GigaVUE Cloud Suite for AWS-GigaVUE V Series 2 Guide

GigaVUE Cloud Suite

Product Version: 6.2

Document Version: 1.0

Last Updated: Thursday, February 16, 2023

(See Change Notes for document updates.)

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

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.2.00	1.0	02/15/2022	The original release of this document with 6.2.00 GA

Contents

GigaVUE Cloud Suite for AWS-GigaVUE V Series 1

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.

Topics:

About GigaVUE Cloud Suite 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 Suite 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 for AWS instance is launched, the rest of the AMIs residing in the Community AMIs are automatically launched from GigaVUE-FM.

Refer to the following sections for details:

Components of GigaVUE Cloud Suite for AWS

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 Suite 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):
  - G-vTAP Controller (only if you are using G-vTAP Agent as the traffic acquisition method)
  - GigaVUE® V Series Controller
  - GigaVUE® V Series 1 node

  To launch the AMI in AWS, refer to AMI and Permissions and Prepare Virtual Machines to Monitor Traffic.
- **G-vTAP Agent** is an agent that is installed in your VM instance. This agent mirrors the selected traffic from the instances (virtual machines) to the GigaVUE Cloud Suite® 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.
- **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. A G-vTAP Controller can only manage G-vTAP Agents that has the same version. For example, the G-vTAP Controller v1.7 can only manage G-vTAP Agents v1.7. So, if you have G-vTAP Agents v1.6 still deployed in the EC2 instances, you must configure both G-vTAP Controller v1.6 and v1.7. 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.

  NOTE: A single G-vTAP Controller can manage up to 1000 G-vTAP Agents.
- **GigaVUE® V Series node** is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools. GigaVUE Cloud Suite for AWS uses the standard IP GRE or VXLAN tunnels to deliver traffic to tool endpoints. GigaVUE V Series nodes can be successfully launched only after GigaVUE V Series Controller is fully initialized and the status is displayed as OK. Refer Troubleshoot AWS Cloud Issues to troubleshoot theGigaVUE V Series issues.

  NOTE: With G-vTAP Agents, 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.
- **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 Controller to communicate with the GigaVUE V Series nodes.

Architecture of GigaVUE Cloud Suite for AWS

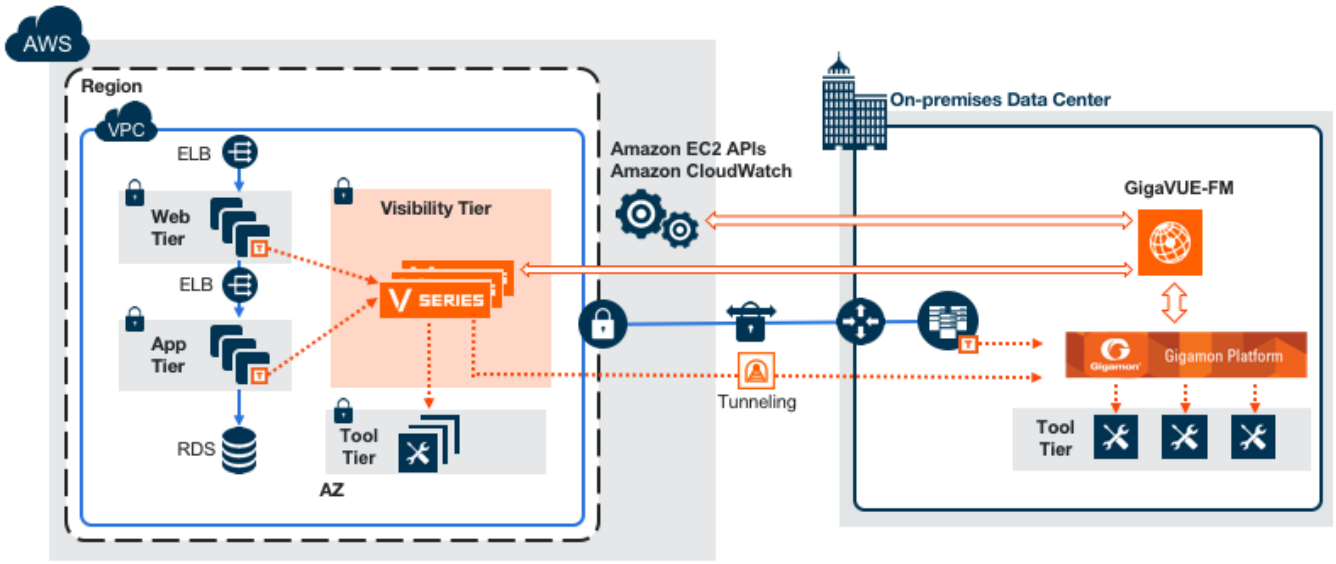
GigaVUE Cloud Suite for AWS supports the following cloud deployment models:

- Hybrid Cloud
- Multi-VPC Cloud

- Centralized Fabric Controllers and Node Configuration

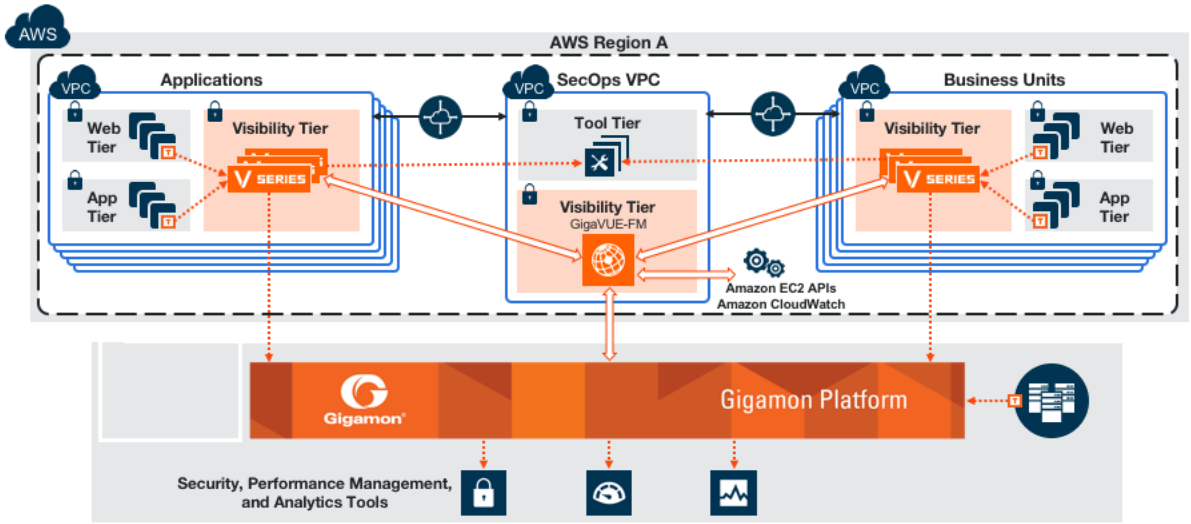
Hybrid Cloud

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.



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.



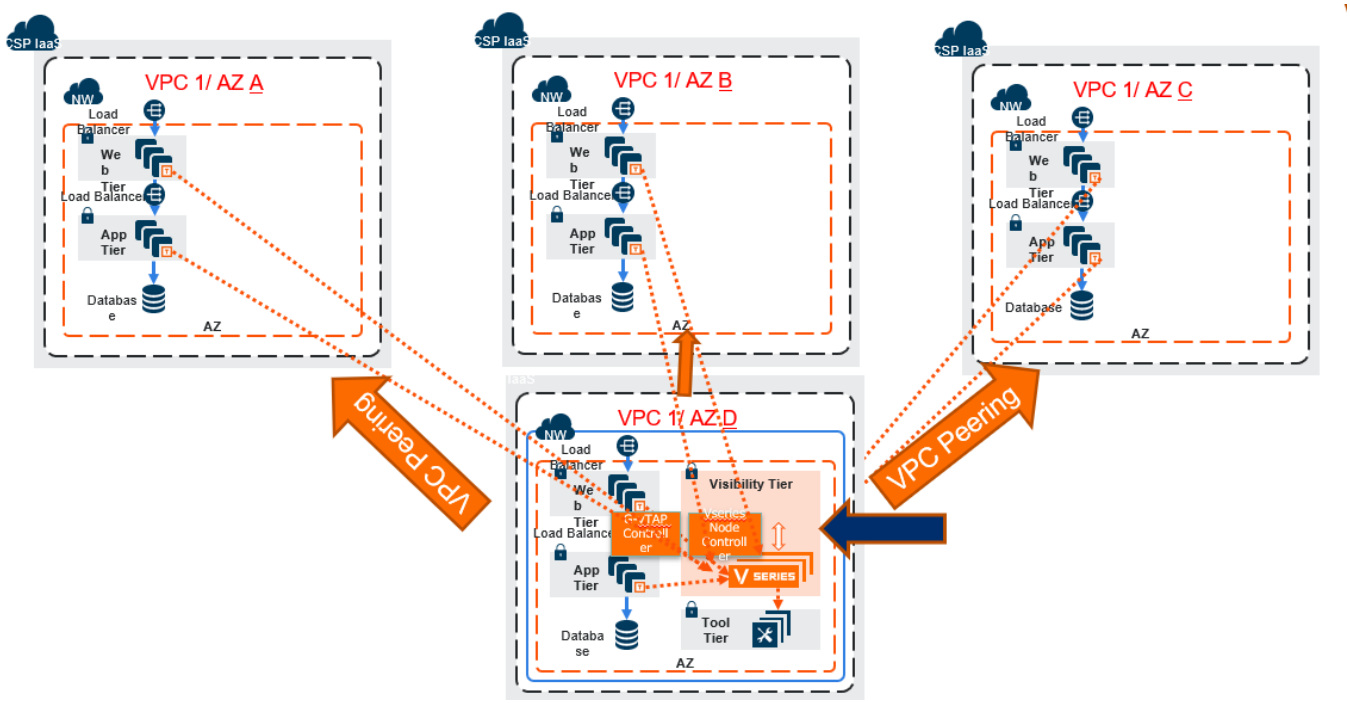
Centralized Fabric Controllers and Node Configuration

In the centralized fabric controllers and node configuration deployment model, the following GigaVUE cloud components are deployed in a 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 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.



Refer Gaining Pervasive Visibility in to the AWS Instances That may or may not Support VPC Mirroring for more detailed information.

Cloud Overview Page

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms,

Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

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

Virtual Dashboard Widgets

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

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

Overview

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

V Series Alarms

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

Connection Status

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

Usage

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

Summary

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

Get Started with GigaVUE Cloud Suite for AWS Deployment

This chapter describes how to plan and start the GigaVUE Cloud Suite for AWS in your AWS cloud.

Refer to the following sections for details:

- License Information
- Prerequisites
- AMI and Permissions
- Install and Upgrade GigaVUE-FM

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.

Refer to the following sections for details:

- Bring Your Own License (BYOL)
- Pay-As-You-Go (PAYG)
- Apply License

Bring Your Own License (BYOL)

BYOL is applicable only for V Series 1 node usage. The licenses 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 (NICs/vNICs)
- Traffic visibility for up to 1000 virtual TAP points (NICs/vNICs)

> **NOTE:** Make sure you purchase a licensing option that can provide traffic visibility to all the TAP points in the private network. If the licensing option cannot support all the TAP points, the NICs/vNICs are selected randomly for monitoring the traffic.

The minimum term for the license is 3 months.

A free trial is made available in your Cloud Provider Marketplace. 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 the TAP points the licensing option supports.

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

Pay-As-You-Go (PAYG)

PAYG is applicable only for V Series 1 node usage. 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.

Apply License

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

Prerequisites

Refer to the following topics for details:

- AWS Security Credentials
- Amazon VPC

AWS Security Credentials

When you first connect GigaVUE-FM with AWS, you need the security credentials for AWS to verify your identity and check if you have permission to access the resources that you are requesting. AWS uses the security credentials to authenticate and authorize your requests.

You need one of the following security credentials:

- **Identity and Access Management (IAM) role**–If GigaVUE-FM is running inside AWS, it is highly recommended to use an IAM role because it can securely make API requests from the instances. Create an IAM role and ensure that the permissions and policies listed in Permissions and Privileges are associated to the role.
- **Access Keys**–If GigaVUE-FM is configured in the enterprise data center, then you need to use the access keys or basic credentials to connect to the VPC. Basic credentials allow full access to all the resources in your AWS account.An access key consists of an access key ID and a secret access key. For detailed instructions on creating access keys, refer to the AWS documentation on Managing Access Keys for Your AWS Account.

  NOTE: To obtain the IAM role or access keys, contact your AWS administrator.

You cannot launch the GigaVUE-FM instance from the EC2 dashboard without having one of these security credentials. If you are launching the GigaVUE-FM instance from the AWS Marketplace, you need to have only the IAM roles.

