GigaVUE Cloud Suite for AWS Configuration Guide

GigaVUE Cloud Suite

Product Version: 5.8.00

Document Version: 1.0

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

CONTENTS

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*.

Topics:

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 Contact Sales on page 99.

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 Contact Sales on page 99.

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 GigaVUE-FM inside your AWS environment, you can simply launch the GigaVUE-FM instance in your VPC. For installing the GigaVUE-FM instance, Configure Components in AWS.
- 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.

Starting with release 5.8.00, GigaVUE-FM introduces several significant changes, which include improvements in usability and performance. These changes include upgrading and replacing databases and changing the underlying operating system. So, you must migrate your existing configurations and data such as audit logs, events, syslogs, and statistics from your current GigaVUE-FM version (either 5.7 or lower) to GigaVUE-FM 5.8.00. You cannot directly upgrade your GigaVUE-FM instance to release 5.8.00. You must first upgrade to GigaVUE-FM 5.7.01.01, a special release that provides the tools to manage and perform the migration. You can then upgrade to GigaVUE-FM 5.8.00. For details about migrating your GigaVUE-FM instance on AWS platform, refer to the *GigaVUE-FM Migration Guide*.

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 6
- Supported Architecture on page 7

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 10 and G-vTAP Agents on page 11.

  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 13.

- **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 1: Configuration options for Controllers and Nodes on page 7).

- **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 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 8
- Multi-VPC Cloud on page 8
- Centralized Fabric Controllers and Node Configuration on page 9

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.

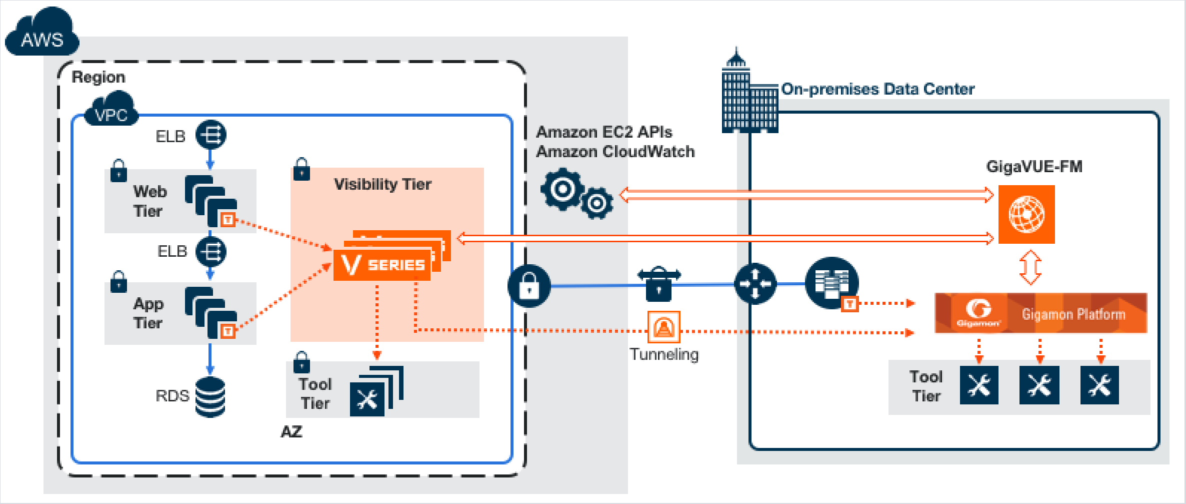


Figure 1: Hybrid Cloud Deployment

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.

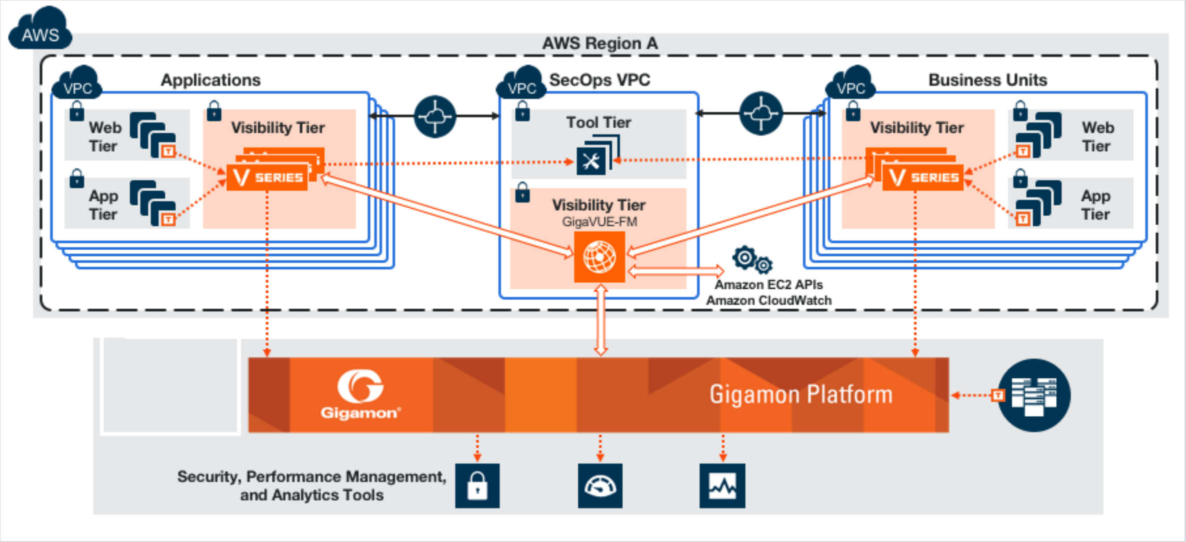


Figure 2: Public Cloud Deployment

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.

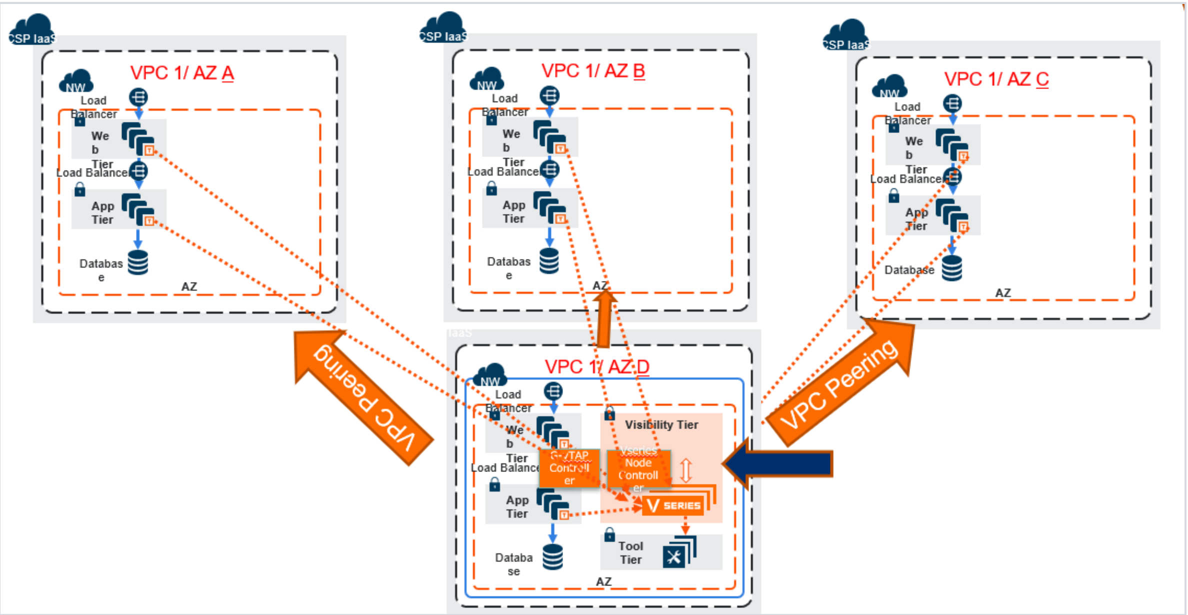


Figure 3: Centralized Controller/V Series Node Deployment Model

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 10
- G-vTAP Agents on page 11

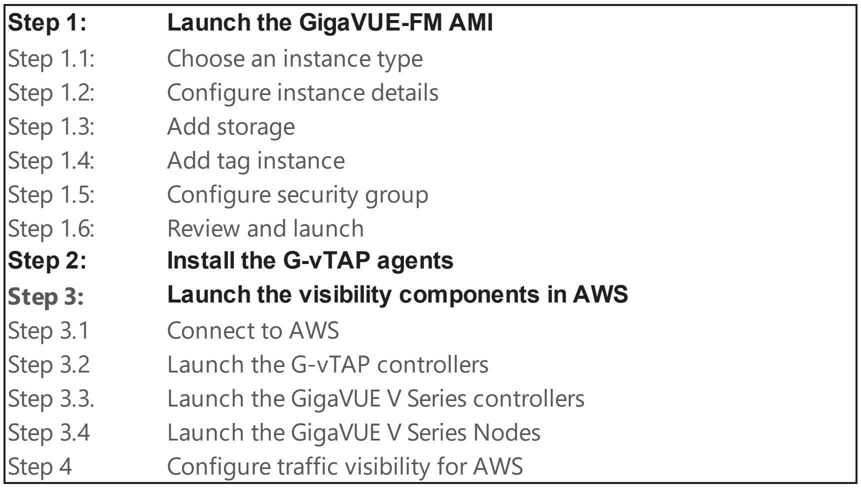
VPN Connectivity

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 84

At a Glance

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



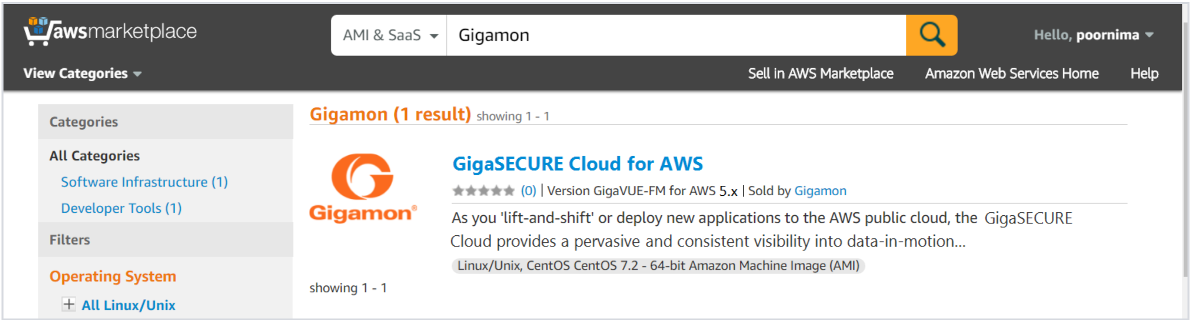
Step 1:	**Launch the GigaVUE-FM AMI**
Step 1.1:	Choose an instance type
Step 1.2:	Configure instance details
Step 1.3:	Add storage
Step 1.4:	Add tag instance
Step 1.5:	Configure security group
Step 1.6:	Review and launch
Step 2:	**Install the G-vTAP agents**
Step 3:	**Launch the visibility components 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 1: AMI in the AWS Public Cloud on page 11 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 1: AMI in the AWS Public Cloud

For purchasing licensing with the BYOL option, contact the Gigamon Sales. Refer to Contact Sales on page 99.

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 12
- Dual ENI Configuration on page 12
- Install G-vTAP Agents on page 13
- Install from Ubuntu/Debian Package on page 13
- Install from RPM Package on page 14

Then refer to Create Images with Agent Installed on page 18.

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 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.

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 18.

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 16
- Install from Red Hat Enterprise Linux and Centos on page 17
- Install from Red Hat Enterprise Linux and Centos with Selinux Enabled on page 17

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 11 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

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.

Create 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.
3. Enter or select the appropriate information as shown in Table 1: Creating a Monitoring Domain on page 20.

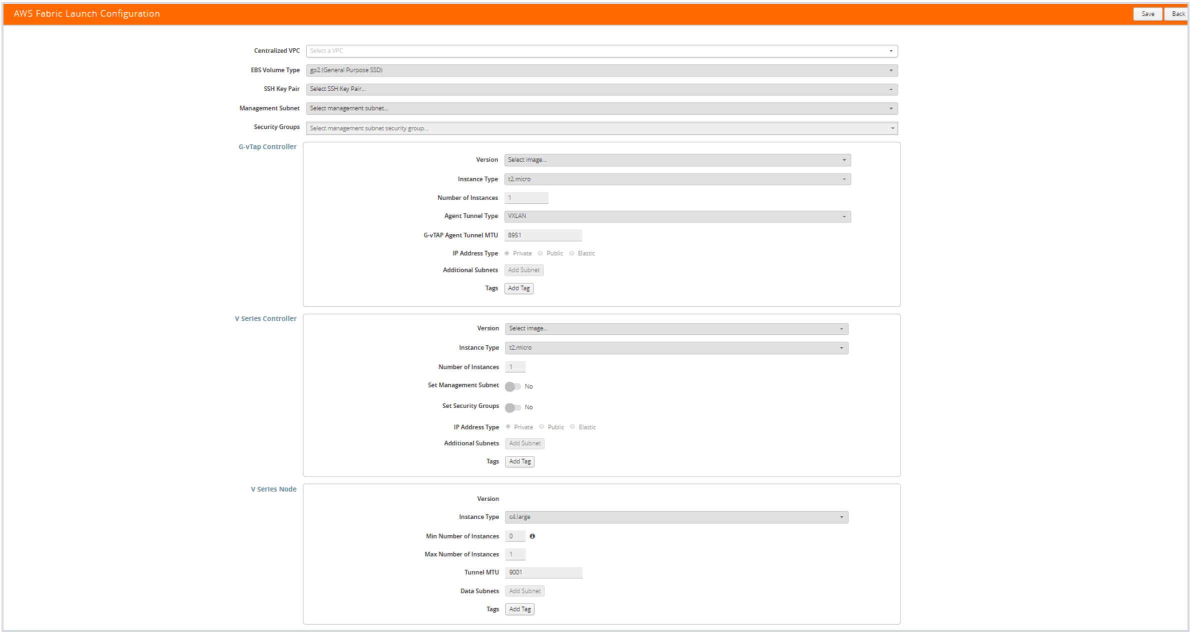
Table 1: Creating a Monitoring Domain

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.

