform.
GigaVUE Cloud Suite for Azure Configuration Guide	
GigaVUE Cloud Suite for OpenStack Configuration Guide	
GigaVUE Cloud Suite for Kubernetes Container Configuration Guide	
GigaVUE Cloud Suite for AnyCloud Configuration Guide	Describes how to deploy the GigaVUE Cloud solution in any of the cloud platforms available in the market.
Reference Guides	
GigaVUE-OS CLI Reference Guide	Describes how to use the CLI (Command Line Interface) to configure and operate the GigaVUE H Series and TA Series software.
GigaVUE-OS Cabling Quick Reference Guide	Provides guidelines to the different types of cables to be used to connect the Gigamon devices as well as connect Gigamon devices to third-party devices.
GigaVUE-OS Compatibility and Interoperability Matrix	Provides information about the compatibility and interoperability requirements for the Gigamon devices.
REST API Getting Started Guide	Introduction to the Application Program Interfaces (APIs) for GigaVUE-FM and provides an overview of these REST APIs, basic work flows, and use cases. The APIs are implemented with the Representational State Transfer (REST) architecture. (Deprecation announcement: This has not been updated since 5.4. The content will be merged into the GigaVUE-FM User's Guide in a subsequent release.)
Release Notes	
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, and GigaVUE Cloud Suite Release Notes	Summarizes new features, resolved issues, and known issues in this release for GigaVUE-OS, GigaVUE-FM, and GigaVUE Cloud Suite. Also provides important notes regarding installing and upgrading to this release.

Documentation Feedback

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

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

Contacting Technical Support

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

Contacting Sales

Use the following information to contact sales:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

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