IMPORTANT:

- Always run GigaVUE-FM inside AWS to manage your AWS workloads.
- Always attach an IAM role to the instance running GigaVUE-FM in AWS to connect it to your AWS account.
- Do NOT use access keys and secret keys to connect GigaVUE-FM to AWS. This requires GigaVUE-FM to store these keys and is NOT recommended.
- Well architected guidelines highly recommend the use of IAM roles.

NOTE: Running GigaVUE-FM outside of AWS requires the credentials to be stored internally. Although GigaVUE-FM encrypts access keys and secret access keys within its database, it is not recommended to connect to AWS from a GigaVUE-FM instance outside of AWS.

Amazon VPC

You must have a Amazon Virtual Private Cloud (VPC) to launch GigaVUE components into your virtual network.

NOTE: To create a VPC, refer to Create a VPC topic in the AWS Documentation.

Your VPC must have the following elements to configure the GigaVUE Cloud Suite for AWS components:

Subnet for VPC

To create a subnet for your VPC, refer to Create a subnet in your VPC topic in the AWS Documentation.

Internet Gateway

To create and attach an internet gateway to your VPC, refer to Create and attach an internet gateway topic in the AWS Documentation.

Route Table

To create a route table for your VPC, refer to Create a custom route table topic in the AWS Documentation.

Security Group

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

To create a security group, refer to Create a security group topic in the AWS Documentation.

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

Direction	Type	Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
GigaVUE-FM Inside AWS					
Inbound	HTTPS	TCP(6)	443	Anywhere Any IP	Allows G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP Agents
GigaVUE V Series Controller					

Direction	Type	Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
Inbound	Custom TCP Rule	TCP	9902	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Controllers
GigaVUE V Series 1 node					
Inbound	Custom TCP Rule	TCP	9903	Custom GigaVUE V Series Controller IP	Allows GigaVUE V Series Controllers to communicate with GigaVUE V Series nodes
VXLAN Traffic					
Inbound	Custom UDP Rule	VXLAN	4789		Allows mirrored traffic from G-vTAP Agents to be sent to GigaVUE V Series nodes using VXLAN tunnel Allows monitored traffic to be sent from GigaVUE V Series nodes to the tools using VXLAN tunnel

Key Pair

A key pair consists of a public key and a private key. You must create a key pair and specify the name of this key pair when you define the specifications for the G-vTAP Controllers, GigaVUE V Series nodes, and GigaVUE V Series Controllers in your VPC.

To create a key pair, refer to Create a key pair using Amazon EC2 topic in the AWS Documentation.

Connect GigaVUE-FM to AWS

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 topic in the AWS Whitepapers.

If you already have GigaVUE-FM running outside of your AWS environment, you can connect that existing GigaVUE-FM to your AWS using the Basic Credentials (Access Keys).

You can connect the GigaVUE-FM running inside of your AWS using the IAM role.

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

AMI and Permissions

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

NOTE: Refer Troubleshoot AWS Cloud Issues to resolve the GigaVUE-FM access issues.

GigaVUE Cloud Suite in AWS Public Cloud

The AMI for the GigaVUE Cloud Suite for AWS is available in the AWS Marketplace for the Bring Your Own License (BYOL) option.

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

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.

Permissions and Privileges

Before you begin configuring the components, you must enable the following permissions and attach the policies to an IAM role. You must then attach this IAM role to the GigaVUE-FM instance running in AWS:

- Full EC2 Instance access
- Read-only permission for IAM role
- EC2 pass role permission
- GigaVUE-FM Instance Role Policy
- KMS Permissions
- Amazon STS Support and Assume Role Policies Configuration

For creating an IAM role, refer to the AWS documentation on AWS identity and Access Management (IAM) service.

For more information on access control of EC2 instances in AWS, refer to the AWS documentation on Controlling Access to Amazon EC2 Resources.

NOTE: For VPC Traffic Mirroring, **"ec2:*TrafficMirror*"** is an additional set of permission required for the IAM role.

A few examples of the permissions and the policies that you must attach to an IAM role are listed below:

- Launch the GigaVUE-FM instance
- IAM Policy for Amazon CloudWatch integration
- IAM Policy for GvTap method
- IAM Policy for VPC mirroring with ELB
- Mirrored IAM Policy for deploying Gigamon Cloud Suite on AWS behind NLB to Gain Cross Account Visibility
- Target IAM policy for deploying Gigamon Cloud Suite on AWS behind NLB to gain Cross Account Visibility

Launch the GigaVUE-FM instance

The following IAM policy must be used for launching the GigaVUE-FM instance:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:Describe*",
"ec2:RebootInstances",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"ec2:ReportInstanceStatus",
"ec2:Disassociate*",
"ec2:AttachVolume",
"ec2:AttachNetworkInterface",
"ec2:Associate*",
"ec2:Allocate*",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DeleteNetworkInterface",
```

```
"ec2:ModifyInstanceAttribute",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyVolumeAttribute",
"ec2:ReleaseAddress",
"elasticloadbalancing:Describe*",
"autoscaling:Describe*"
],
"Resource": "*"
}
]
}
```

IAM Policy for Amazon CloudWatch integration

The following IAM policy must be used for Amazon CloudWatch integration :

```
---S3 Permissions
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:Get*",
"s3:ListAllMyBuckets",
"s3:PutBucketNotification",
"s3:PutBucketTagging",
"s3:PutBucketVersioning",
"s3:PutObject",
"s3:PutObjectTagging",
"s3:ReplicateDelete",
"s3:ReplicateObject",
"s3:RestoreObject",
"cloudwatch:*",
             "logs:*",

"sns:*",
"sqs:*", "events:*"
---IAM Permissions
```

IAM Policy for GvTap method

The following IAM policy must be used for GvTap method:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ec2:AttachVolume",
"ec2:RebootInstances",
"ec2:TerminateInstances",
"ec2:StartInstances",
"ec2:CreateTags",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:RunInstances",
```

```
"ec2:AttachNetworkInterface"
],
"Resource": [
"arn:aws:ec2:*:Insert your AWS Account Number:vpc/*",
"arn:aws:ec2:*:Insert your AWS Account Number:volume/*",
"arn:aws:ec2:*:Insert your AWS Account Number:subnet/*",
"arn:aws:ec2:*:Insert your AWS Account Number:key-pair/*",
"arn:aws:ec2:*:Insert your AWS Account Number:network-interface/*",
"arn:aws:ec2:*:Insert your AWS Account Number:instance/*",
"arn:aws:ec2:*:Insert your AWS Account Number:security-group/*",
"arn:aws:ec2:*::image/*"
]
},
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": [
"ec2:DescribeImages",
"ec2:DescribeAddresses",
"ec2:DescribeInstances",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups"
],
"Resource": "*"
},
{
"Sid": "VisualEditor2",
"Effect": "Allow",
"Action": "ec2:Associate*",
"Resource": [
"arn:aws:ec2:*:Insert your AWS Account Number:vpc/*",
"arn:aws:ec2:*:Insert your AWS Account Number:subnet/*",
"arn:aws:ec2:*:Insert your AWS Account Number:volume/*",
"arn:aws:ec2:*:Insert your AWS Account Number:key-pair/*",
"arn:aws:ec2:*:Insert your AWS Account Number:network-interface/*",
"arn:aws:ec2:*:Insert your AWS Account Number:instance/*",
"arn:aws:ec2:*:Insert your AWS Account Number:security-group/*",
"arn:aws:ec2:*::image/*"
]
}
]
}
```

IAM Policy for VPC mirroring with ELB

The following IAM policy must be used for VPC mirroring with ELB:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ec2:TerminateInstances",
```

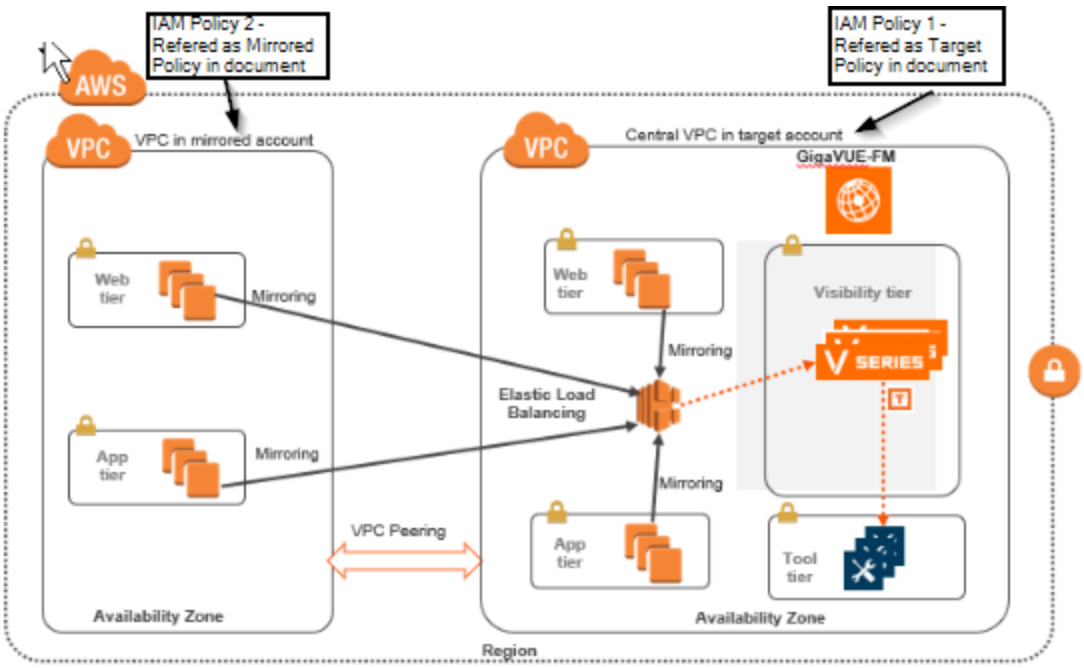
```
"ec2:RunInstances",
"ec2:CreateTags",
"ec2:DeleteTags",
"ec2:DeleteTrafficMirrorFilter",
"ec2:CreateTrafficMirrorFilter",
"ec2:CreateTrafficMirrorTarget",
"ec2:DeleteTrafficMirrorTarget",
"ec2:CreateTrafficMirrorFilterRule",
"ec2:DeleteTrafficMirrorFilterRule",
"ec2:DeleteTrafficMirrorSession",
"ec2:CreateTrafficMirrorSession",

],
"Resource": [
"arn:aws:ec2:*:Insert your AWS Account Number:vpc/*",
"arn:aws:ec2:*:Insert your AWS Account Number:volume/*",
"arn:aws:ec2:*:Insert your AWS Account Number:subnet/*",
"arn:aws:ec2:*:Insert your AWS Account Number:key-pair/*",
"arn:aws:ec2:*:Insert your AWS Account Number:network-interface/*",
"arn:aws:ec2:*:Insert your AWS Account Number:instance/*",
"arn:aws:ec2:*:Insert your AWS Account Number:security-group/*",
"arn:aws:ec2:*:Insert your AWS Account Number:traffic-mirror-target/*",
"arn:aws:ec2:*:Insert your AWS Account Number:traffic-mirror-filter/*",
"arn:aws:ec2:*:Insert your AWS Account Number:traffic-mirror-filter-rule/*",
"arn:aws:ec2:*:Insert your AWS Account Number:traffic-mirror-session/*",
"arn:aws:elasticloadbalancing:*:Insert your AWS Account Number:targetgroup/*",
"arn:aws:ec2:*::image/*"
]
},
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": [
"ec2:DescribeImages",
"ec2:DescribeAddresses",
"ec2:DescribeInstances",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorTargets"
],
"Resource": "*"
}

]
}
```

Mirrored and Target IAM Policy for deploying Gigamon Cloud Suite on AWS behind NLB to Gain Cross Account Visibility

In the architecture, the GigaVUE Cloud Suite fabric components in a centralized VPC where the target VMs from Web tier and App tier across multiple AWS accounts are deployed behind an external AWS network load balancer. GigaVUE FM creates VPC mirroring on the target VMs to mirror and forward the traffic to the load balancer.



Mirrored IAM Policy for deploying Gigamon Cloud Suite on AWS behind NLB to Gain Cross Account Visibility

The following mirrored IAM policy for deploying Gigamon Cloud Suite on AWS behind NLB to Gain Cross Account Visibility

```
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"ec2:CreateTags",
"ec2:DeleteTags",
"ec2:Describe*",
"ec2:*TrafficMirror*",
"ram:GetResourceShareInvitations"
```

```
],
"Resource": "*",
"Effect": "Allow"
}
]
}
```

Target IAM policy for deploying Gigamon Cloud Suite on AWS behind NLB to gain Cross Account Visibility

The following target IAM policy for deploying Gigamon Cloud Suite on AWS behind NLB to gain Cross Account Visibility :

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ec2:TerminateInstances",
"ec2:RunInstances",
"ec2:CreateTags",
"ec2:DeleteTrafficMirrorFilter",
"ec2:CreateTrafficMirrorFilter",
"ec2:CreateTrafficMirrorTarget",
"ec2:DeleteTrafficMirrorTarget",
"ec2:CreateTrafficMirrorFilterRule",
"ec2:DeleteTrafficMirrorFilterRule",
"ec2:DeleteTrafficMirrorSession",
"ec2:CreateTrafficMirrorSession",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:DeregisterTargets",
"ram:CreateResourceShare",
"ram:AssociateResourceShare",
"ram:DisassociateResourceShare",
"ram:DeleteResourceShare"
],
"Resource": [
"arn:aws:ec2:*:Insert your AWS Source Account Number:vpc/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:volume/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:subnet/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:key-pair/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:network-interface/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:instance/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:security-group/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:traffic-mirror-target/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:traffic-mirror-filter/*",
"arn:aws:ec2:*:Insert your AWS Source Account Number:traffic-mirror-filter-
rule/*",
```

```
"arn:aws:ec2:*:Insert your AWS Source Account Number:traffic-mirror-session/*",
"arn:aws:elasticloadbalancing:*:Insert your AWS Source Account
Number:targetgroup/*",
"arn:aws:ram:*:Insert your AWS Source Account Number:resource-share/*",
"arn:aws:ec2:*::image/*"
]
},
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": [
"ec2:DescribeImages",
"ec2:DescribeAddresses",
"ec2:DescribeInstances",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorTargets",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:DescribeTargetGroups",
"autoscaling:DescribeAutoScalingGroups",
"iam:ListPolicies",
"iam:GetPolicy",
"iam:GetPolicyVersion"
],
"Resource": "*"
},
{
"Sid": "VisualEditor2",
"Effect": "Allow",
"Action": "sts:AssumeRole",
"Resource": [
"arn:aws:iam::Insert your AWS Target Account Number:role/Insert your STS Assume
Role Created in the Target Account"
]
}
]
}
```

For detailed instruction on creating an IAM policy, refer to the AWS documentation on Creating Customer Managed Policies.