Field	Description
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 • **VPC Traffic Mirroring**: If you select *VPC Traffic Mirrorinng* option as tapping method, then you need not configure the G-vTAP Controller **NOTE:** For VPC Traffic Mirrorning option, additional permissions are required. Refer to the GigaVUE CLoud Suite for AWS Quick Start Guide for details.
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.
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 84
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 84.

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 2: Configuring fabric components

5. Enter or select the appropriate information as shown in

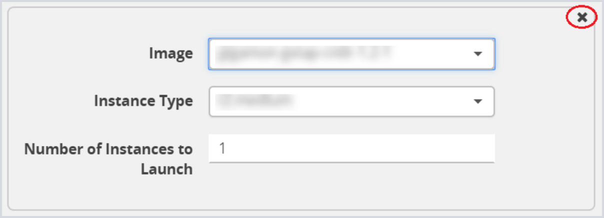
Table 2: AWS Fabric Launch Configuration - Common fields

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*.

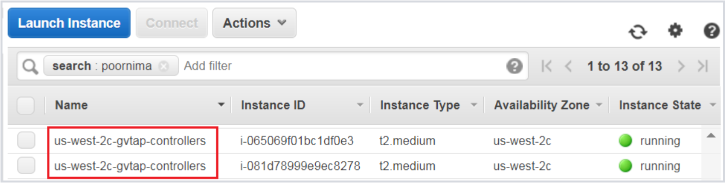
6. Enter or select appropriate information as shown in Table 3: Fields for G-vTAP Controller Configuration on page 23 for G-vTAP Controller Configuration.

Table 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.

Fields	Description
	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 [illegible] Instance Type [illegible] Number of Instances to Launch 1 *Figure 3: 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.
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.

Fields	Description
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.
Additional Subnet(s)	(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 **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.

Fields	Description
Tag(s)	(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, **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-gvtap-controllers. When the G-vTAP Controllers are launched in the VPC, they appear as shown in Figure 4: G-vTAP Controllers with Custom Tag Name on page 26:  Launch Instance Connect Actions search : poornima Add filter 1 to 13 of 13 Name — Instance ID — Instance Type — Availability Zone — Instance State us-west-2c-gvtap-controllers — i-065069f01bc1df0e3 — t2.medium — us-west-2c — ● running us-west-2c-gvtap-controllers — i-081d78999e9ec8278 — t2.medium — us-west-2c — ● running *Figure 4: G-vTAP Controllers with Custom Tag Name*

7. Enter or select appropriate information as shown in Table 3: Fields for G-vTAP Controller Configuration on page 23 for GigaVUE V Series Controller Configuration.

Table 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.

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 5: Fields for V Series Nodes on page 27 for GigaVUE V Series Node Configuration.

Table 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.

Fields	Description
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.
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.

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 on page 29
- Create Tunnel Endpoints on page 32
- Create Monitoring Session on page 34
- Clone Monitoring Session on page 35
- Configure AWS Settings on page 83
- Configure Proxy Server on page 84
- Events on page 86
- Audit Logs on page 90

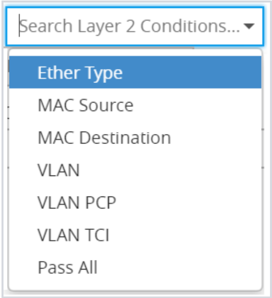
Overview of GigaVUE Cloud in AWS Components

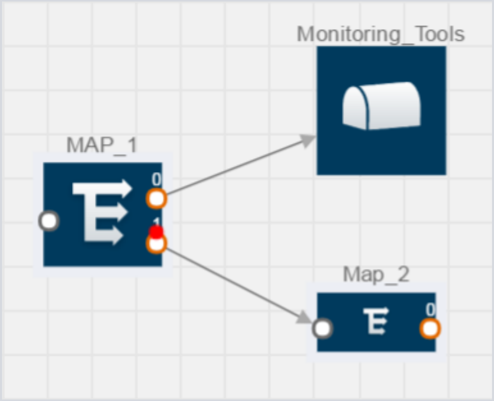
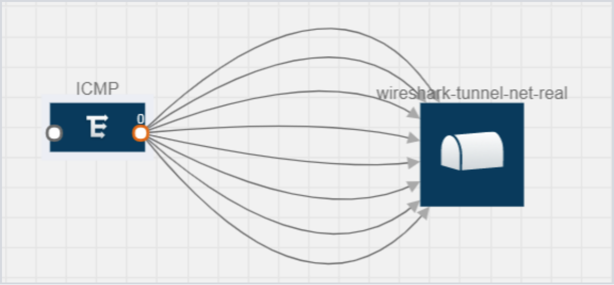
The GigaVUE V Series node aggregates the traffic from multiple G-vTAP agents and filters them using maps. It applies intelligence and optimization to the aggregated traffic using GigaSMART applications such as Flow Mapping™, sampling, slicing, and masking, and distributes them to the tunnel endpoints.

The following table lists the components of the monitoring session:

Table 1: Components of Traffic Visibility Sessions

Parameter	Description
Map	A map (M) is used to filter the traffic flowing through the 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.

Parameter	Description
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 1: Layer 2 Rule Conditions on page 30.  Search Layer 2 Conditions... Ether Type MAC Source MAC Destination VLAN VLAN PCP VLAN TCI Pass All *Figure 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.

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 2: Action Set on page 31), 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 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 3: Action Set with Multiple Links on page 31.  *Figure 3: Action Set with Multiple Links*
Link	A link directs the packets to flow from a map to the destination. The destination could be the other maps, applications, and the monitoring tools. In Figure 2: Action Set on page 31, 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 76.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

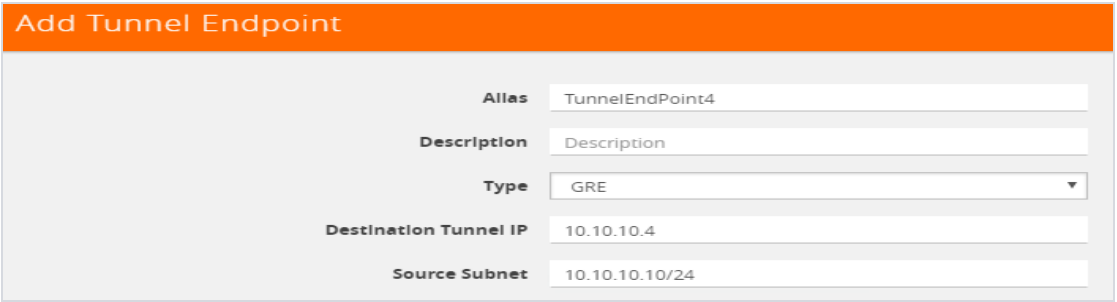
Parameter	Description
Application	An application performs operations such as sampling, slicing, and masking on the traffic.
Inclusion Map	An inclusion map determines the instances or ENIs to be included for monitoring. This map is used only for target selection.
Exclusion Map	An exclusion map determines the instances or ENIs to be excluded from monitoring. This map is used only for target selection.
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: Adding a Tunnel Endpoint on page 32.



Add Tunnel Endpoint

Alias	TunnelEndPoint4
Description	Description
Type	GRE
Destination Tunnel IP	10.10.10.4
Source Subnet	10.10.10.10/24

Figure 4: Adding a Tunnel Endpoint

3. Select or enter the appropriate information as shown in Table 2: Fields for Tunnel Endpoint on page 33.

Table 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.
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:

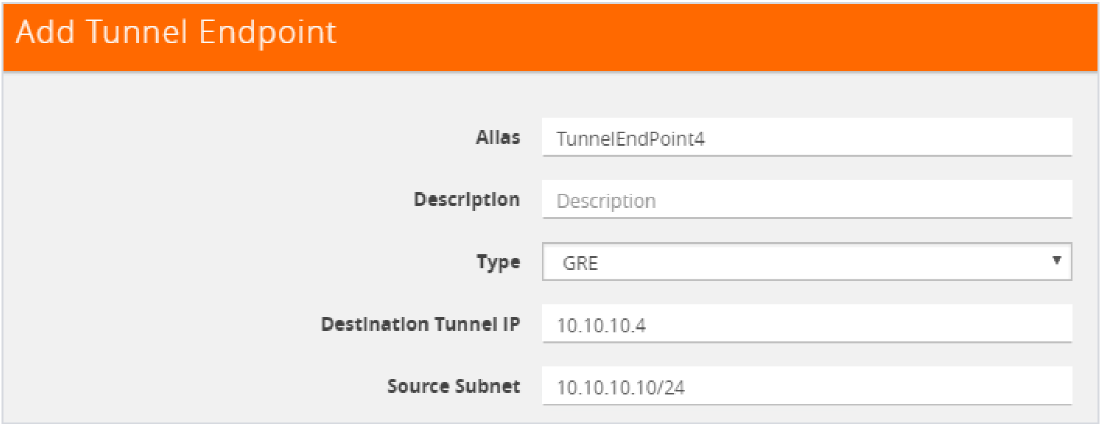
- Create New Session on page 34
- Clone Monitoring Session on page 35
- Add Applications to Monitoring Session on page 46
- Deploy Monitoring Session on page 72
- Add Header Transformations on page 76
- View Statistics on page 79
- View Topology on page 80

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: Adding a Tunnel Endpoint on page 32.



Add Tunnel Endpoint

Alias: TunnelEndPoint4

Description: Description

Type: GRE

Destination Tunnel IP: 10.10.10.4

Source Subnet: 10.10.10.10/24

Figure 5: Creating Monitoring Session

3. Enter the appropriate information in the **Create a New Monitoring Session** dialog box as shown in Table 3: Fields for Creating Monitoring Session on page 35.

Table 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 44.

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: Fields for Cloning the Monitoring Session. on page 36.

Table 4: Fields for Cloning the Monitoring Session.

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

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

Create Map

Each map can have up to 32 rules associated with it. Table 5: Conditions for the Rules on page 36 lists the various conditions that you can select for creating a map, inclusion map, and exclusion map.

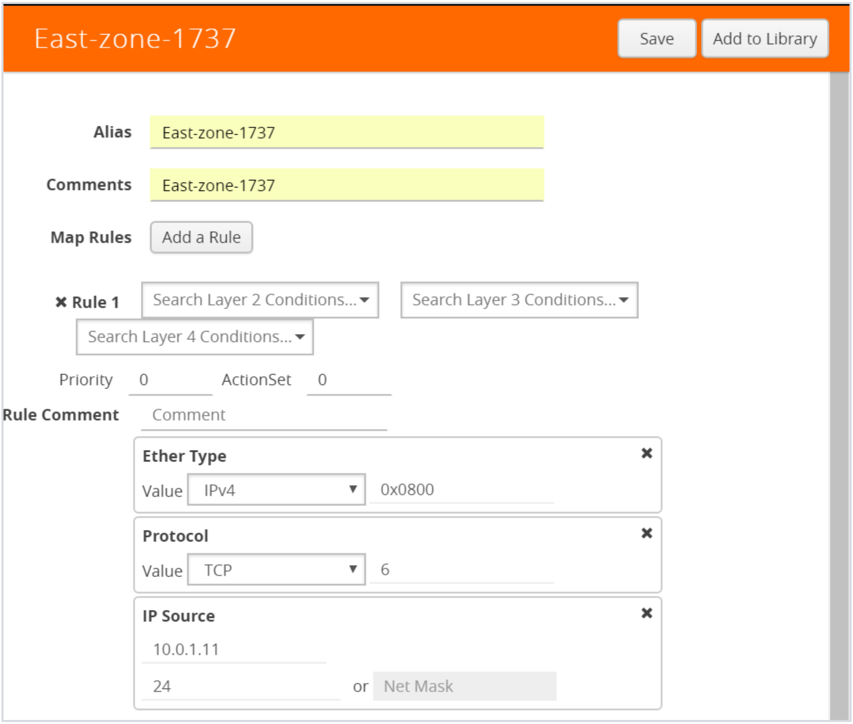
Table 5: Conditions for the Rules

Conditions	Description
L2, L3, and L4 Filters	

Conditions	Description
Ether Type	The packets are filtered based on the selected ethertype. The following conditions are displayed: • IPv4 • IPv6 • ARP • RARP • Other **L3 Filters** If you choose IPv4 or IPv6, the following L3 filter conditions are displayed: • Protocol • IP Fragmentation • IP Time to live (TTL) • IP Type of Service (TOS) • IP Explicit Congestion Notification (ECN) • IP Source • IP Destination **L4 Filters** If you select TCP or UDP protocol, the following L4 filter conditions are displayed: • Port Source • Port Destination
MAC Source	The egress traffic from the instances or ENIs matching the specified source MAC address is selected.
MAC Destination	The ingress traffic from the instances or ENIs matching the specified destination MAC address is selected.
VLAN	All the traffic matching the specified IEEE 802.1q Virtual LAN tag is filtered. Specify a number from 0 to 4094.
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 6: Creating a Map for Tapping Egress Traffic on page 38, the egress traffic from the instances in the subnet 10.0.1.0/24 is selected for monitoring the traffic.