KMS Permissions

From 6.0 onwards, the following KMS permission policy is required:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
```

```
"Action": [
"kms:Decrypt",
"kms:GenerateDataKey",
"kms:DescribeKey"
],
"Resource": "arn:aws:kms:*:<Insert your AWS Account Number>:key/*"
},
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": "kms:ListAliases",
"Resource": "*"
}
]
}
```

Amazon STS Support and Assume Role Policies Configuration

GigaVUE-FM supports VPC connections in only one account. You can add additional accounts using *Access and Secret Keys*. From GigaVUE-FM version 5.7.01, GigaVUE-FM connections to AWS can use the Amazons STS (Secure Token Service) and Assume Role policies. Using these policies, you can attach a role to a GigaVUE-FM instance running in AWS, thus enabling GigaVUE-FM to monitor multiple accounts in AWS.

You can still use the *Access and Secret Keys* to create additional accounts. However, using the STS option is the recommended best practice for security reasons.

This section provides guidance on configuring your GigaVUE-FM instance to enable Amazon STS support.

Prerequisites

You must complete the following prerequisites before configuring GigaVUE-FM for Amazon STS support.

- A policy must be created in the account in which GigaVUE-FM is running.
  - Attach the created policy to a Role.
  - Attach the same Role to GigaVUE-FM, as an IAM instance Role.
- A policy must be included in other accounts as well.
  - These policies must allow GigaVUE-FM to assume the role in that account.

Procedure

For the purposes of these instructions, the AWS account that runs the GigaVUE-FM instance is called the source account, and any other AWS account that runs monitored instances is called a target account.

To configure GigaVUE-FM for Amazon STS support:

1. In each target account, create an IAM role with the source account number as a trusted entity and attach policies with permissions allowing GigaVUE-FM to perform its functions. Record the ARN of each role created.

   NOTE: This role must exist in all accounts to support the ability to create a single Monitoring Domain in GigaVUE-FM that includes multiple accounts.

2. In the source account, create a new IAM policy that allows GigaVUE-FM to retrieve IAM policies.

   IMPORTANT: The following example is provided as an illustration only.

```
{
   "Version": "2012-10-17",
   "Statement": {
     "Effect": "Allow",
     "Action": [
       "iam:ListPolicies",
       "iam:GetPolicy",
       "iam:GetPolicyVersion"
   ],
     "Resource": "*"
   }
}
```

3. In the source account, create a new IAM policy that allows the “sts:AssumeRole” action on all role ARNs created in Step 1.
   IMPORTANT: The following example is provided as an illustration only.

```
{
   "Version": "2012-10-17",
   "Statement": {
     "Effect": "Allow",
     "Action": "sts:AssumeRole",
     "Resource": [
       "arn:aws:iam::123456789012:role/FM-Role-target-account"
       ]
     }
}
```

   NOTE: In this example, 123456789012 is a target account and FM-Role-target-account is the role in the target account configured in step 1 with permissions required for GigaVUE-FM.

4. In the source account, attach the policies created in steps 2 and 3 to the IAM role that is attached to the GigaVUE-FM instance.

Install and Upgrade GigaVUE-FM

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

- Cloud–To install GigaVUE-FM inside your AWS environment, you can deploy GigaVUE-FM using the AWS CloudFormation Templates (CFT) found in the AWS Marketplace or manually deploy the latest GigaVUE-FM instance using the public images (AMI) through the AWS EC2.
  For the GigaVUE-FM installation procedures, refer to Install GigaVUE-FM on AWS.
- On-premises–To install and upgrade GigaVUE-FM in your enterprise data center, refer to *GigaVUE-FM Installation and Upgrade Guide* available in the Gigamon Documentation Library.

For GigaVUE-FM upgrade issues, refer to Troubleshoot AWS Cloud Issues.

Deploy GigaVUE Cloud Suite for AWS

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

If you already have GigaVUE-FM running outside of your AWS environment, you can connect that existing GigaVUE-FM to your AWS using the Basic Credentials (Access Keys).

Refer to the following sections for details:

- Prepare G-vTAP Agent to Monitor Traffic
- Create a Monitoring Domain
- Configure GigaVUE Fabric Components

Prepare G-vTAP Agent to Monitor Traffic

A G-vTAP Agent is the primary Gigamon monitoring module that is installed in your Virtual Machines (VMs). G-vTAP mirrors the selected traffic from a source interface to a destination mirror interface. The mirrored traffic is encapsulated using GRE or VXLAN tunneling and then sent to the GigaVUE Cloud Suite® V Series node.

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

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 L2GRE/VXLAN tunnel interface or IPSec tunnel interface to the GigaVUE V Series node.

NOTE: If the secure tunnel option is selected, then IPSec is used to establish secure tunnel between G-vTAP Agent and GigaVUE V Series nodes.

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.

Refer to the following sections for more information:

- Linux G-vTAP Agent Installation
- Windows G-vTAP Agent Installation
- Install IPSec on G-vTAP Agent
- Create Images with Agent Installed

Refer Troubleshoot AWS Cloud Issues to resolve G-vTAP deployment issues.

Linux G-vTAP Agent Installation

Refer to the following sections for the Linux agent installation:

- Single ENI Configuration
- Dual ENI Configuration
- Install G-vTAP Agents

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 NIC/ENI will initialize at boot time.

> **NOTE:** Before installing G-vTAP Agent **.deb** or **.rpm** packages on your Linux VMs, you must install packages like Python3 and Python modules (netifaces, urllib3, and requests). Package iproute-tc is also required on RHEL and CentOS VMs.

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

Refer to the following topics for details:

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

Install G-vTAP from Ubuntu/Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent `6.2.00` Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gvtap-agent_6.2.00_amd64.deb
$ sudo dpkg -i gvtap-agent_6.2.00_amd64.deb
```

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

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

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

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

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

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

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

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

4. Save the file.

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

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

6. Reboot the instance.

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

```
$ sudo /etc/init.d/gvtap-agent status
G-vTAP Agent is running
```

Install G-vTAP from RPM package

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

1. Download the G-vTAP Agent **6.2.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gvtap-agent_6.2.00_x86_64.rpm
$ sudo rpm -i gvtap-agent_6.2.00_x86_64.rpm
```

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

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

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

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

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

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

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

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

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

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

6. Reboot the instance.

Check the status with the following command:

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

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

1. Launch the RHEL/CentOS agent AMI image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**6.2.00**_x86_64.rpm
   - gvtap.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
5. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_6.2.00_x86_64.rpm
   ```
6. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

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

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent `6.2.00` MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator** and the G-vTAP Agent service starts automatically.
3. Once the G-vTAP package is installed, modify the file **C:\ProgramData\Gvtap-agent\gvtap-agent.conf** to configure and register the source and destination interfaces.

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

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

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

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

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

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

4. Save the file.

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

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

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

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

Windows G-vTAP Agent Installation Using ZIP Package

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

1. Download the Windows G-vTAP Agent **6.2.00** ZIP package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Extract the contents of the .zip file into a convenient location.
3. Run 'install.bat' as an **Administrator** and the G-vTAP Agent service starts automatically.

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

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

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

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

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

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

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

5. Save the file.

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

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

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

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

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

Install IPSec on G-vTAP Agent

If IPSec is used to establish secure connection between G-vTAP Agents andGigaVUE V Seriesnodes, 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

NOTE: IPSec cannot be installed on G-vTAP Agents that are running on Windows OS. Therefore, if a monitoring session has targets with both Windows and Linux OS, only the Linux agents will communicate over the secure connection. Windows agent will communicate only through the VXLAN Tunnel.

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

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

Install G-vTAP from Ubuntu/Debian Package

1. Launch the Ubuntu/Debian image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_6.2.00_amd64.deb
   - gvtap-ipsec_6.2.00_amd64.deb
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.
4. Install the G-vTAP Agent package file:
   ```
   sudo dpkg -i gvtap-agent_6.2.00_amd64.deb
   ```
5. Modify the **/etc/gvtap-agent/gvtap-agent.conf** file to configure and register the source and destination interfaces:

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

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

   NOTE: You can view the G-vTAP log using `cat /var/log/gvtap-agent.log` command.
6. 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
   ```
7. Install IPSec package:
   ```
   sudo dpkg -i gvtap-ipsec_6.2.00_amd64.deb
   ```

Install G-vTAP from Red Hat Enterprise Linux and CentOS

1. Launch RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_6.2.00_x86_64.rpm
   - gvtap-ipsec_6.2.00_x86_64.rpm
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.
4. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_6.2.00_x86_64.rpm
   ```

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

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

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

6. 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
   ```
7. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_6.2.00_x86_64.rpm
   ```

NOTE: You must install IPSec package after installing StrongSwan.

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

1. Launch the RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_6.2.00_x86_64.rpm
   - gvtap-ipsec_6.2.00_x86_64.rpm
   - gvtap.te and gvtap_ipsec.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
5. 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
   ```
6. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_6.2.00_x86_64.rpm
   ```

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

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

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

8. 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
   ```
9. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_6.2.00_x86_64.rpm
   ```
10. Reboot the instance.

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.

To save the G-vTAP Agent as an AMI from your EC2 console, right click on the instance and navigate to **Image** > **Create Image**.

Create a Monitoring Domain

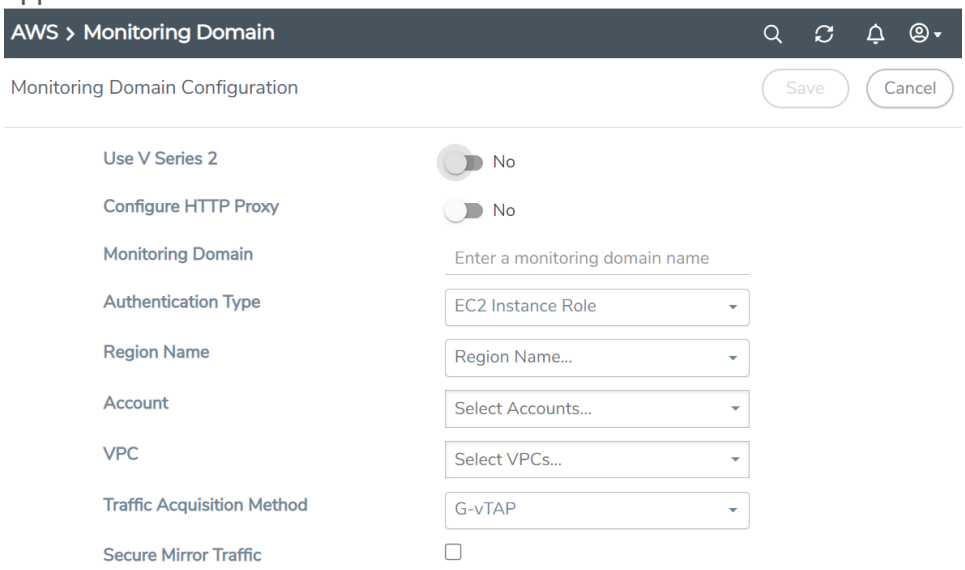
GigaVUE-FM connects to the VPC through the EC2 API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the EC2 API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

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.

NOTE: To configure the monitoring domain and launch the fabric components in AWS, you must be a user with **fm_super_admin** role or a user with write access to the **Physical Device Infrastructure Management** category.