East-zone-1737
Save
Add to Library
Add a Rule
✖ Rule 1
Search Layer 2 Conditions...
Search Layer 3 Conditions...
Search Layer 4 Conditions...
✖
✖
✖

Alias: East-zone-1737

Comments: East-zone-1737

Map Rules

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

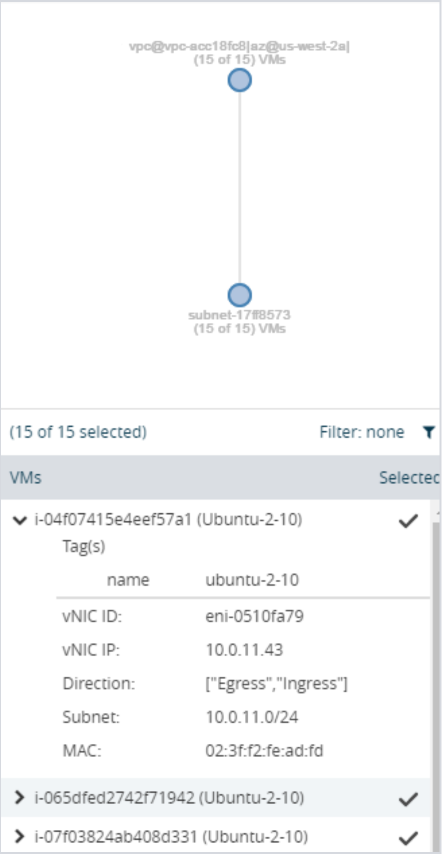
Figure 6: Creating a Map for Tapping Egress Traffic

> **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 34.
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 7: Creating a New Map on page 39.



(15 of 15 selected) Filter: none

VMs	Selectec
i-04f07415e4eef57a1 (Ubuntu-2-10)	✓
i-065dfed2742f71942 (Ubuntu-2-10)	✓
i-07f03824ab408d331 (Ubuntu-2-10)	✓

Tag(s)

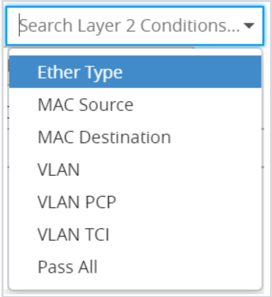
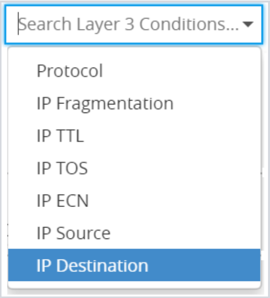
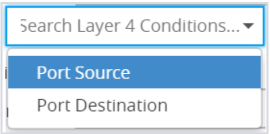
name	ubuntu-2-10
vNIC ID:	eni-0510fa79
vNIC IP:	10.0.11.43
Direction:	["Egress","Ingress"]
Subnet:	10.0.11.0/24
MAC:	02:3f:f2:fe:ad:fd

Figure 7: Creating a New Map

5. Enter the appropriate information for creating a new map as shown in Table 6: Fields for Creating a New Map on page 40.

Table 6: Fields for Creating a New Map

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

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 8: L2 Conditions on page 41.  Search Layer 2 Conditions... Ether Type MAC Source MAC Destination VLAN VLAN PCP VLAN TCI Pass All *Figure 8: L2 Conditions* **c.** Select a condition from the **Search L3 Conditions** drop-down list and specify a value. Refer to Figure 9: L3 Conditions on page 41.  Search Layer 3 Conditions... Protocol IP Fragmentation IP TTL IP TOS IP ECN IP Source IP Destination *Figure 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 10: L4 Conditions on page 41.  Search Layer 4 Conditions... Port Source Port Destination *Figure 10: L4 Conditions*

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 11: Editing or Deleting a Map on page 42.

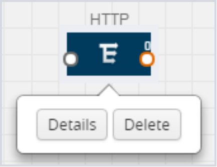


Figure 11: Editing or Deleting a Map

Click the **Show Targets** button to view the monitoring targets highlighted in orange. Refer to Figure 12: Viewing the Topology on page 43.

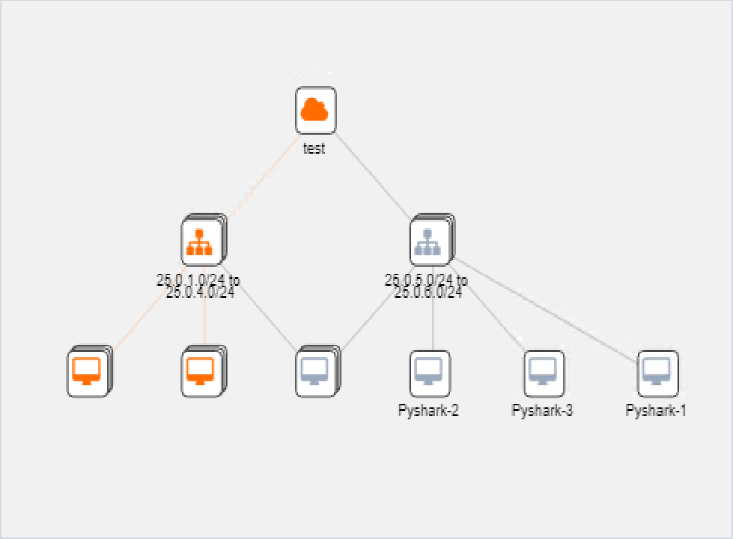
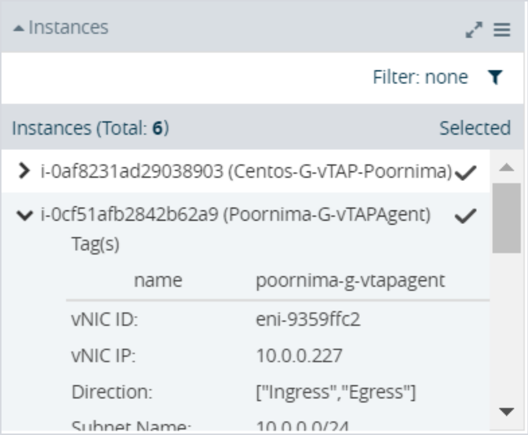


Figure 12: Viewing the Topology

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 13: Viewing Instance Details on page 43.



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 13: Viewing Instance Details

Filter the instances based on the Instance Name Prefix, IP address, or the MAC address. Refer to Figure 14: Filtering the instances on page 44.

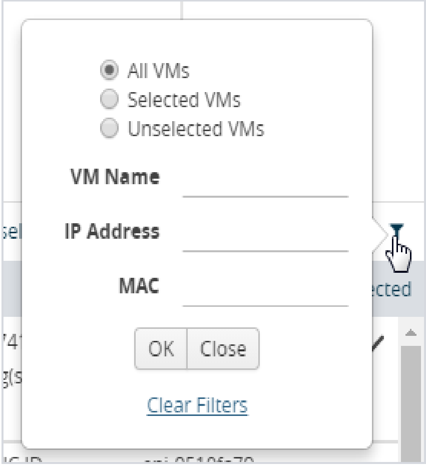


Figure 14: Filtering the instances

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:

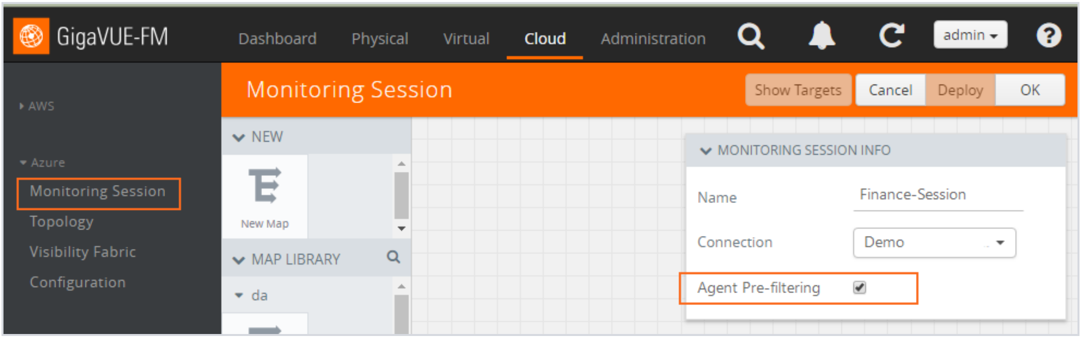
- The agent pre-filtering option can be enabled or disabled at the monitoring-session level and is enabled by default.
- When enabled, traffic is filtered at the G-vTAP agent-level, before mirroring to the V Series Nodes. Consequently, traffic flow to the V Series Nodes is reduced, which reduces the 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:

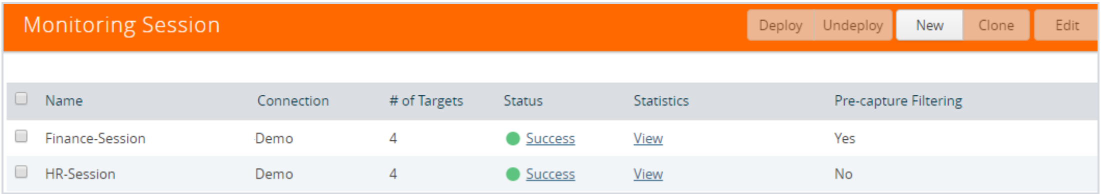
1. **Cloud > AWS > Monitoring Session**.
2. Open a monitoring session by doing one of the following:
   a. Click **New** to create a new session.
   b. Click the check box next to a session and then click **Edit** to edit an existing session.



Name	Finance-Session
Connection	Demo
Agent Pre-filtering	☑

Figure 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 50
- NetFlow on page 53

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.

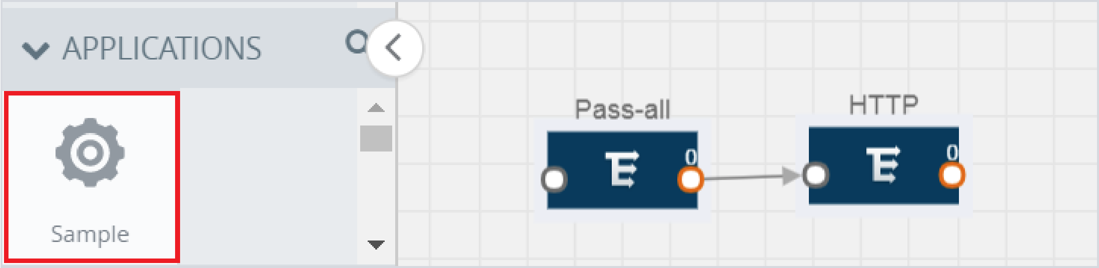


Figure 16: Dragging the Sample Application

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

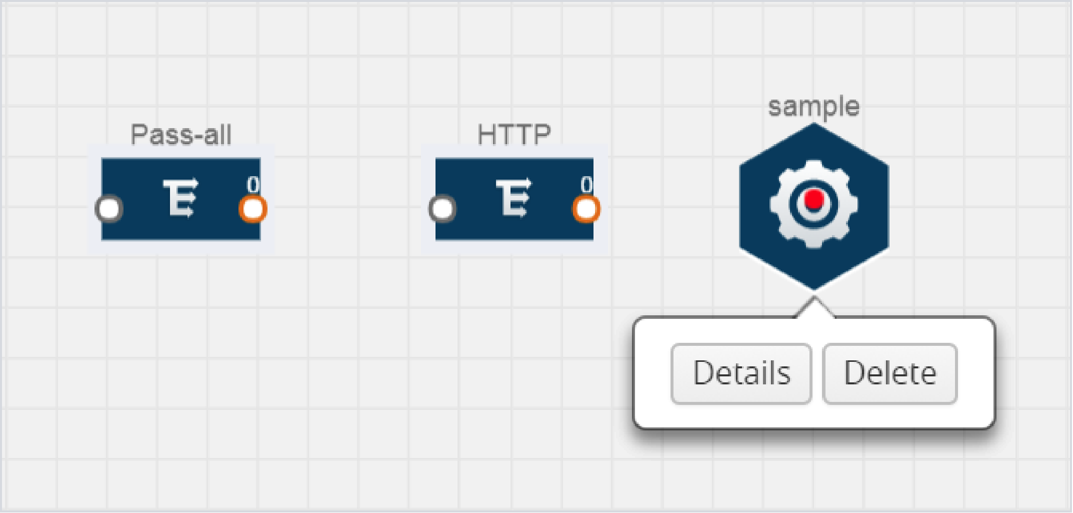
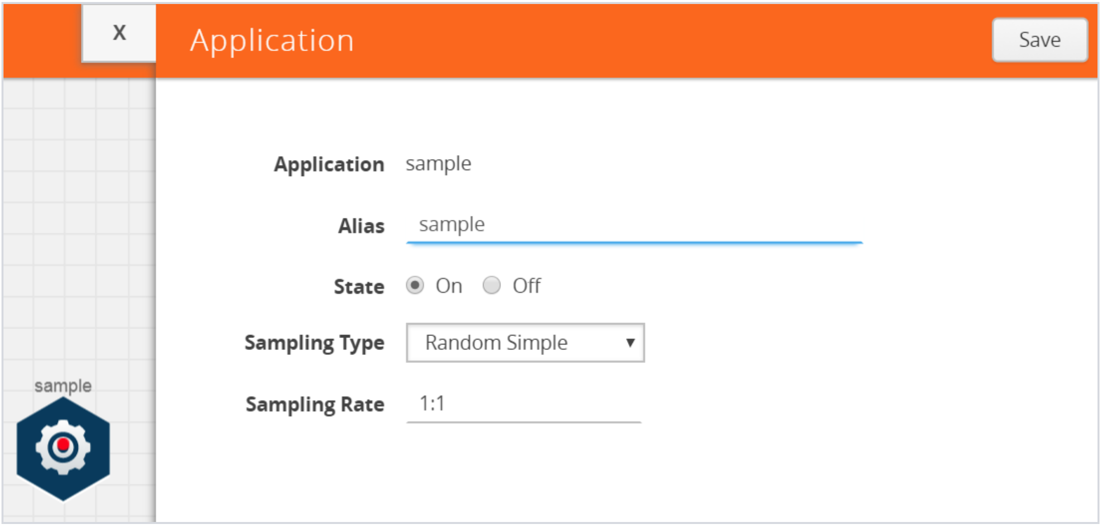


Figure 17: Selecting Details

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



Application sample

Alias sample

State ● On ○ Off

Sampling Type Random Simple

Sampling Rate 1:1

Figure 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.

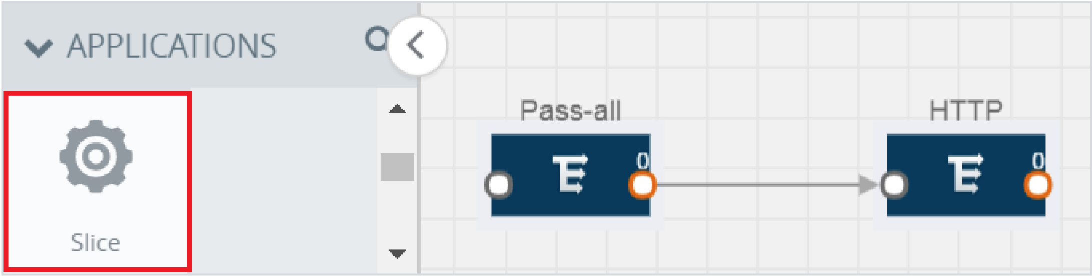


Figure 19: Dragging the Slice Application

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

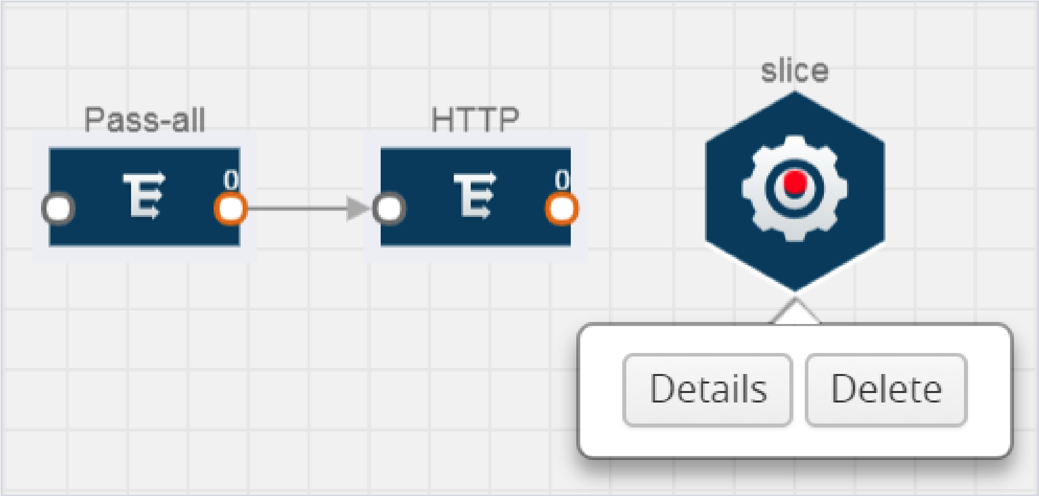
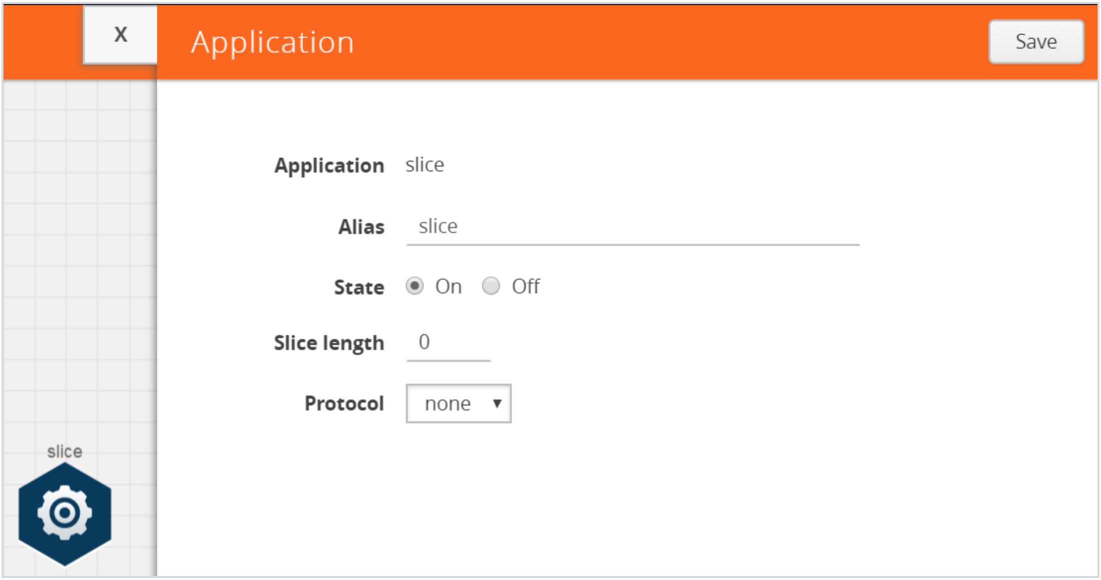


Figure 20: Selecting Details

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



Application

Application slice

Alias slice

State ● On ○ Off

Slice length 0

Protocol none ▾

Figure 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.

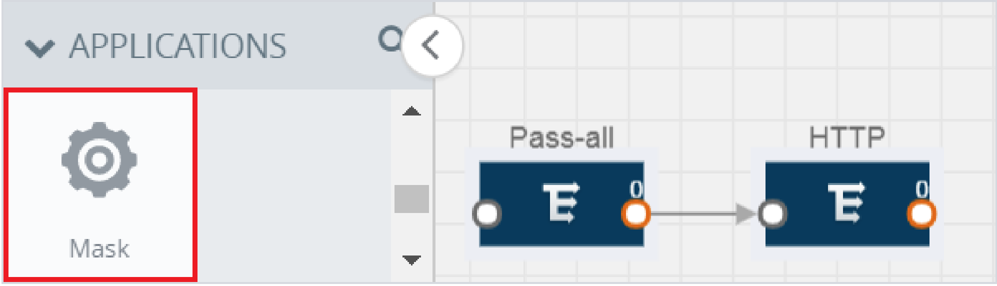


Figure 22: Dragging the Mask Application

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

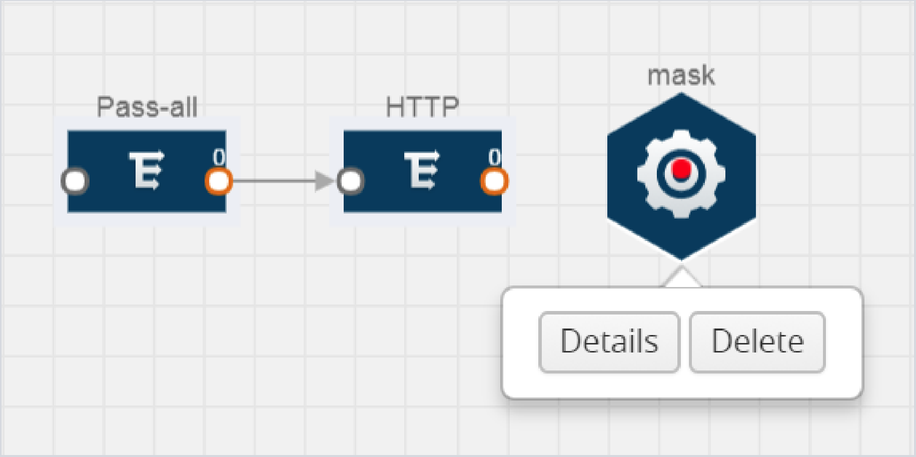
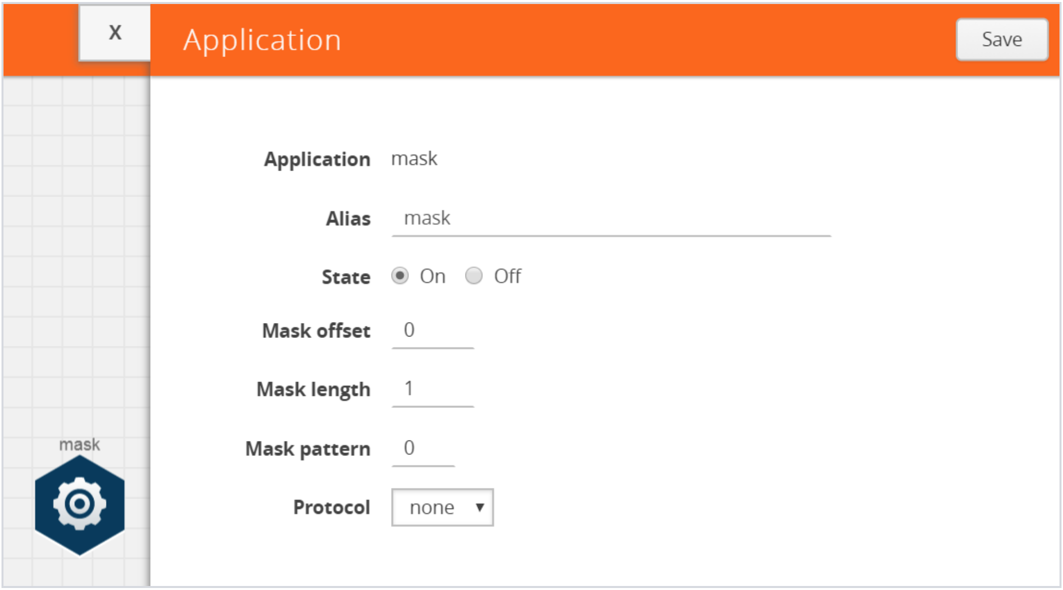


Figure 23: Selecting Details

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 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 55. 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 58.

Figure 25: NetFlow on GigaVUE V Series Node on page 54 shows an example of a NetFlow application created on a GigaVUE V Series node in the monitoring session.

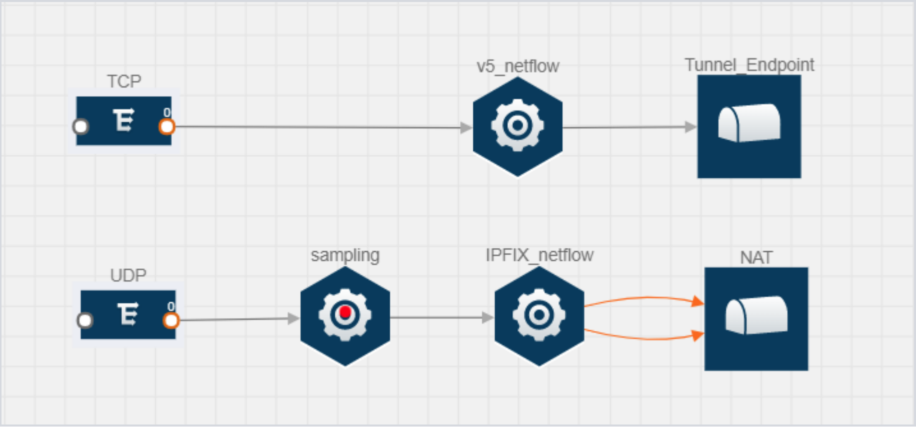


Figure 25: NetFlow on GigaVUE V Series Node

The NetFlow record generation is performed on GigaVUE V Series node running the NetFlow application. In Figure 25: NetFlow on GigaVUE V Series Node on page 54, 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 65.

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

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

- IPFIX—The extended version of version 9 supports variable length fields as well as enterprise-defined fields.

Match/Key Fields

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

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

Table 7: Match/Key Elements

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

	Description	Supported NetFlow Versions
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a key field.	IPFIX
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9 and IPFIX
IP DSCP	Configures the value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field as a key field.	IPFIX
IP Header Length	Configures the length of the IP header as a key field.	IPFIX
IP Precedence	Configures the value of the IP Precedence as a key field.	IPFIX
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9 and IPFIX
IP Total Length	Configures the total length of the IP packet as a key field.	IPFIX
IP TTL	For IPv4, configures the value of Time to Live (TTL) as a key field. For IPv6, configures the value of the Hop Limit 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

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

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

Collect/Non-Key Fields

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

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

Table 8: Collect/Non-Key Elements

	Description	Supported NetFlow Versions
Counter		
Byte Count	Configures the number of octets since the previous report in incoming packets for the current flow as a non-key field.	v9 and IPFIX
Packet Count	Configures the number of incoming packets since the previous report for this flow as a non-key field.	v9 and IPFIX
Data Link		
Destination MAC	Configures the destination MAC address as a non-key field.	v9 and IPFIX
Egress Des MAC	Configures the post source MAC address as a non-key field.	IPFIX
Ingress Des MAC	Configures the IEEE 802 destination MAC address as a non-key field.	IPFIX

	Description	Supported NetFlow Versions
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

	Description	Supported NetFlow Versions
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a non-key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a non-key field.	IPFIX
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9
IP Version	Configures the IP version field in the IP packet header as a key field.	v9
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a non-key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport header as a non-key field.	v9 and IPFIX
TCP AcK Number	Configures the acknowledgment number in the TCP header as a non-key field.	IPFIX

	Description	Supported NetFlow Versions
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.

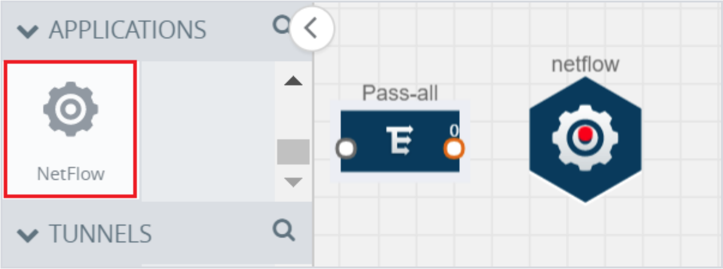


Figure 26: Dragging the NetFlow Application

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

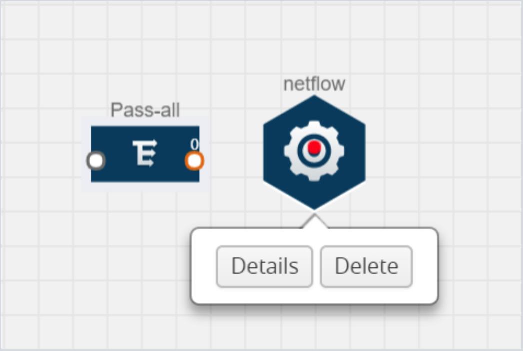
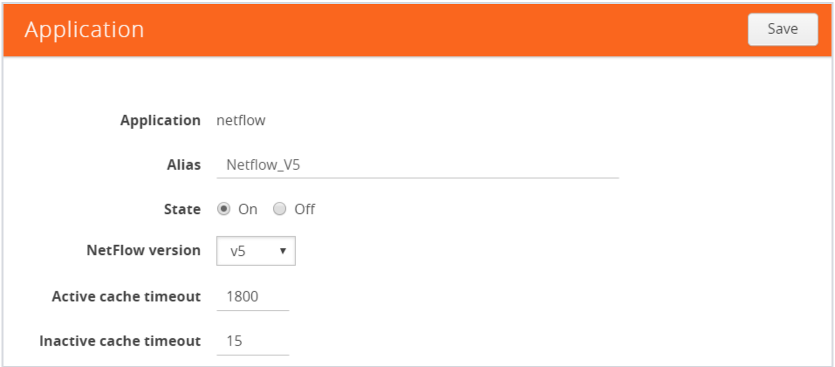


Figure 27: Selecting Details

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 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 67.