To create a Monitoring Domain:

1. From the left navigation pane, click **Inventory > AWS**, and then click **Monitoring Domain**.
2. On the Monitoring Domain page, click the **New** button. The Monitoring Domain Configuration page appears.



3. Enter or select the appropriate information as shown in the following table.

Field	Description
Use V Series 2	Select **No** to configure V Series 1 node.
Configure HTTP Proxy	Select **Yes** to add a proxy server. Proxy server enables communication from GigaVUE-FM to the Internet, if GigaVUE-FM is deployed in a private network. On selecting a Proxy Server, enter the following information: • **Proxy Server**–Select a 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 • **Add Proxy Server**–Add a new Proxy Server. For field information, refer to Configure Proxy Server.
Monitoring Domain	An alias used to identify the monitoring domain.
Authentication Type	Authentication type for the connection. You can select one of the following: ■ **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	Select the VPCs to monitor
Traffic Acquisition Method	Select a Tapping method. The available options are: • **G-vTAP**: G-vTAP Agents are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to communicate to the G-vTAP Agents from GigaVUE-FM. • **VPC Traffic Mirroring**: If you select the VPC Traffic Mirroring option, the mirrored traffic from the VPC connections is monitored directly using the GigaVUE V Series nodes, and you need not configure the G-vTAP Agents and G-vTAP Controllers. For more information on VPC Peering, refer to VPC peering connections in the AWS Documentation. • G-vTAP Controller configuration is not applicable for VPC Traffic Mirroring. • For VPC Traffic Mirrorning option, additional permissions are required. Refer to the Permissions and Privileges for details. • After deploying the Monitoring Session in GigaVUE-FM, a traffic mirror session is created in your AWS VPC. For more details, refer to Traffic Mirroring in AWS Documentation.
Secure Mirror Traffic	Check box to establish secure tunnel between G-vTAP Agents and GigaVUE V Series nodes for traffic across VPCs.

4. Click **Save**. The **AWS Fabric Launch Configuration** page appears.

Configure GigaVUE Fabric Components

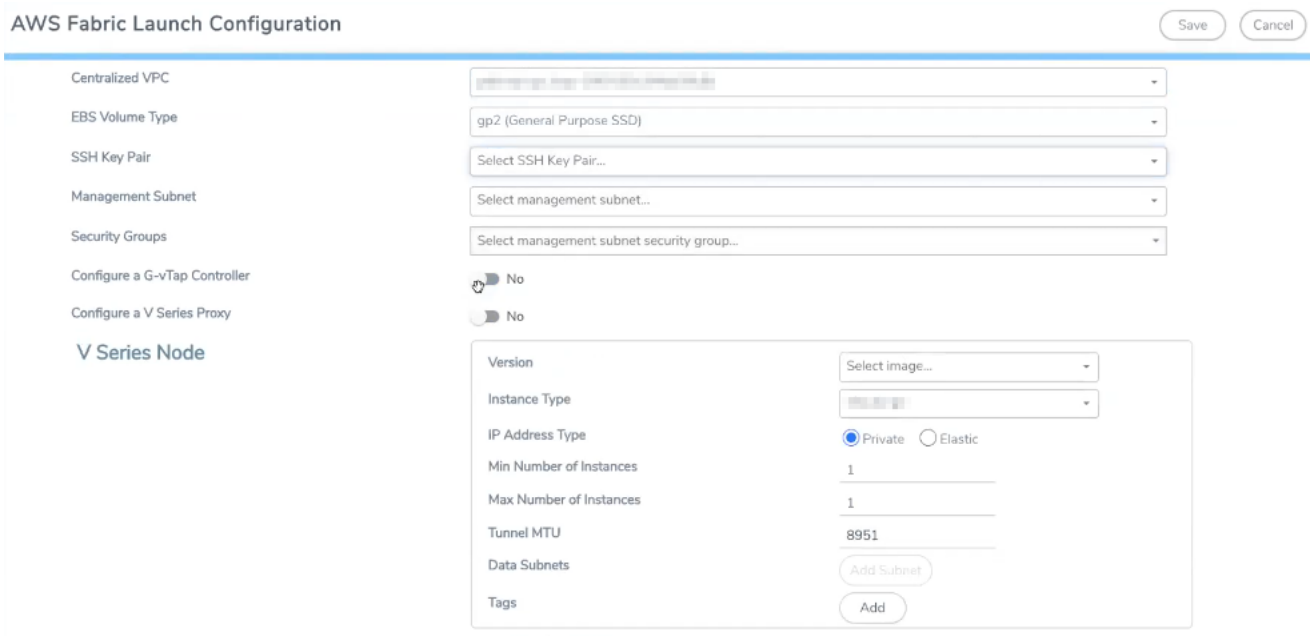
After configuring the Monitoring Domain, you will be navigated to the AWS Fabric Launch Configuration page.

In the same **AWS Fabric Launch Configuration** page, you can configure the following fabric components:

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

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

Fields	Description
Centralized VPC	Alias of the centralized VPC in which the G-vTAP Controllers, V Series Proxies 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 GigaVUE fabric nodes. For more information on Key Pairs, refer to Key Pair.
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 GigaVUE fabric nodes. For more information on security groups, refer to Security Group

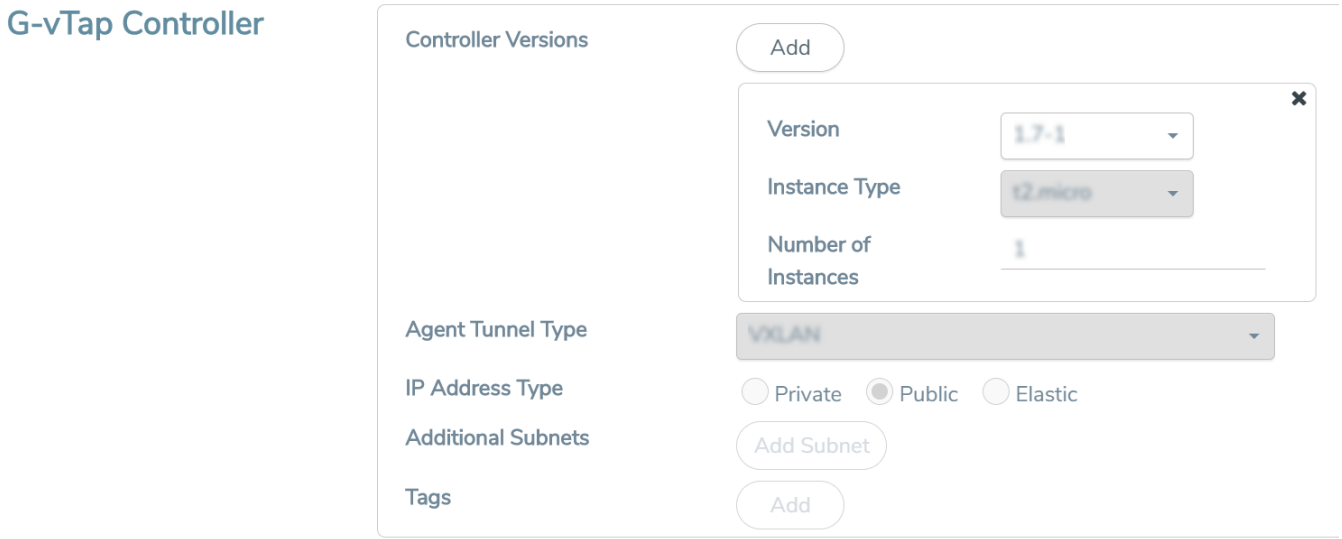


Configure G-vTAP Controller

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

NOTE: A G-vTAP Controller can only manage G-vTAP Agents of the same version.

Select **Yes** for the Configure a G-vTAP Controller field.



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

Fields	Description
Controller Version	The G-vTAP Controller version. 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. Click **Add** to add multiple versions of G-vTAP Controllers: Under **Controller Versions**, click **Add**. a. From the **Version** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP Agents installed in the instances. b. From the **Instance Type** drop-down list, select a size for the G-vTAP Controller. c. In **Number of Instances**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.
Instance Type	The instance type for the G-vTAP controller. The recommended instance type is t2.micro.
Number of Instances	The number of G-vTAP Controllers to deploy in the monitoring domain.
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.
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.
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.

Configure GigaVUE V Series Controller

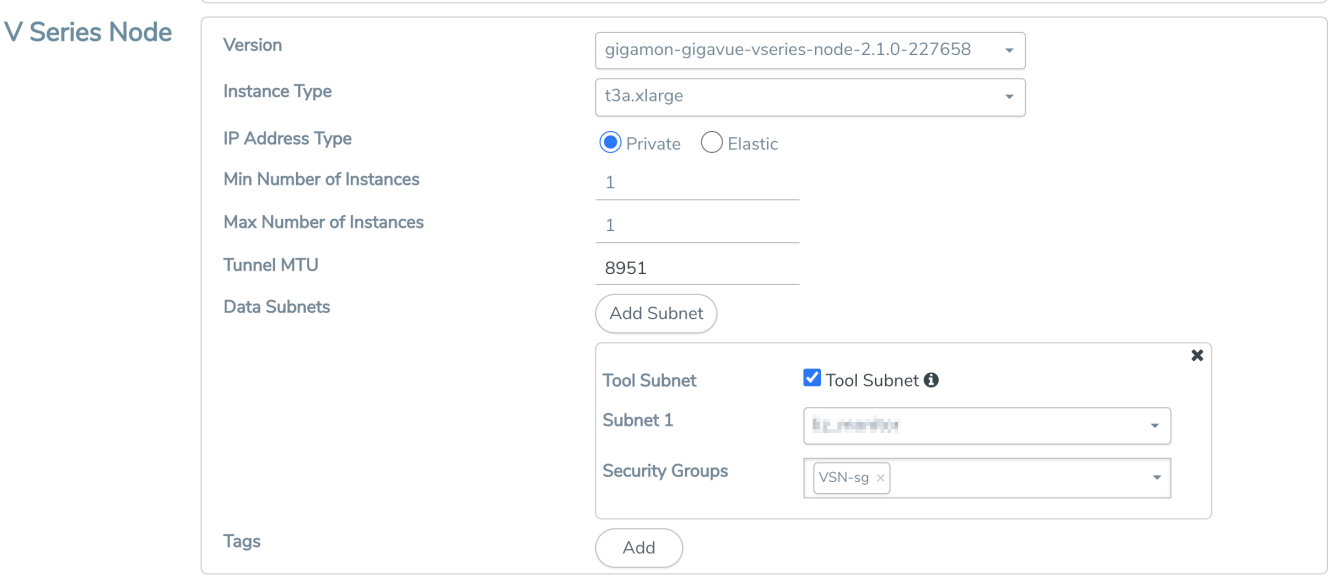
Select **Yes** for the Configure a V Series Controller field.
Enter or select the appropriate information as described in the following table for GigaVUE V Series Controller Configuration.

Fields	Description
Version	GigaVUE V Series Controller version.
Instance Type	Instance type for the GigaVUE V Series Controller. The recommended minimum instance type is t2.micro.

Fields	Description
Number of Instances	Number of GigaVUE V Series Controller to deploy in the monitoring domain.
Set Management Subnet	Use the toggle button to select a management subnet. • **Yes** to use the management subnet that you selected previously. • **No** to use another management subnet.
Set Security Groups	Toggle option to **Yes** to set the security group that is created for the GigaVUE V Series Controller. Refer to Security Group for more details.
IP Address Type	Select one of the following IP address types: ■ 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.

Configure GigaVUE V Series Node

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



Enter or select appropriate information as described in the following table for GigaVUE V Series Node Configuration.

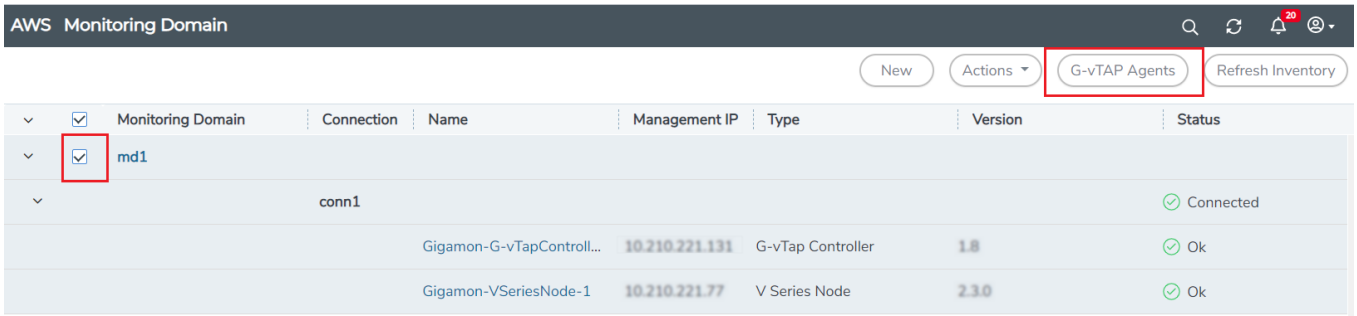
Fields	Description
Version	GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. The default instance type is nitro-based t3a.xlarge. The recommended instance type is c5n.xlarge for 4vcpu and c5n.2xlarge for 8vcpu.
Min Number of Instances	The minimum number of GigaVUE V Series Nodes that must be deployed in the monitoring domain. The minimum number of instances must be 1. When 0 is entered, no GigaVUE V Series Node is launched. **NOTE:** If the minimum number of instances is set as '0', then the nodes will be launched when a monitoring session is deployed if GigaVUE-FM discovers some targets to monitor.

Fields	Description
Max Number of Instances	The maximum number of GigaVUE V Series Nodes that can be deployed in the monitoring domain.
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 theGigaVUE V Series 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.

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

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

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



Configure Monitoring Session

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. 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 Cloud Suite H Series node.

Refer to the following sections for details:

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

Create a Monitoring Session

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

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

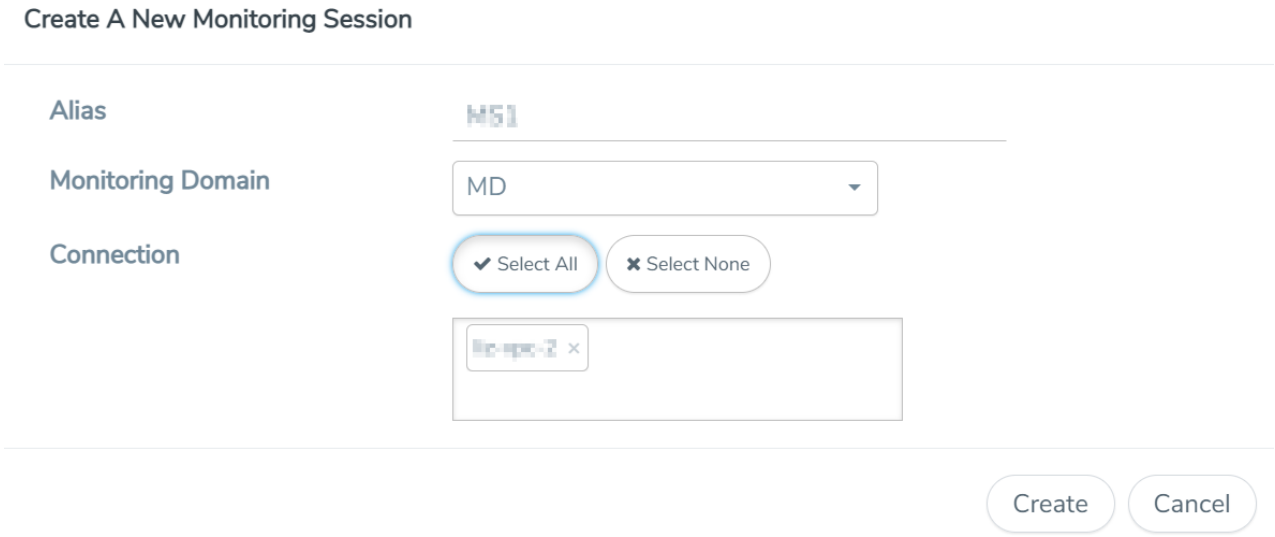
For the connections without G-vTAPs there is no targets that are automatically selected. You can use Customer Orchestrated Source in the monitoring session to accept a tunnel from anywhere.

You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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



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

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

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

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

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

Applying Prefiltering policy template to Monitoring Session

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

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page.

3. Create a new monitoring session. To create a new monitoring session, refer to Create a Monitoring Session.
4. In the Edit Monitoring Session page, expand **Prefiltering**.
5. Select the required Prefiltering template from the **Template** drop-down list. The rules and filters configured in the template appear. You can also change the values as per the requirement. By default, the changes are not saved in the template. You can save the changes as a new template by clicking **Save as Template**.
6. Click **Next**. The topology view appears.

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

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

Creating Prefiltering policy template

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

To create a prefiltering policy template do the following steps:

1. Go to **Resources** > **Prefiltering**, and then click **G-vTAP**.

2. Click **New**.

3. Enter the name of the template in the **Template Name** field.

4. Enter the name of a rule in the **Rule Name** field.

5. Click any one of the following options:

- Pass – Passes the traffic.
- Drop – Drops the traffic.

6. Click any one of the following options as per the requirement:

- Bi-Directional –- Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
- Ingress – Filters the traffic that flows in.
- Egress – Filters the traffic that flows out.

7. Enter the value of the priority based on which the rules must be prioritized for filtering. Select the value as 1 to pass or drop a rule in top priority. Similarly, you can select the value as 2, 3, 4 to 8 where 8 can be used for setting a rule with least priority. Drop rules are added based on the priority and then pass rules are added.

8. Select the **Filter Type** from anyone of the following options:

- L3
- L4

9. Select the **Filter Name** from any one of the following options:

- ip4Src
- ip4Dst
- ip6Src
- ip6Dst
- Proto - It is common for both ipv4, ipv6.

10. Select the **Filter Relation** from any one of the following options:

- Not Equal to
- Equal to

11. Enter the value for the given filter.

12. Click **Save**.

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

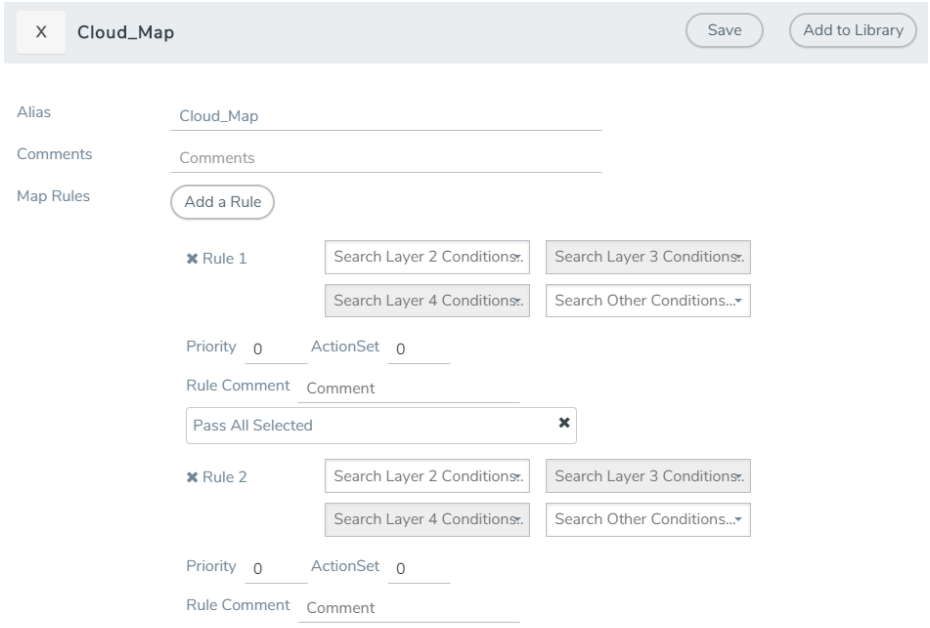
Create Map

Each map can have up to 32 rules associated with it. The following table lists the various conditions that you can select for creating a map, inclusion map, and exclusion map.

Conditions	Description
L2, L3, and L4 Filters	
EtherType	The packets are filtered based on the selected ethertype. The following conditions are displayed: ■ 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 EtherType, TCP as the protocol, and do not specify IP source or destination, then both egress and ingress traffic is selected for monitoring purpose.

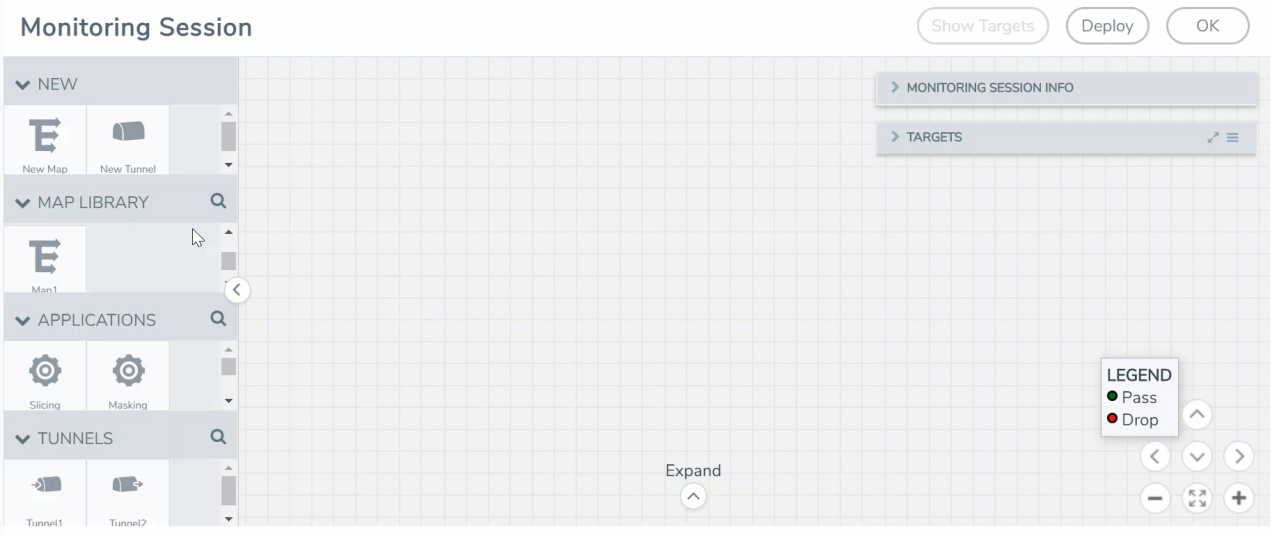
When you select a condition with either source or destination specified, it determines the direction based on the selection. For example, if only IP source is selected as shown in the following figure, the egress traffic from the instances in the subnet 10.0.1.0/24 is selected for monitoring the traffic.



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

To create a new map:

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



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

Parameter	Description
Alias	The name of the new map. NOTE: The name can contain alphanumeric characters with no spaces.
Description	The description of the map.
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. c. Select a condition from the **Search L3 Conditions** drop-down list and specify a value. 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. 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. • Repeat steps **b** through **f** to add more conditions. • Repeat steps **a** through **f** to add nested rules

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

4. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
   - Select an existing group from the **Select Group** list 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.
5. Click **OK**.

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

Agent Pre-filtering

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

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

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

Agent Pre-filtering Guidelines

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

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

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

Agent Pre-filtering Rules and Notes

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

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

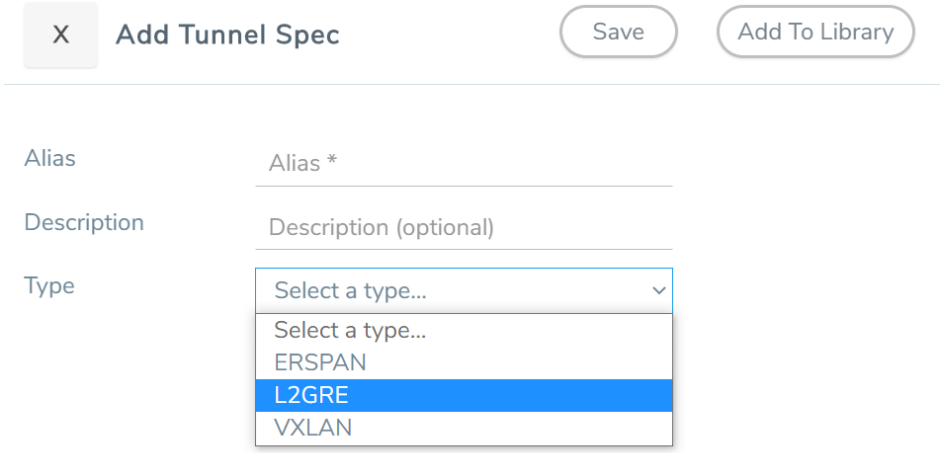
Create Tunnel Endpoints

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.

NOTE: To configure the tunnel end points, you must be a user with **fm_super_admin** role or a user with write access to the **Traffic Control Management** category.

To create a new tunnel:

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



3. In the Add Tunnel Spec quick view, select or enter the appropriate information as described in the following table.

Field	Description
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Type	The type of the tunnel. Select 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 for V Series 1 nodes.
Remote Tunnel IP	The IP address of the tunnel destination endpoint.

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

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

Add Applications to Monitoring Session

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

- Sampling
- Slicing

- Masking
- NetFlow

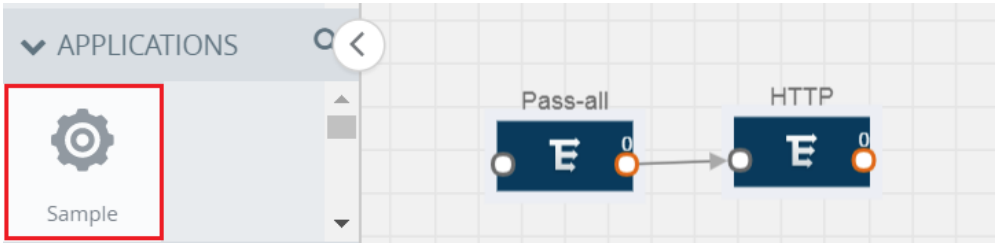
You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools.