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.

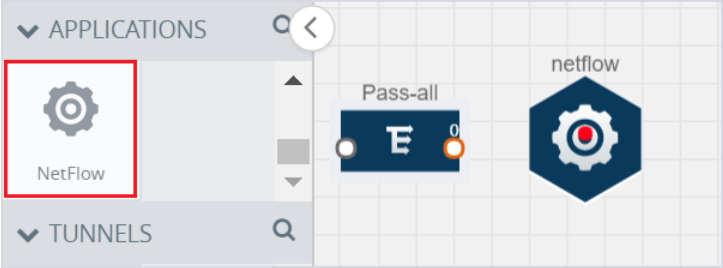


Figure 29: Dragging the NetFlow Application

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

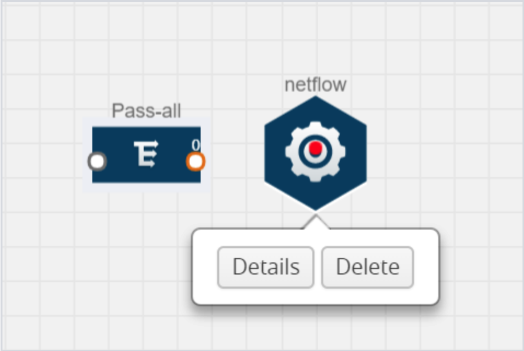
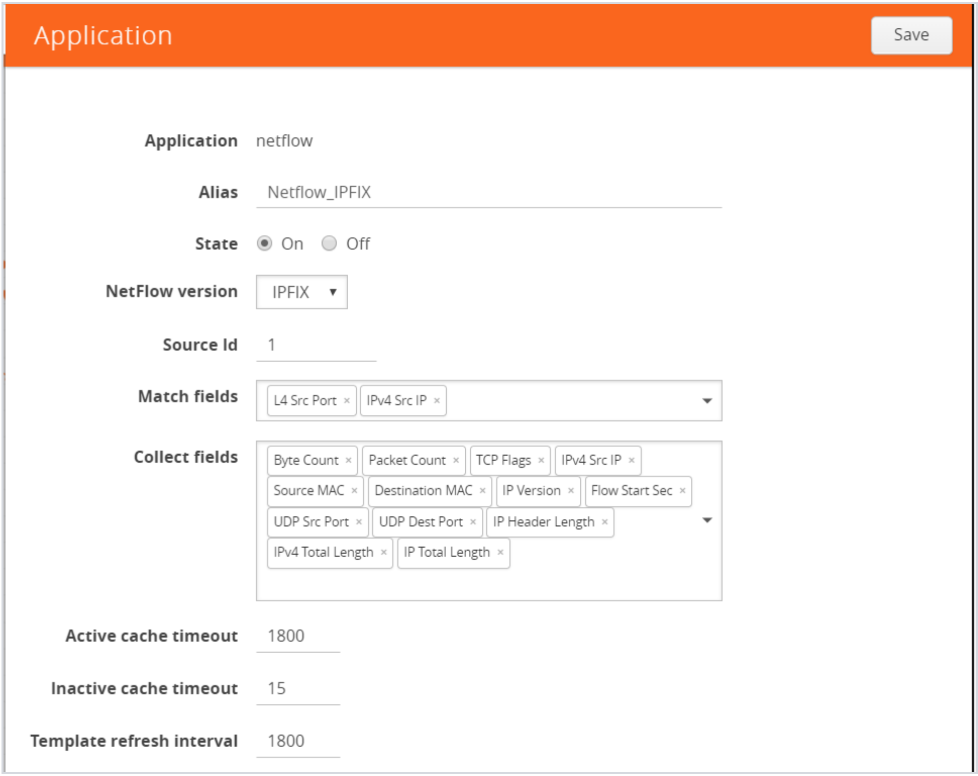


Figure 30: Selecting NetFlow Details

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 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 55.
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 58.
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 67.

Network Address Translation (NAT)

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

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

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

Add NAT

To add a NAT device:

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

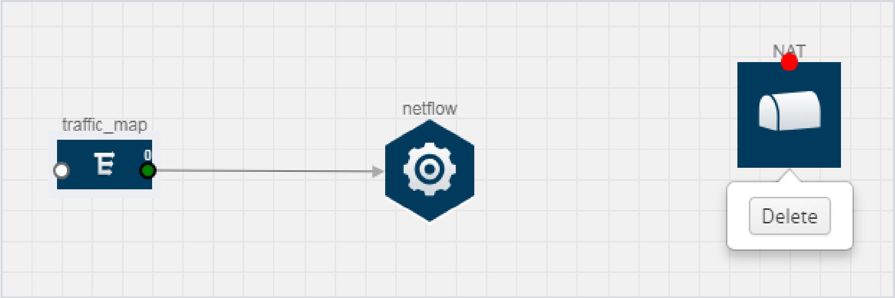
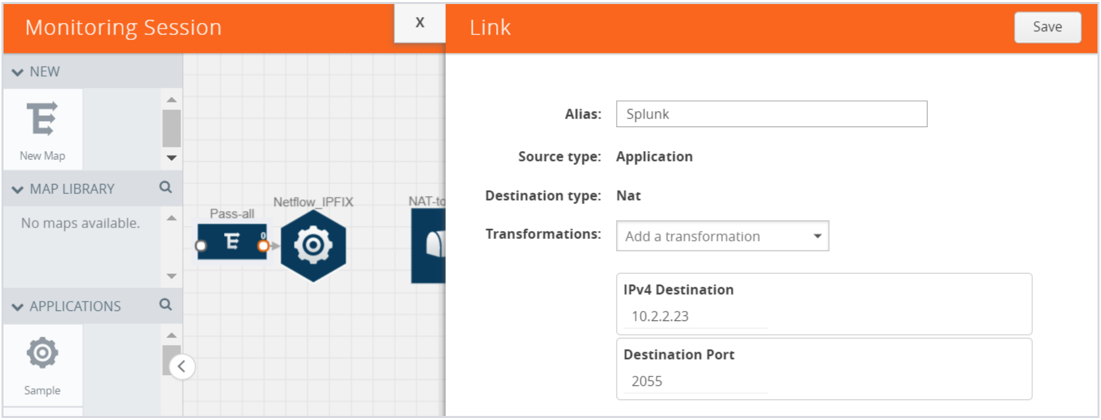


Figure 32: Adding NAT

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 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.

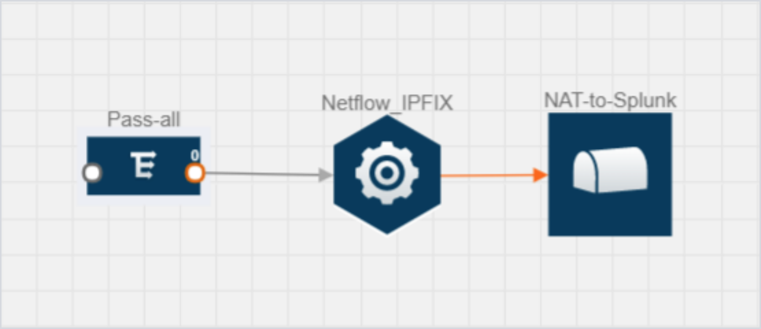


Figure 34: Linking NetFlow to NAT

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

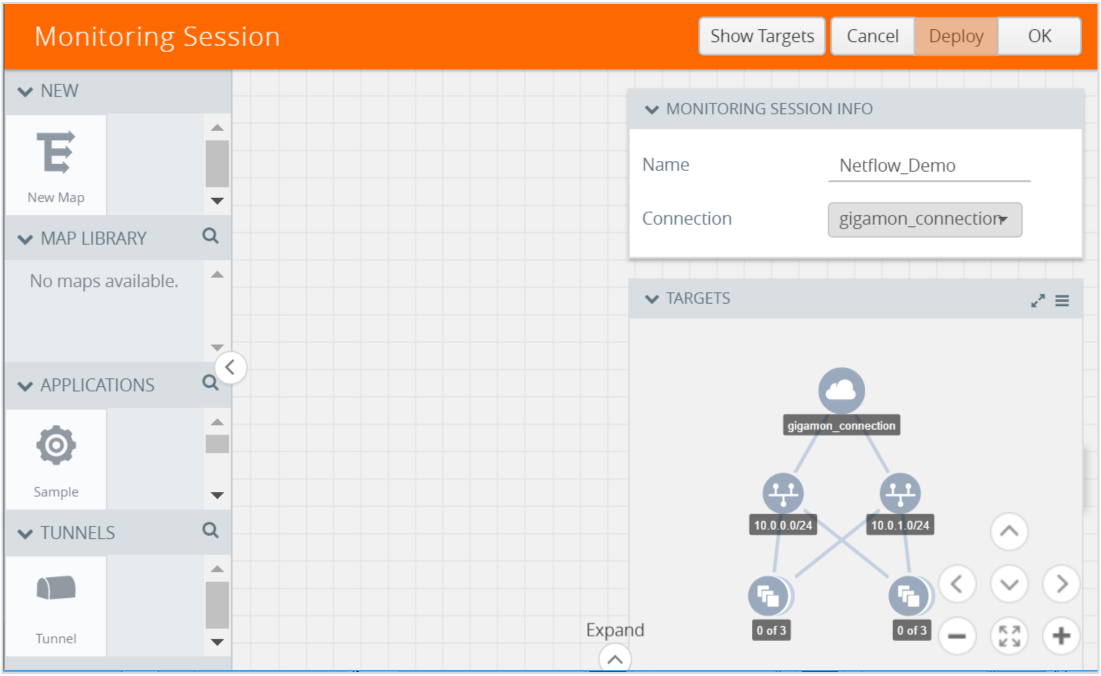
NetFlow Examples

This section provides an example to demonstrate the NetFlow application configuration in the GigaVUE V Series nodes. Refer Example 1 on page 67 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 34.

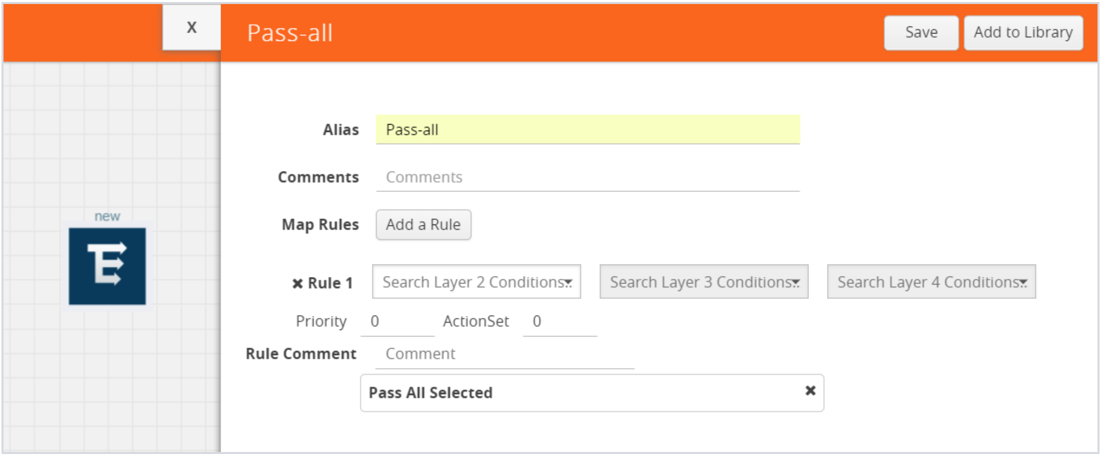


Name Netflow_Demo

Connection gigamon_connection

Figure 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 35.


x
Pass-all
Save
Add to Library
new
Add a Rule
Search Layer 2 Conditions
Search Layer 3 Conditions
Search Layer 4 Conditions

Alias Pass-all

Comments Comments

Map Rules Add a Rule

✖ Rule 1

Priority 0 ActionSet 0

Rule Comment Comment

Pass All Selected ✖

Figure 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.

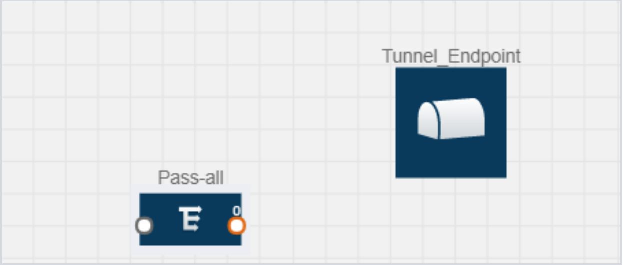


Figure 37: Adding a Tunnel

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.

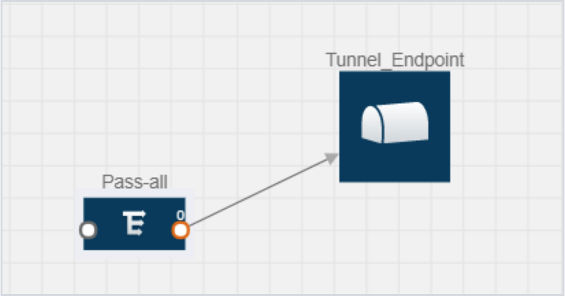


Figure 38: Creating a Link from Pass-all Map to Tunnel_Endpoint

5. Drag and drop a v5 NetFlow application.

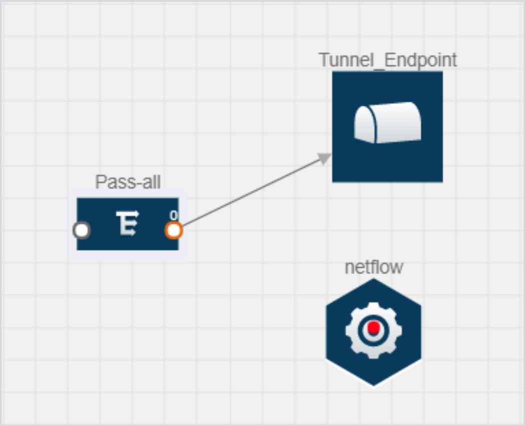
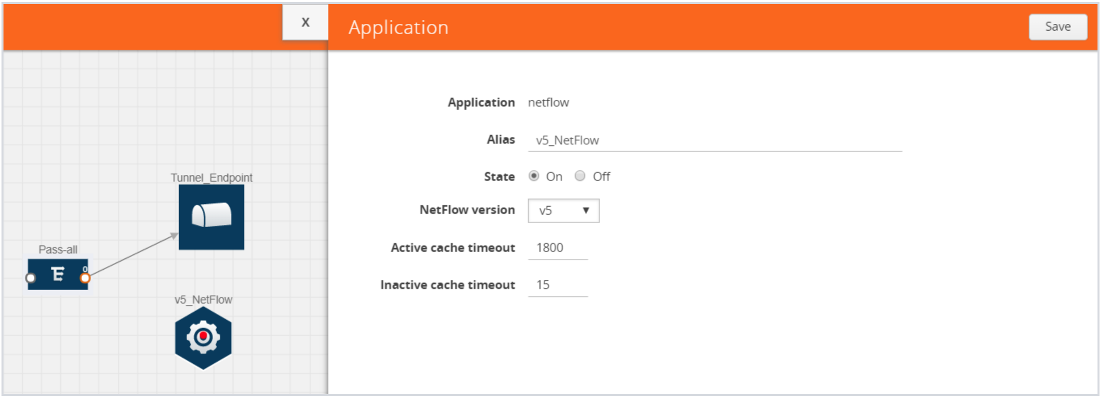


Figure 39: Adding a link from Pass-all Map to Tunnel_Endpoint

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 61.



Application netflow

Alias v5_NetFlow

State ● On ○ Off

NetFlow version v5

Active cache timeout 1800

Inactive cache timeout 15

Figure 40: Configuring the NetFlow Application

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

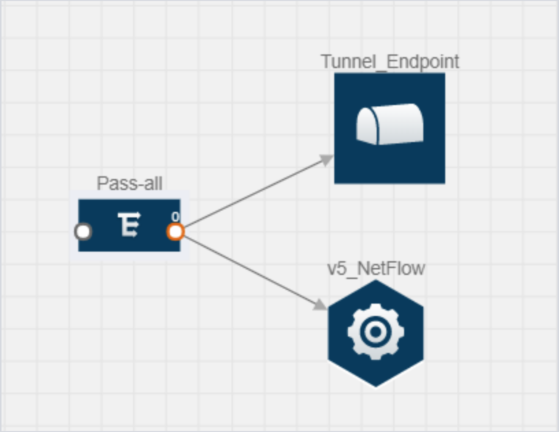


Figure 41: Adding a link from Pass-all Map to v5_NetFlow

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

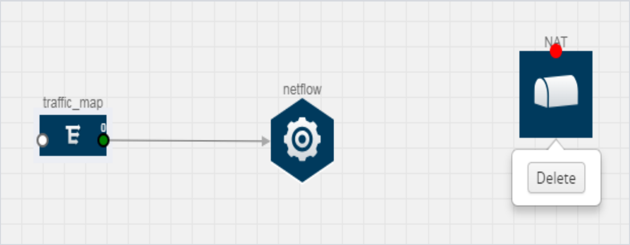
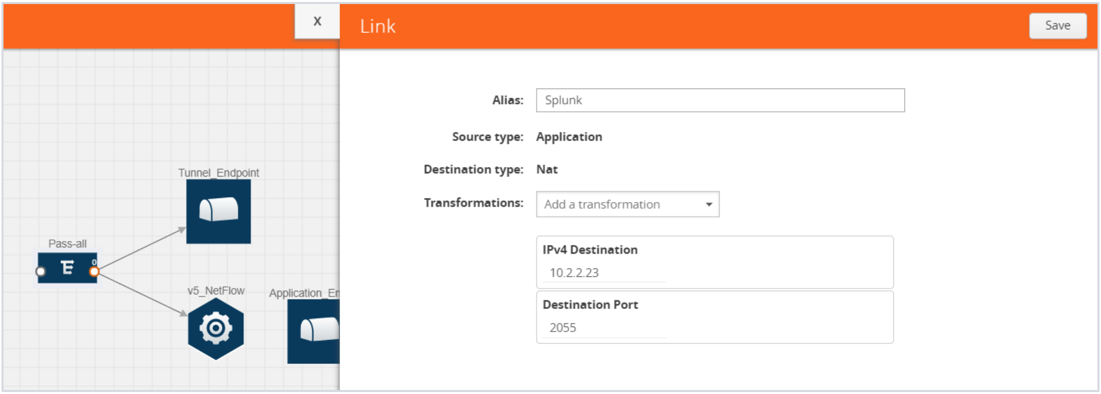


Figure 42: Adding a NAT Device

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 66.



Alias: Splunk

Source type: Application

Destination type: Nat

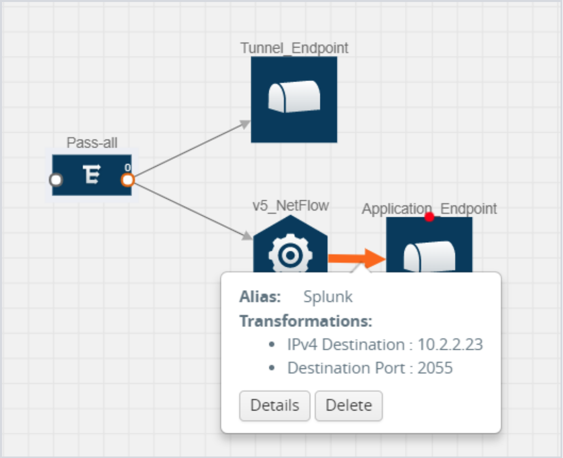
Transformations: Add a transformation

IPv4 Destination 10.2.2.23

Destination Port 2055

Figure 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 44: Viewing the Transformation Dialog Box

Deploy Monitoring Session

To deploy the monitoring session:

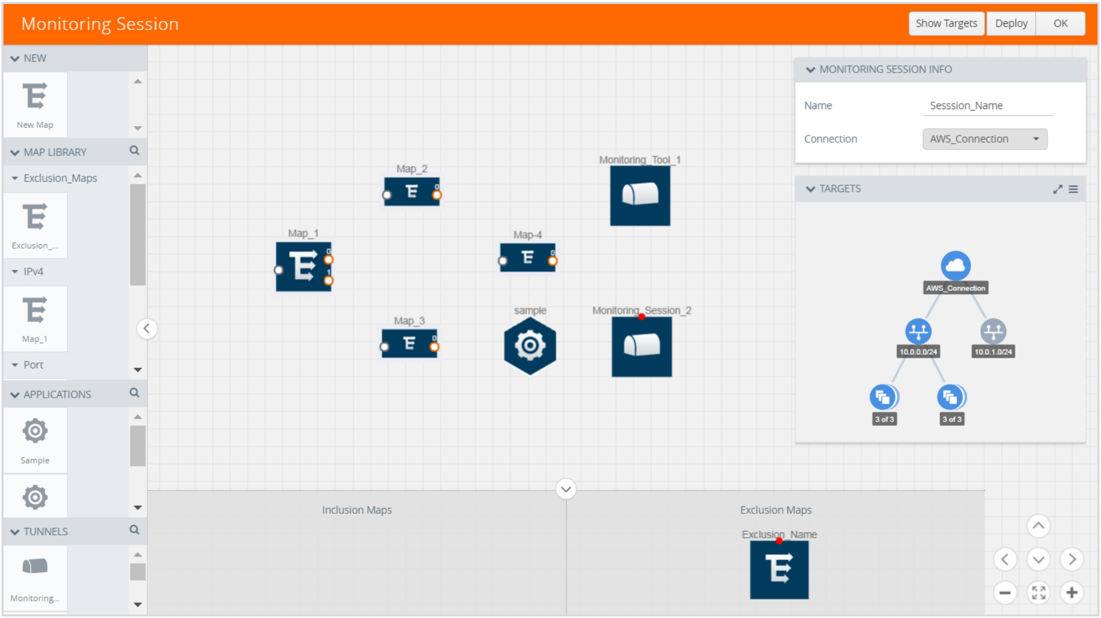
1. Drag and drop one or more maps from the **MAP Library** to the workspace.
2. (Optional) To add Inclusion and Exclusion maps, drag and drop the maps from the Map Library to their respective section at the bottom of the workspace.

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 46.

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

   Figure 45: Dragging and Dropping the Maps, Applications, and Monitoring Tools on page 73 illustrates three maps, one exclusion map, one application, and two tunnel endpoints dragged and dropped to the workspace.



Name: Sesssion_Name

Connection: AWS_Connection

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

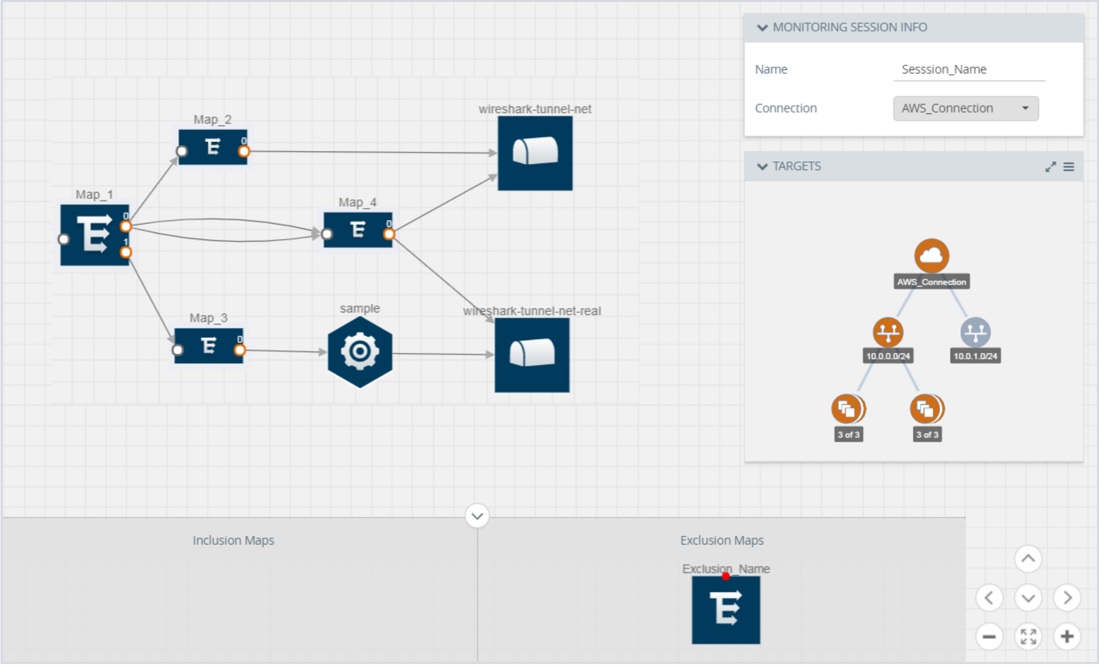
> **NOTE:** You can add up to 8 links from a single map to different maps, applications, or monitoring tools.

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 46: Connecting the Maps, Applications, and Monitoring Tools on page 74. For information about adding link transformation, refer to Add Header Transformations on page 76.

6. Hover your mouse on the application, click the red dot, and drag the link (arrow) over to the tunnel endpoints.

   In Figure 46: Connecting the Maps, Applications, and Monitoring Tools on page 74, the traffic matching the rules in each action set is routed to maps, applications, or monitoring tools.



Name: Sesssion_Name

Connection: AWS_Connection

Figure 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.

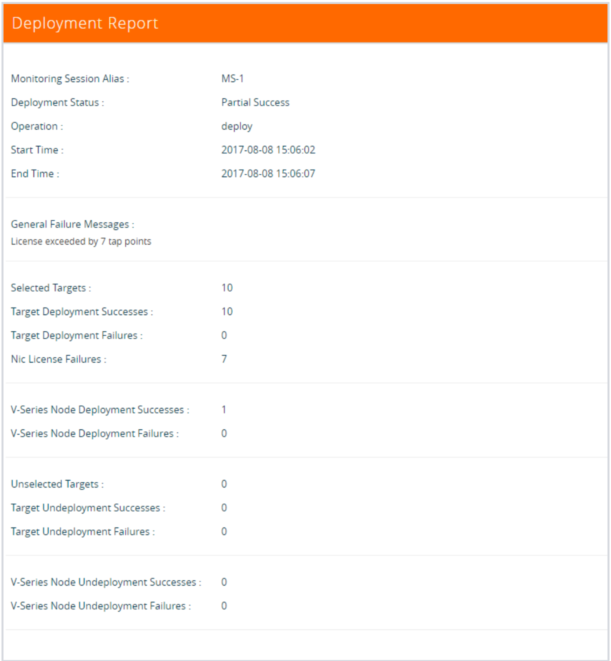
8. Click **Deploy** to deploy the monitoring session.

   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 47: Deployment Status on page 75.