Sampling

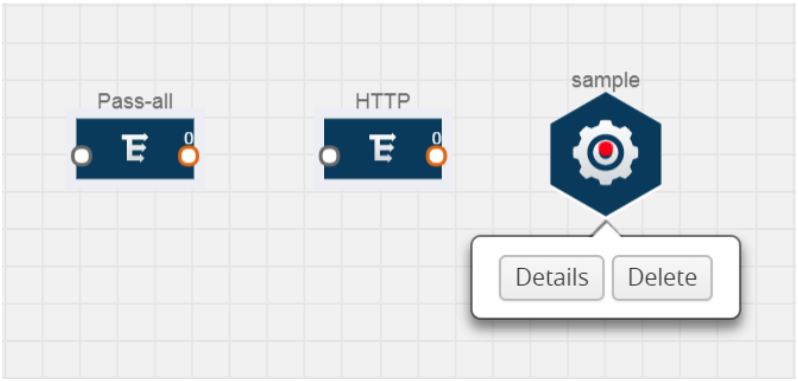
Sampling lets you sample the packets randomly based on the configured sampling rate and then forwards the sampled packets to the monitoring tools.

To add a sampling application:

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



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



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

- **Random Systematic** –The first packet is selected randomly. Then, every nth packet is selected, where n is the value specified in the **Sampling Rate** field.For example, if the first packet selected is 5 and the sampling rate is 1:10, then every 10th packet is selected for sampling: 15, 25, 35, and so on.

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

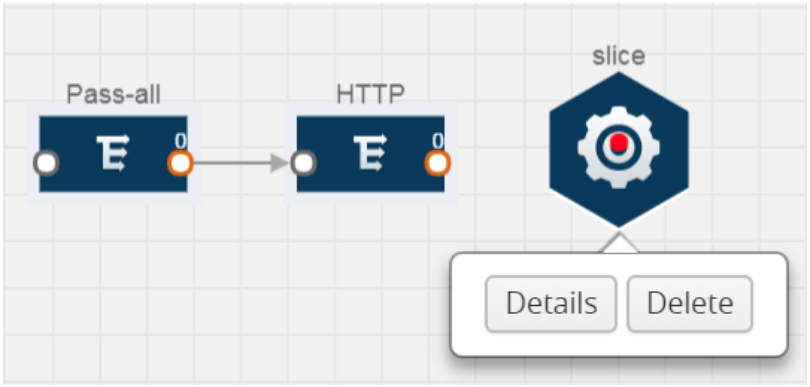
Slicing

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

To add a slicing application:

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

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



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

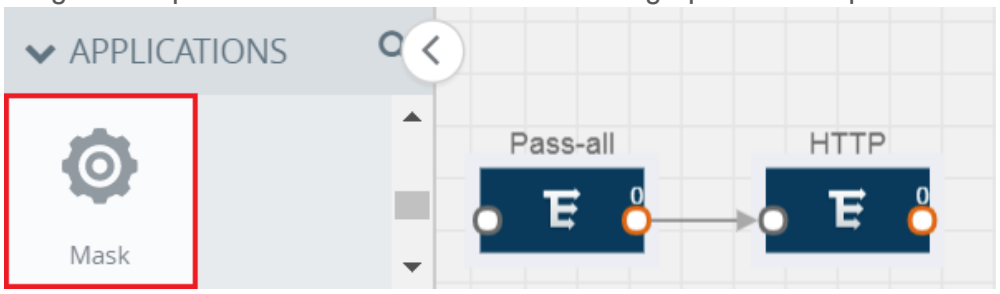
6. From the Protocol drop-down list, specify an optional parameter for slicing the specified length of the protocol. The options are as follows:
   - None
   - IPv4
   - IPv6
   - UDP
   - TCP
7. Click **Save**.

Masking

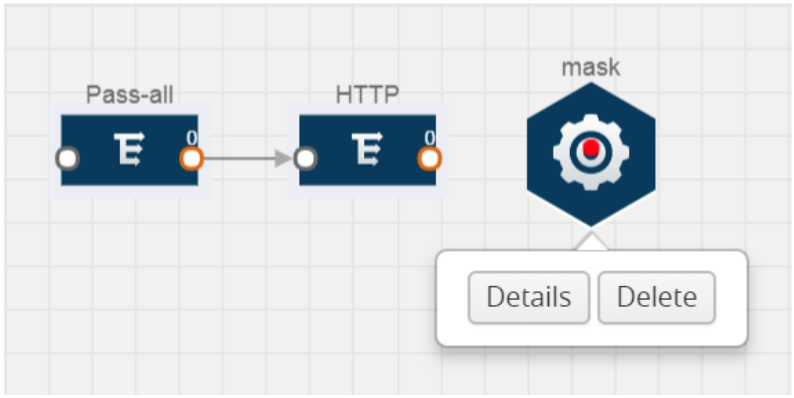
Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.

To add a masking application:

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



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



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

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

NetFlow

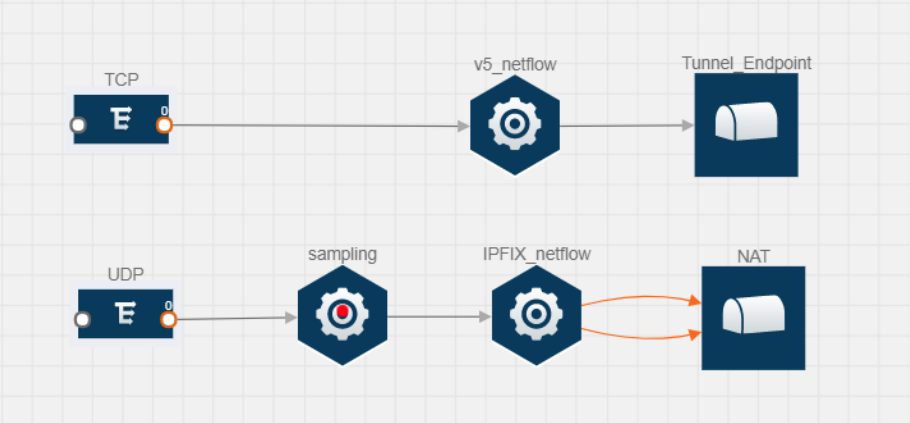
NetFlow collects IP network traffic on all interfaces where NetFlow monitoring is enabled. It gathers information about the traffic flows and exports the NetFlow records, which includes data and templates, to at least one NetFlow collector. The application that serves as a NetFlow collector receives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

The following are the key benefits of NetFlow application:

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

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

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



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

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

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

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

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

Match/Key Fields

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

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

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

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

Collect/Non-Key Fields

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

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

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

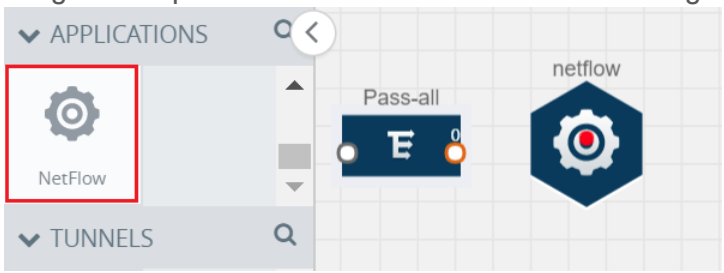
	Description	Supported NetFlow Versions
IPv4 ICMP Type	Configures the type of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a non-key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as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

	Description	Supported NetFlow Versions
	key field.	
UDP Dest Port	Configures the destination port identifier in the UDP header as a non-key field.	IPFIX
UDP Src Port	Configures the source port identifier in the UDP header as a non-key field.	IPFIX

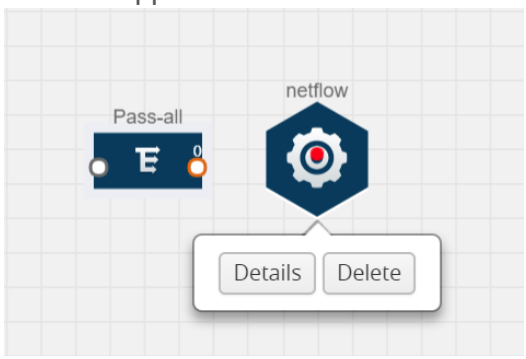
Add Version 5 NetFlow Application

To add a version 5 NetFlow application:

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



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



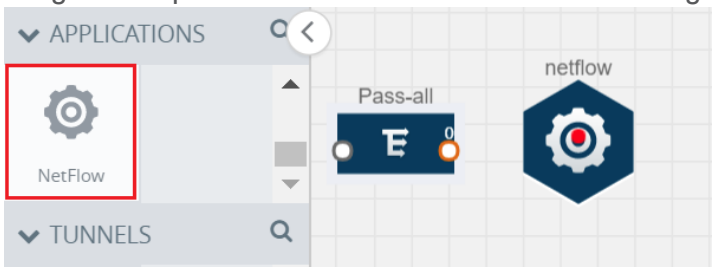
3. In the **Alias** field, enter a name for the v5 NetFlow application.
4. For State, select the **On** check box to determine that the application is currently running. Select the **Off** check box to determine that the application is currently not running. The state can be changed at anytime whenever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

For more examples demonstrating the NetFlow application configuration in the GigaVUE V Series nodes, refer to NetFlow Examples.

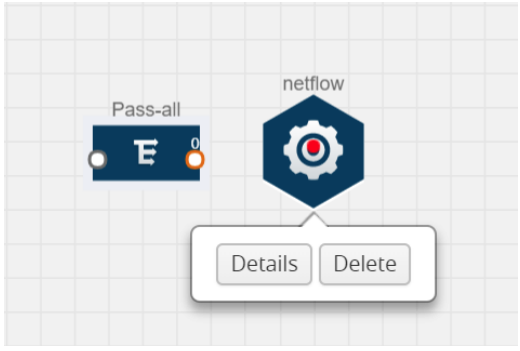
Add Version 9 and IPFIX NetFlow Application

To add a v9 and IPFIX NetFlow application:

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



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



3. In the **Alias** field, enter a name for the NetFlow application.
4. For State, select the **On** check box to determine that the application is generating NetFlow records from the packets coming from the G-vTAP Agents. Select the **Off** check box to determine that the application is not currently generating NetFlow records. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select the version you want to use to generate the NetFlow records. The default version selected is v5.
6. In the **Source ID** field, enter the observation domain to isolate the traffic. The NetFlow application uses source ID to segregate the records into categories. For example, you can assign source ID 1 for traffic coming over TCP. This results in generating a separate NetFlow record for TCP data. Similarly, you can assign Source ID 2 for traffic coming over UDP. This results in generating a separate NetFlow record for UDP data.
7. From the **Match fields** drop-down list, select the parameters that identify what you want to collect from the incoming packets. The Match fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to Match/Key Fields.
8. From the **Collect fields** drop-down list, select the parameters that identify what you want to collect from the NetFlow records. The Collect fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to Collect/Non-Key Fields.

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

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

Network Address Translation (NAT)

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

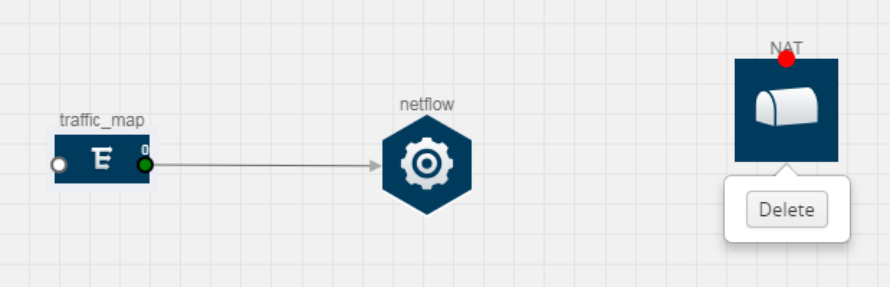
The NetFlow records are exported to the collector over UDP protocol with the configurable source IP and destination IP.

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

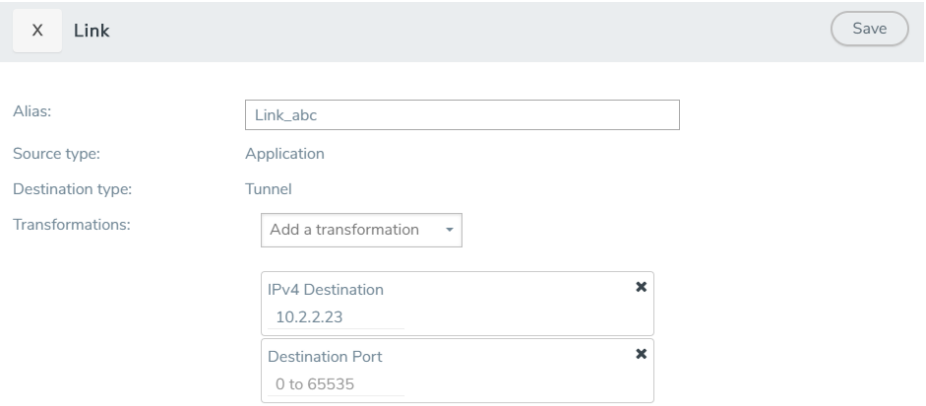
Add NAT and Link NetFlow Application to NAT

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

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



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



3. Creating a Link from NetFlow to NAT
4. In the **Alias** field, enter a name for the link.
5. From the **Transformations** drop-down list, select any one of the header transformations:
   - IPv4 Destination
   - ToS
   - Destination Port

   NOTE: Only the above three header transformations are allowed on the link from the NetFlow application to a NAT device.
6. In **IPv4 Destination**, enter the IP address of the NetFlow collector.
7. (Optional) By default, the Destination Port is 2055. To change the destination port, enter a port number.
8. Click **Save**. The transformed link is displayed in Orange.
9. Repeat steps 7 to 10 to send additional NetFlow records to NAT.

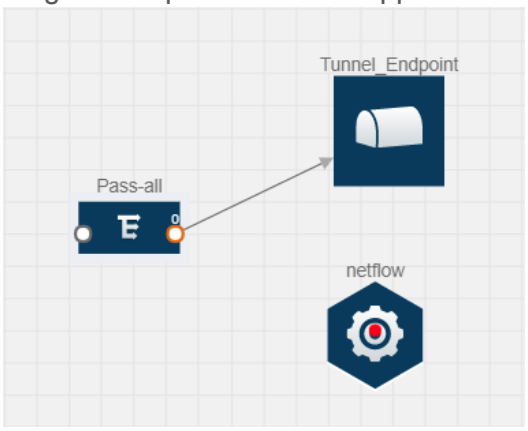
NetFlow Examples

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

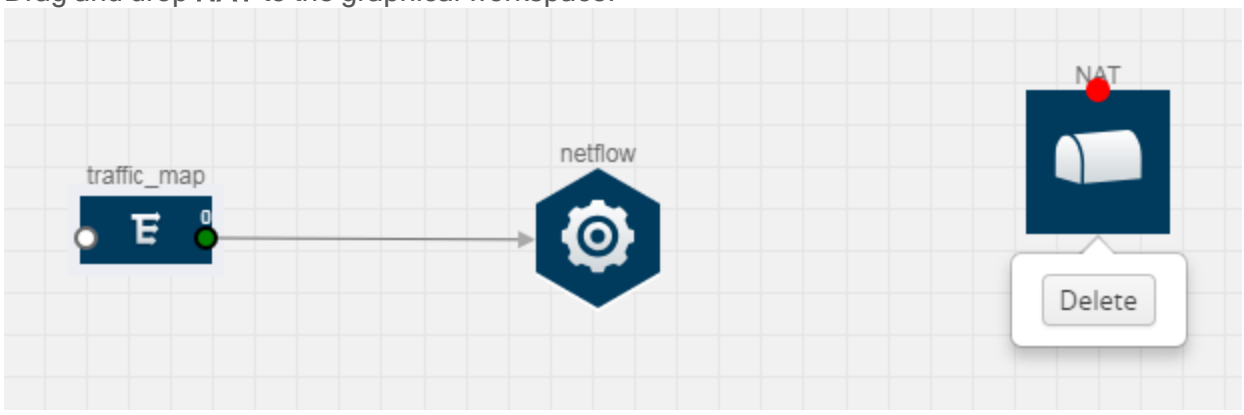
Example 1

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

1. Create a monitoring session.
2. In the monitoring session, create a Pass all map. A pass all map sends all the traffic received from the G-vTAP Agents to the tunnel endpoint or NAT.
3. Drag and drop a tunnel from **Tunnels**. A tunnel encapsulates the flow records and then sends them to the tools for full packet inspection.
4. Create a link from the Pass-all map to the tunnel endpoint. The traffic from the Pass-all map is forwarded to the tunnel endpoint that is connected to a tool.
5. Drag and drop a v5 NetFlow application.



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



9. Create a link from the v5 NetFlow application to NAT. The link must be configured with the destination IP address of the NetFlow collector and the GigaVUE V Series node interface. For steps to configure the link, refer to Add Applications to Monitoring Session.

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

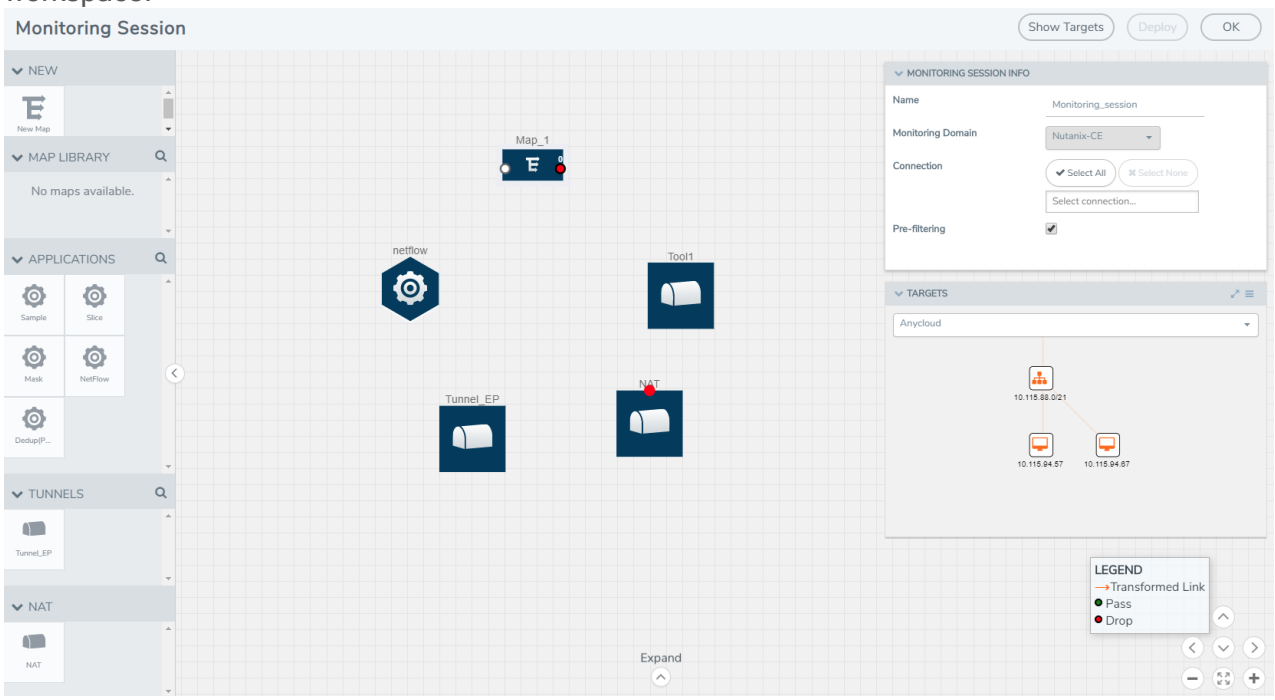
Deploy Monitoring Session

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.

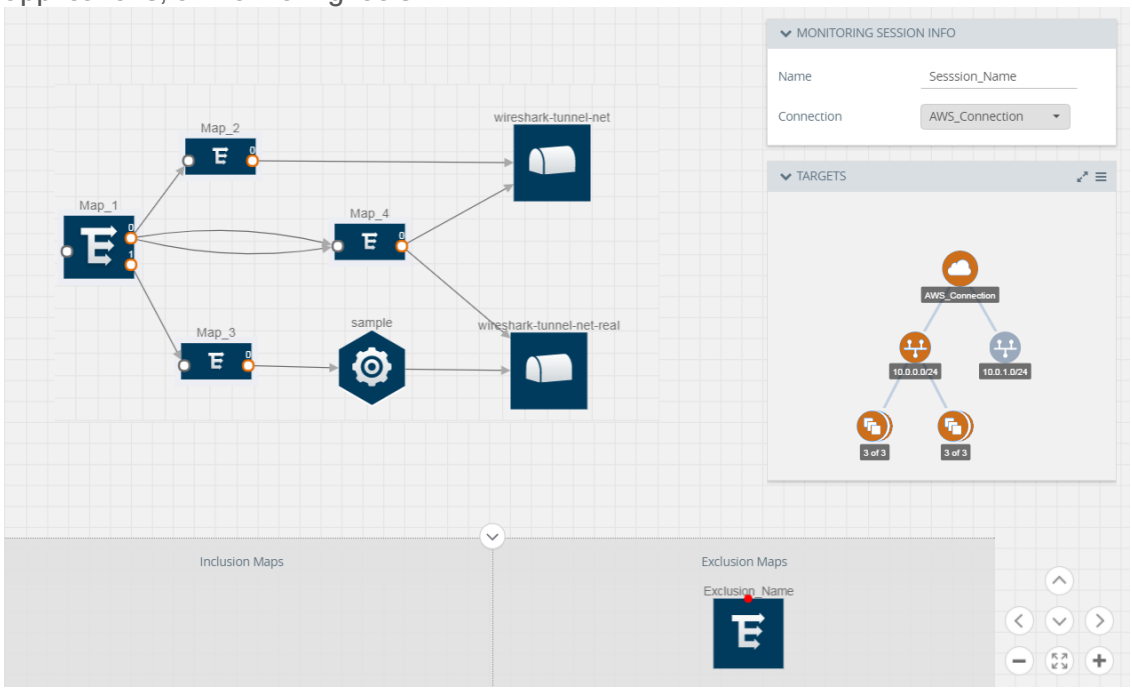
4. Drag and drop one or more tunnels from the **TUNNELS** section. The following figure illustrates three maps, one exclusion map, one application, and two tunnel endpoints dragged and dropped to the workspace.



   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. For information about adding link transformation, refer to Add Header Transformations.

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



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.For monitoring session deployment failures, refer to Troubleshoot AWS Cloud Issues.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.
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 VNets with the same subnet range. You can add VLAN ID, VLAN priority, and DSCP bits to the header for distinguishing the traffic coming from multiple VNets with the same subnet range.

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

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

GigaVUE V Series node supports the following header transformations:

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

To add a header transformation:

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

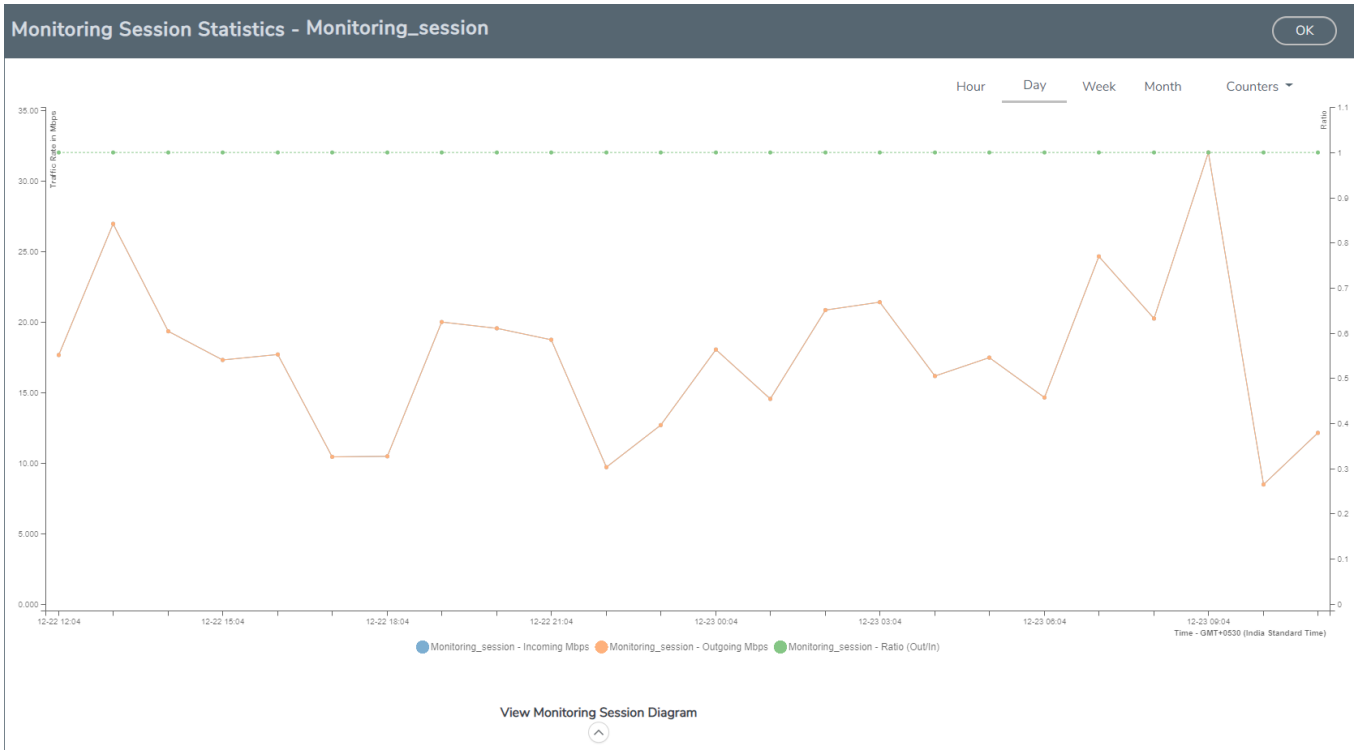
   NOTE: Do not apply VLAN Id and VLAN PCP transformation types with the Strip VLAN ID transformation type on the same link.
3. Click **Save**. The selected transformation is applied to the packets passing through the link.
4. Click **Deploy** to deploy the monitoring session.