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 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

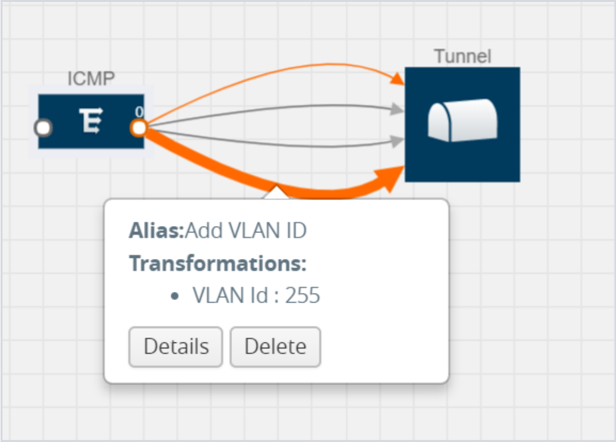
Header transformation is performed on a link in a monitoring session. You can select a link and modify the packet header before they are sent to the destination. The header transformation feature is supported only with GigaVUE V Series node version 1.3-1 and above.

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 48: Action Set with Multiple Links on page 77, 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 48: Action Set with Multiple Links

GigaVUE V Series node supports the following header transformations:

Table 9: Header Transformations

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

Option	Description
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.

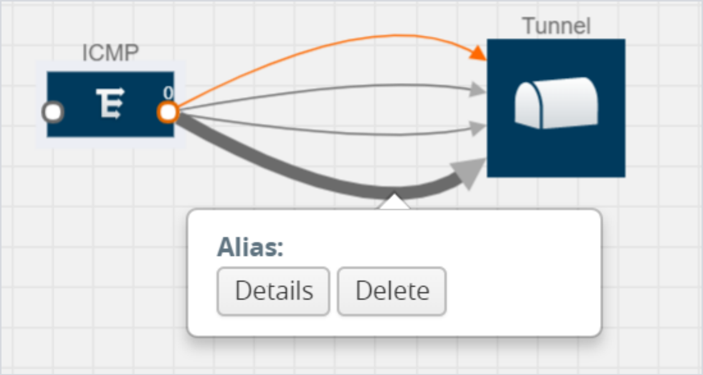
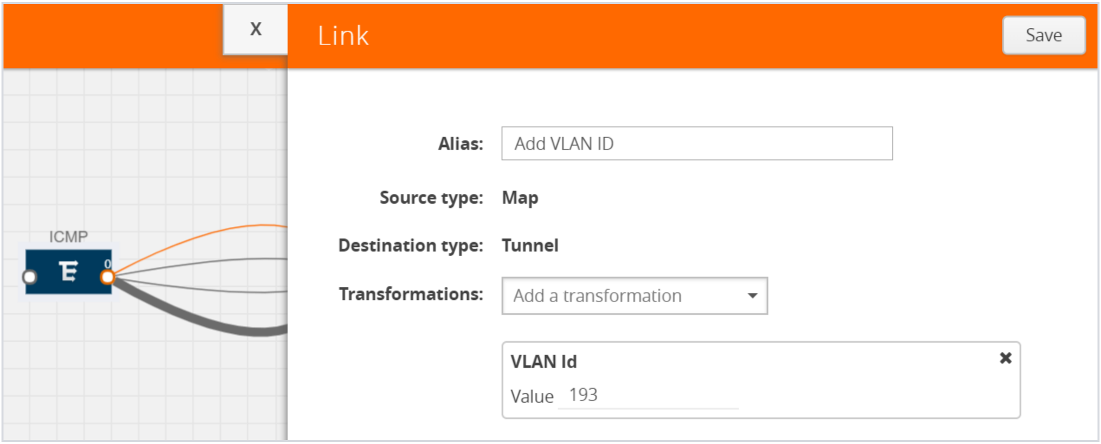


Figure 49: Opening the Link Quick View

1From 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 50: Adding Transformation

2. Click **Save**. The selected transformation is applied to the packets passing through the link.
3. 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.

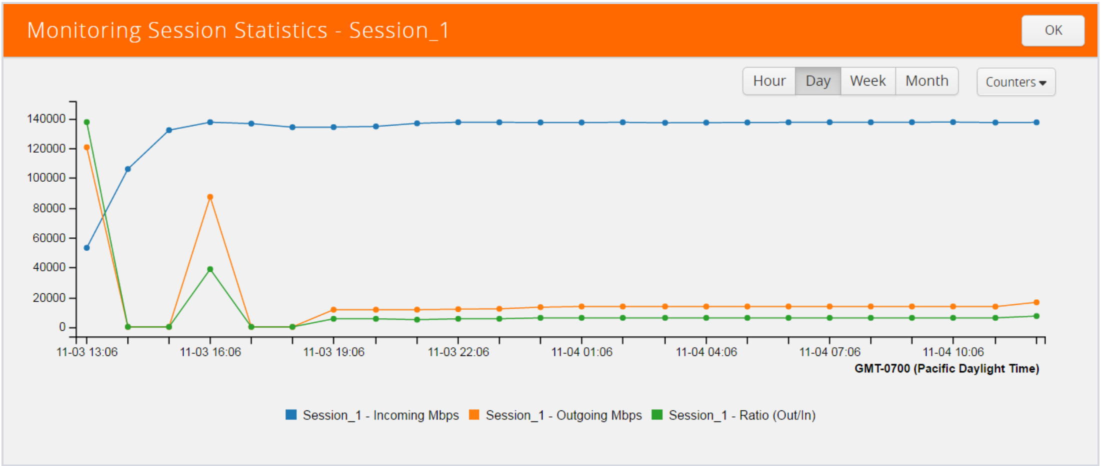
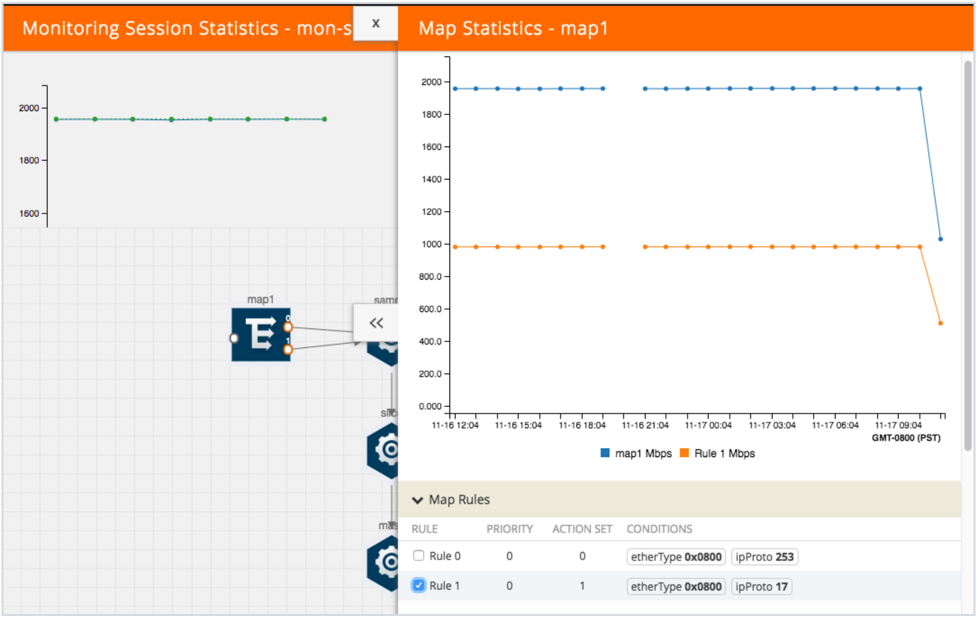


Figure 51: Viewing the Monitoring Session Statistics

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.



Map Rules

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

Figure 52: Viewing the Map Statistics

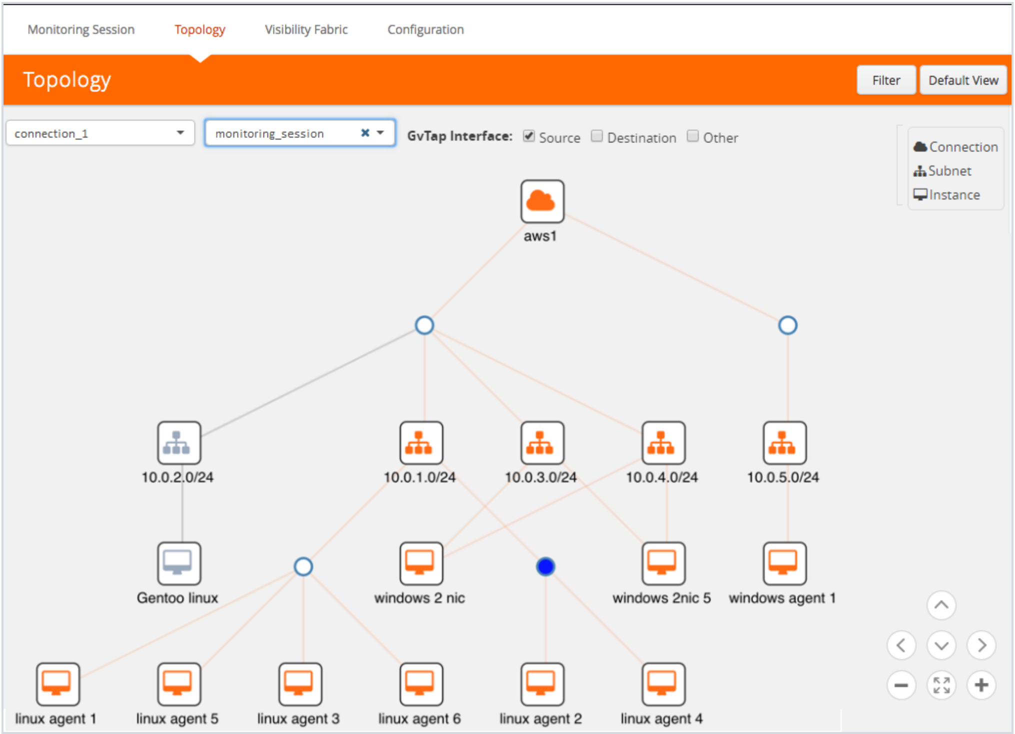
View Topology

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.



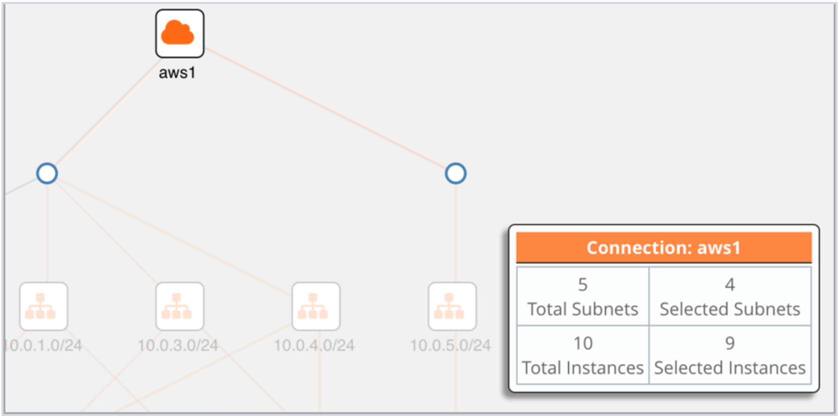
connection_1

monitoring_session

GvTap Interface: ☑ Source □ Destination □ Other

Figure 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 54: Filtering in Topology View on page 83.

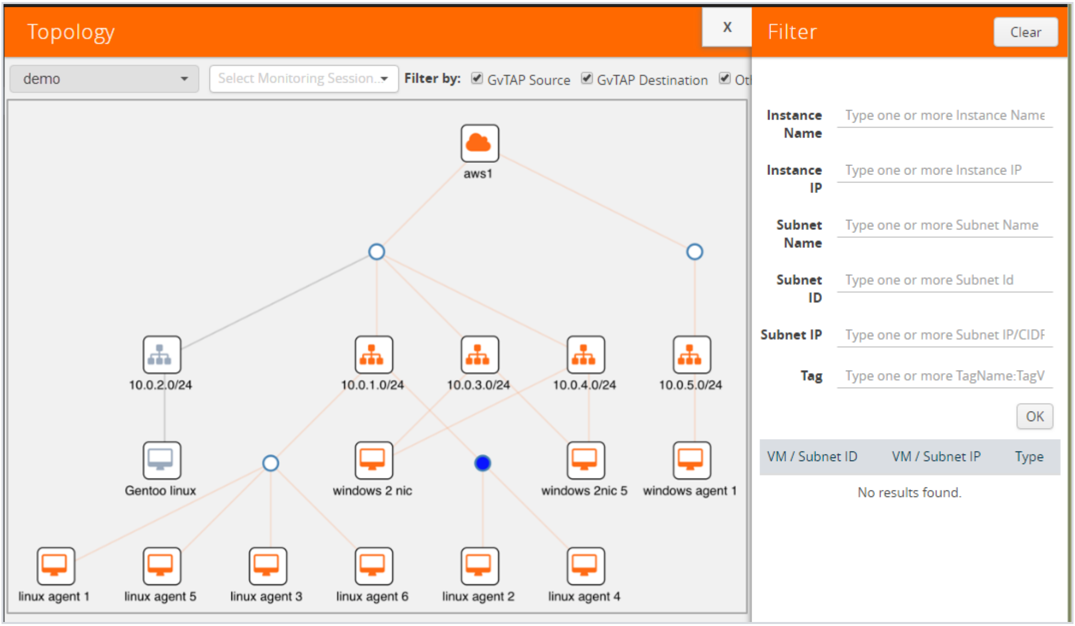


Figure 54: Filtering in Topology View

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 10: AWS Settings on page 83 for more information about the settings:

Table 10: AWS Settings

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of VPC connections you can establish in GigaVUE-FM.