View Monitoring Session Statistics

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

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

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



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

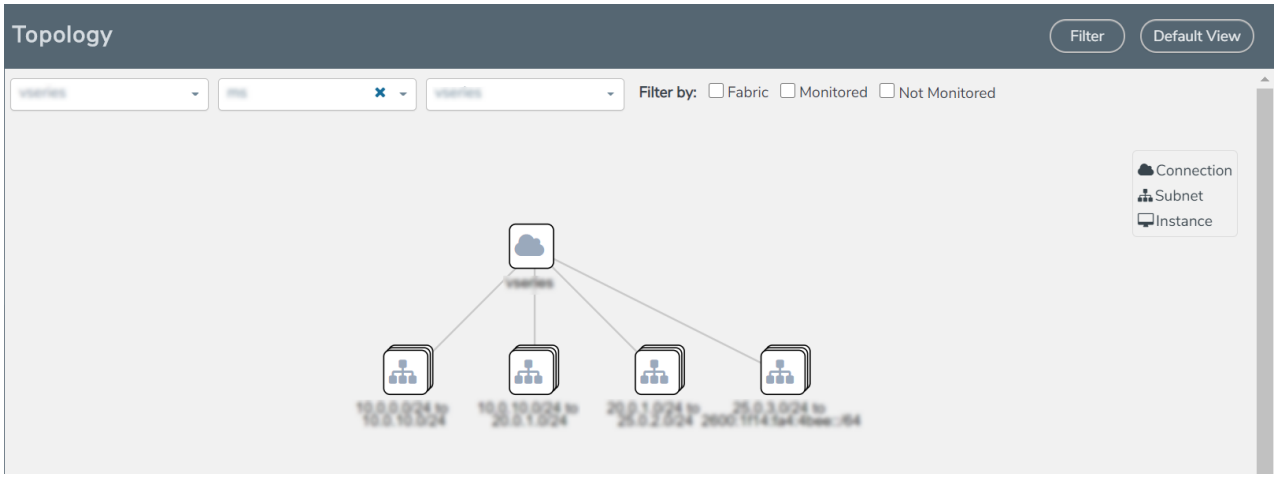
- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view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

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

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

Administer GigaVUE Cloud Suite for AWS

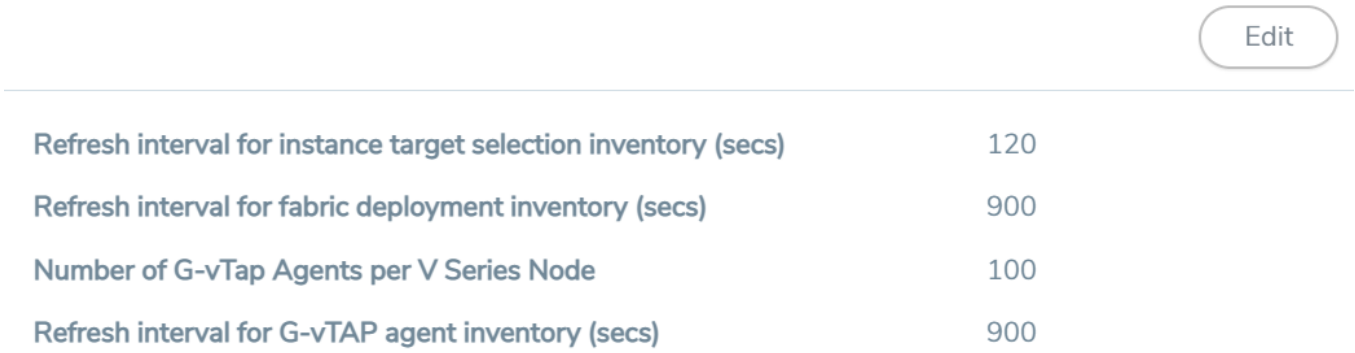
You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

- Configure AWS Settings
- Configure Proxy Server
- Role Based Access Control
- About Events
- About Audit Logs

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.

Go to **Inventory > VIRTUAL > AWS** and then click **Settings**.



In the Settings page, select **Advanced** tab to edit these AWS settings.

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 G-vTAP Agents per V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node. You can modify the number of instances for the nitro-based instance types
Refresh interval for G-vTAP Agent inventory (secs)	Specifies the frequency for discovering the G-vTAP Agents available in the VPC.

Refer Troubleshoot AWS Cloud Issues to troubleshoot the AWS Settings issues.

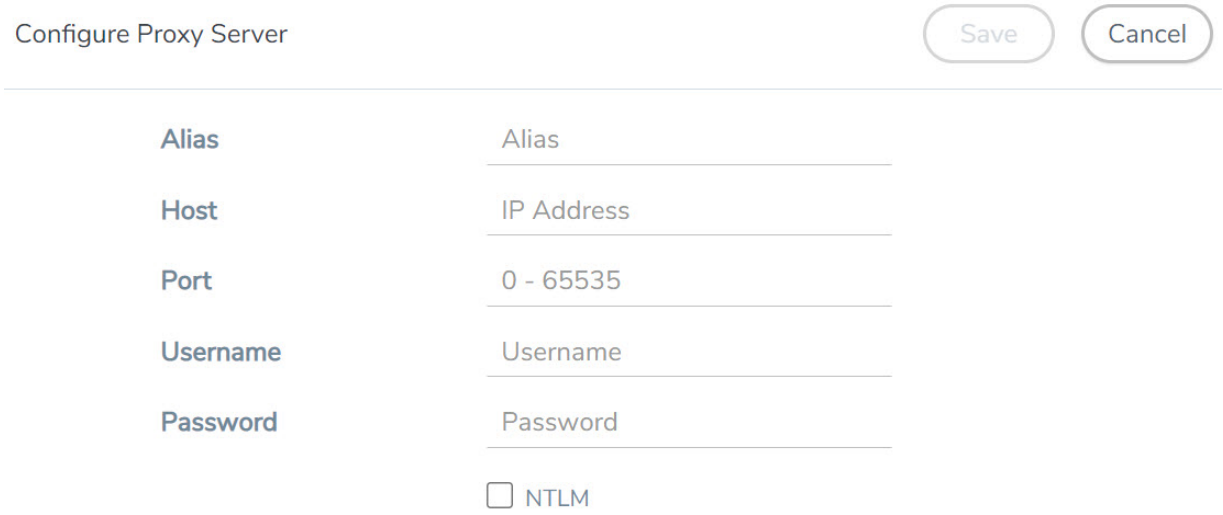
Configure Proxy Server

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.

NOTE: To configure the proxy server, you must be a user with **fm_super_admin** role or a user with write access to the **Physical Device Infrastructure Management** category.

To create a proxy server:

1. Go to **Inventory > VIRTUAL > AWS and** then click **Settings**. In the Settings page, select **Proxy Server Configuration** tab to edit these AWS settings.
2. Click **Add**. The Add Proxy Server page is displayed.



3. Select or enter the appropriate information as shown in the following table.

Field	Description
Alias	The name of the proxy server.
Host	The host name or the IP address of the proxy server.
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. On enabling NTML, enter the following information: • **Domain**–domain name of the client accessing the proxy server. • **Workstation**–name of the workstation or the computer accessing the proxy server.

4. Click **Save**. The new proxy server configuration is added to the Proxy Server Configuration page. The proxy server is also listed in the AWS Connection page.

Role Based Access Control

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

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

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

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

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

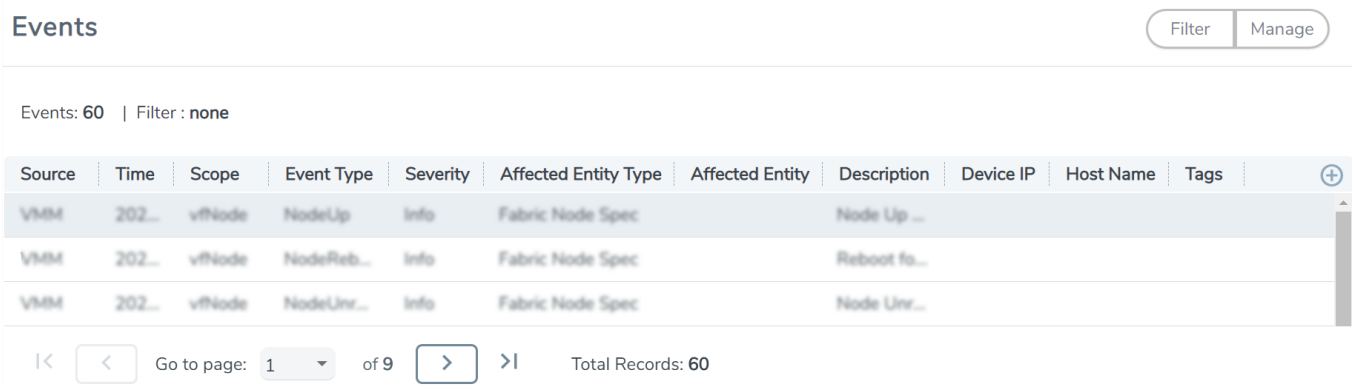
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

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

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

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

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



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

Controls/ Parameters	Description
Source	The source from where the alarms and events are generated.
Time	The timestamp when the event occurred. **IMPORTANT:** Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured timezone.
Scope	The category to which the alarms or events belong. Alarms and events can belong to the following category: Virtual Fabric Node, VM Domain, VM Manager.
Event Type	The type of event that generated the alarms and events.
Severity	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when GigaVUE V Series nodes are installed, such a message is displayed as Info.

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.

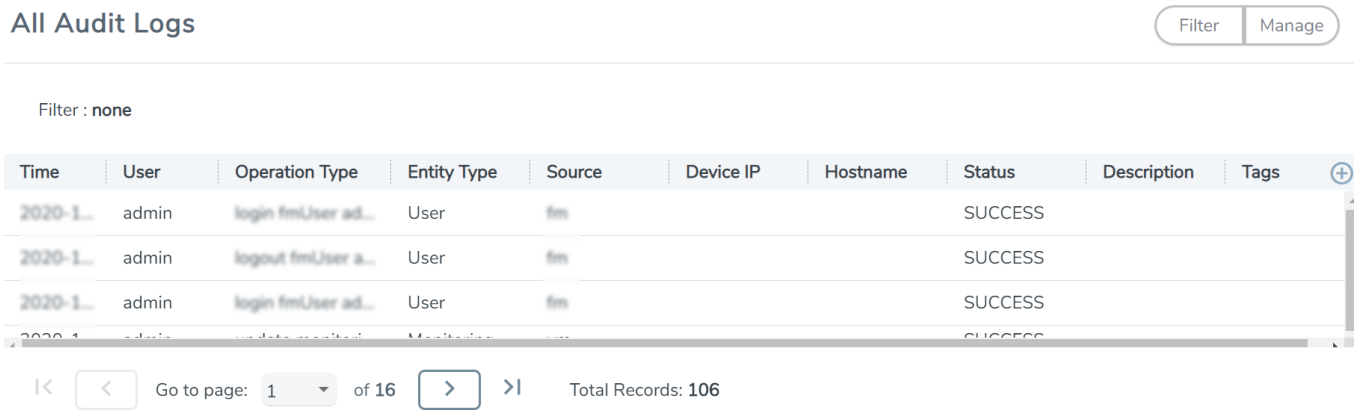
To filter the alarms and event:

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

About Audit Logs

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

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



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.

Parameters	Description
Source	Provides details on whether the user was in FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

GigaVUE-FM Version Compatibility Matrix

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

NOTE: GigaVUE-FM version 6.2 supports the latest fabric components version as well as earlier versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

GigaVUE-FM Version Compatibility for V Series 1 Configuration

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

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 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

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 VÜE Community

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA10 Hardware Installation Guide

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
GigaVUE-TA40 Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA100-CXP Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
*GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS-GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure-GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack-GigaVUE V Series 2 Guide
*GigaVUE Cloud Suite for Nutanix Guide–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for VMware–GigaVUE V Series Guide
*GigaVUE Cloud Suite for Third Party Orchestration
GigaVUE Cloud Suite for AnyCloud Guide
Universal Container Tap Guide

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for AWS-GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure-GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for OpenStack-GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

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

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)