Settings	Description
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
AWS secret region	Specifies the AWS secret region. The following are the available AWS secret regions: • **C2S**—Commercial Cloud Services. Refer to *GigaVUE Cloud Suite for AWS Secret Regions Configuration Guide* for more information. • **SC2S**—Secret Commercial Cloud Services. Refer to *GigaVUE Cloud Suite for AWS Secret Regions Configuration Guide* for more information. • **Other**—Regular AWS Cloud Services

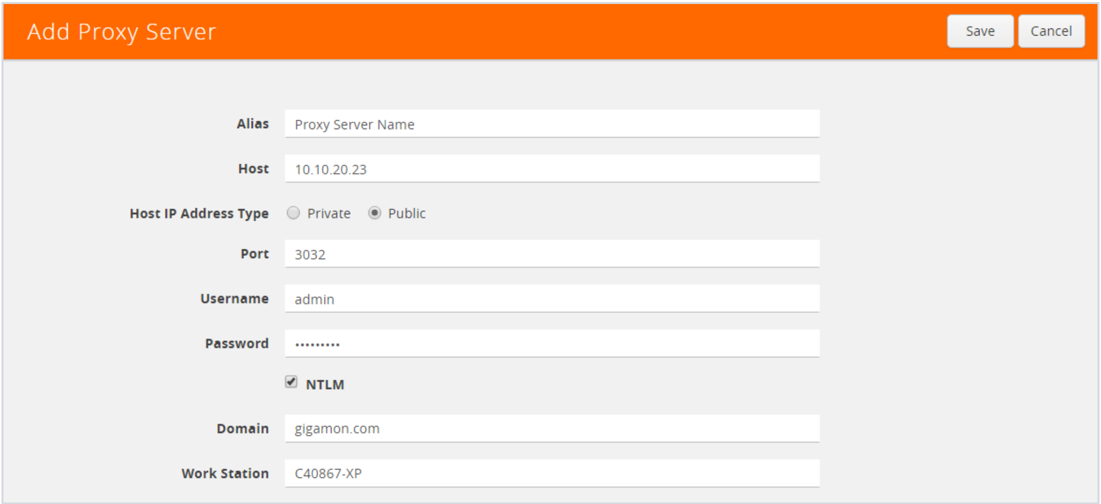
Configure Proxy Server

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 55: Adding a Proxy Server on page 85.



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 55: Adding a Proxy Server

3. Select or enter the appropriate information as shown in Table 11: Fields for Proxy Sever Configuration on page 85.

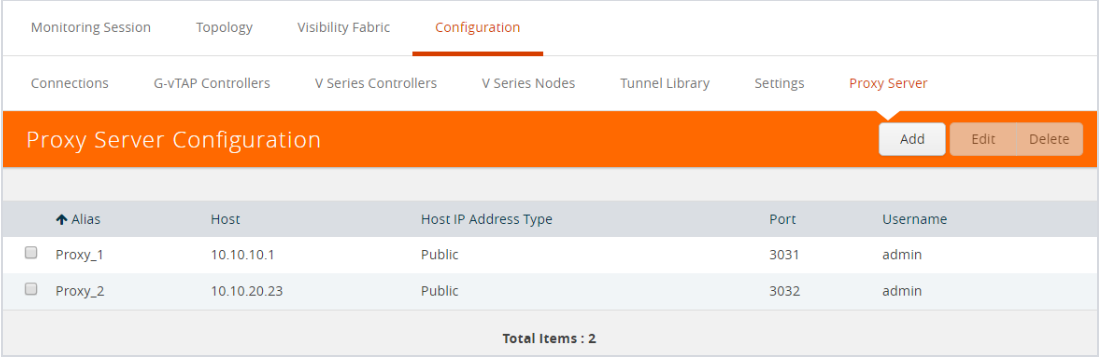
Table 11: Fields for Proxy Sever Configuration

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.

Field	Description
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.

1Click **Save**.

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



	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 56: Proxy Server Configuration Page

Events

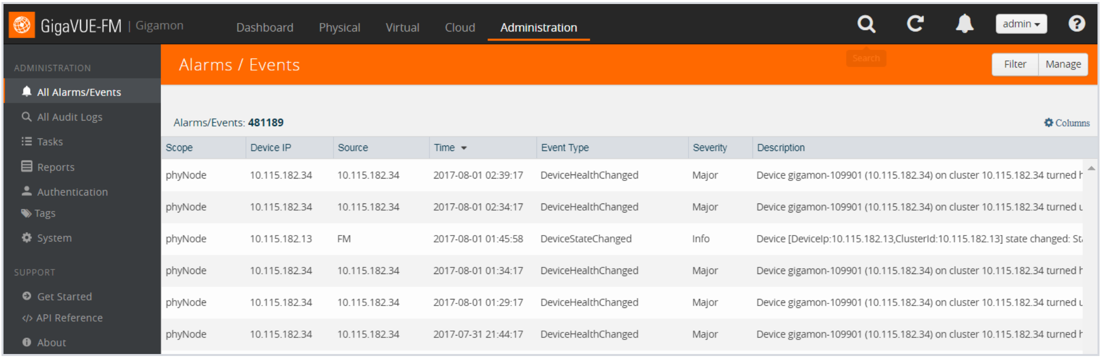
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- 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: **481189**

Scope	Device IP	Source	Time	Event Type	Severity	Description
phyNode	10.115.182.34	10.115.182.34	2017-08-01 02:39:17	DeviceHealthChanged	Major	Device gigamon-109901 (10.115.182.34) on cluster 10.115.182.34 turned h
phyNode	10.115.182.34	10.115.182.34	2017-08-01 02:34:17	DeviceHealthChanged	Major	Device gigamon-109901 (10.115.182.34) on cluster 10.115.182.34 turned u
phyNode	10.115.182.13	FM	2017-08-01 01:45:58	DeviceStateChanged	Info	Device [DeviceIp:10.115.182.13,ClusterId:10.115.182.13] state changed: St
phyNode	10.115.182.34	10.115.182.34	2017-08-01 01:34:17	DeviceHealthChanged	Major	Device gigamon-109901 (10.115.182.34) on cluster 10.115.182.34 turned h
phyNode	10.115.182.34	10.115.182.34	2017-08-01 01:29:17	DeviceHealthChanged	Major	Device gigamon-109901 (10.115.182.34) on cluster 10.115.182.34 turned u
phyNode	10.115.182.34	10.115.182.34	2017-07-31 21:44:17	DeviceHealthChanged	Major	Device gigamon-109901 (10.115.182.34) on cluster 10.115.182.34 turned h

Figure 57: Alarms

Table 12: Event Parameters describes the parameters recording for each event. You can also use filters to narrow down the results. Refer to Filter Events on page 88.

Table 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.

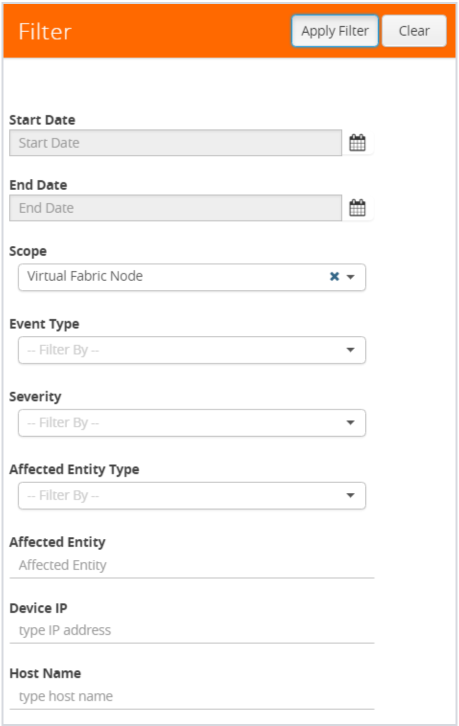
Controls/ Parameters	Description
Affected Entity Type	The resource type associated with the alarm or event.
Affected Entity	The resource ID of the affected entity type.
Description	The description of the event, which includes any of the possible notifications with additional identifying information where 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.



Start Date
Start Date

End Date
End Date

Scope
Virtual Fabric Node

Event Type
-- Filter By --

Severity
-- Filter By --

Affected Entity Type
-- Filter By --

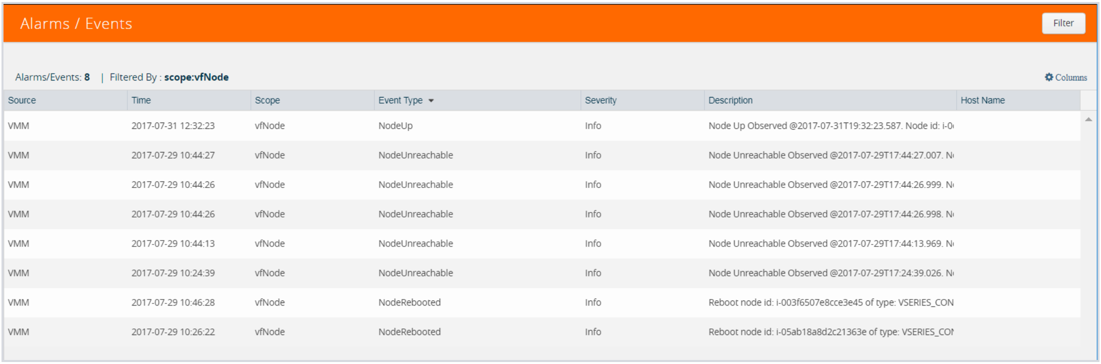
Affected Entity
Affected Entity

Device IP
type IP address

Host Name
type host name

Figure 58: Filtering Alarms/Events

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



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

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 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.

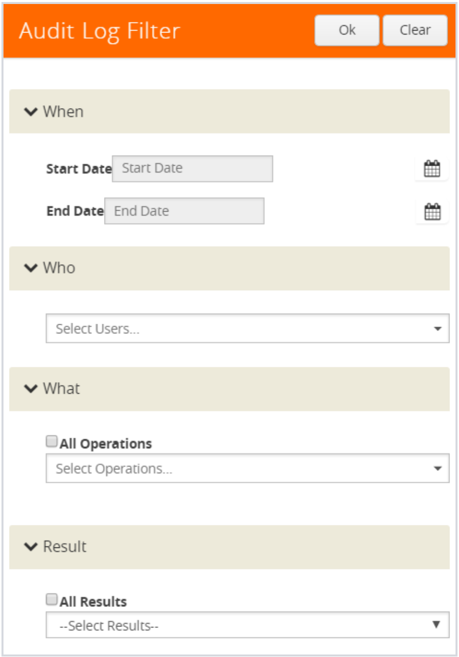


Figure 60: Audit Logs Filter

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.

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

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 on page 94
- Supported Features in GigaVUE V Series Nodes on page 94
- Supported Features in G-vTAP Agents on page 95

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
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

Additional Sources of Information

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

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

Documentation

The following table provides a list of the additional documentation provided for GigaVUE H Series and TA Series nodes. "*" indicates new documents in this release.

> **TIP**: If you keep all PDFs for a particular release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.

Table 1: Documentation Suite for Gigamon Products

Summary	Document
• complete doc set for the respective release, minus Release Notes, in a zip file	**All-Documents Zip**
• new features, resolved issues, and known issues in this release • important notes regarding installing and upgrading to this release **NOTE:** In 5.7.00, the Release Notes documents combines GigaVUE-OS, GigaVUE-FM, and GigaVUE Cloud Suite into one document.	**GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, and GigaVUE Cloud Suite Release Notes** **NOTE:** Registered Customers can download the Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download PDFs from My Gigamon.
Hardware Installation Guides	

Summary	Document
• how to unpack, assemble, rack-mount, connect, and initially configure the respective GigaVUE devices • reference information and specifications for the respective GigaVUE devices	**GigaVUE-HC1 Hardware Installation Guide**
	GigaVUE-HC2 Hardware Installation Guide
	GigaVUE-HC3 Hardware Installation Guide
	GigaVUE TA Series Hardware Installation Guide
Software Installation and Upgrade Guides	
• how to migrate GigaVUE-FM on VMware ESXi, Hardware Appliance, and AWS.	***GigaVUE-FM Migration Guide**
• how to install and upgrade GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM	**GigaVUE-FM Installation and Upgrade Guide**
• how to upgrade the embedded GigaVUE-OS on GigaVUE H Series and GigaVUE TA Series nodes	**GigaVUE-OS Upgrade Guide**
Administration Guide	
• how to administer the GigaVUE-OS and GigaVUE-FM software	**GigaVUE-OS and GigaVUE-FM Administration Guide**
Configuration and Monitoring Guides	
• how to install, deploy, and operate GigaVUE-FM • how to configure GigaSMART operations	**GigaVUE-FM User's Guide**
• how to deploy the GigaVUE Cloud Suite solution in any cloud platform	**GigaVUE Cloud Suite for AnyCloud Configuration Guide**
• how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the respective cloud platform	**GigaVUE Cloud Suite for AWS Configuration Guide**
	GigaVUE Cloud Suite for AWS QuickStart Guide
	***GigaVUE Cloud Suite for AWS Secret Regions Configuration Guide**
	GigaVUE Cloud Suite for Azure Configuration Guide
	GigaVUE Cloud Suite for Kubernetes Configuration Guide
	***GigaVUE Cloud Suite for Nutanix Configuration Guide**
	GigaVUE Cloud Suite for OpenStack Configuration Guide
	GigaVUE Cloud Suite for VMware Configuration Guide

Summary	Document
Reference Guides	
• library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices	**GigaVUE-OS CLI Reference Guide**
• guidelines for the different types of cables used to connect Gigamon devices	**GigaVUE-OS Cabling Quick Reference Guide**
• compatibility information and interoperability requirements for Gigamon devices	**GigaVUE-OS Compatibility and Interoperability Matrix**
• samples uses of the GigaVUE-FM Application Program Interfaces (APIs) **NOTE:** Content will be merged into the GigaVUE-FM User's Guide in a future release.	**GigaVUE-FM REST API Getting Started Guide**
In-Product Help	
• how to install, deploy, and operate GigaVUE-FM. Provided from the GigaVUE-FM interface.	**GigaVUE-FM Online Help**
• the web-based GUI for the GigaVUE-OS. Provided from the GigaVUE-OS H-VUE interface.	**GigaVUE-OS H-VUE Online Help**

NOTE: Registered customers can log in to My Gigamon to download documentation for specific releases under Software & Documentation Downloads. Refer to How to Download PDFs from My Gigamon.

How to Download PDFs from My Gigamon

To download release-specific PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Documentation** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.7," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.7.xx.

Documentation Feedback

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

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

Contact Technical Support

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

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

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

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

Register today at community.gigamon.com

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