GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide

GigaVUE Cloud Suite

Product Version: 6.2

Document Version: 1.0

Last Updated: Wednesday, March 8, 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 2

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:

Overview of 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 Proxy
  - GigaVUE® V Series 2 node

  To launch the AMI in AWS, refer to AMI and Permissions and Prepare G-vTAP Agent to Monitor Traffic
- **G-vTAP Agent** is an agent that is installed in the 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.
- **Next generation G-vTAP Agent** is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the G-vTAP agent mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the agent to V Series node and in-turn reduces the V Series load. Next generation G-vTAP gets activated only on Linux systems with a Kernel version above 5.4. 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 template can be applied to a monitoring session.
- **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 Proxy 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 Proxy** 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 Proxies to communicate with the GigaVUE V Series nodes.

For GigaVUE V Series configuration, you can configure the GigaVUE fabric components in a Centralized VPC only. In case of a shared VPC, you must select a VPC as your Centralized VPC for fabric configuration.

Following table describes the components that are required for the traffic acquisition methods

Traffic Acquisition Method	GigaVUE Fabric Components
G-vTAP	• G-vTAP Agent • G-vTAP Controller • GigaVUE V Series Node • GigaVUE V Series Proxy (optional)
VPC Traffic Mirroring without Load Balancer	• GigaVUE V Series Node • GigaVUE V Series Proxy (optional)
VPC Traffic Mirroring with Load Balancer	• GigaVUE V Series Node • GigaVUE V Series Proxy (optional)
Tunnel as a Source (TaaS)	• GigaVUE V Series Node

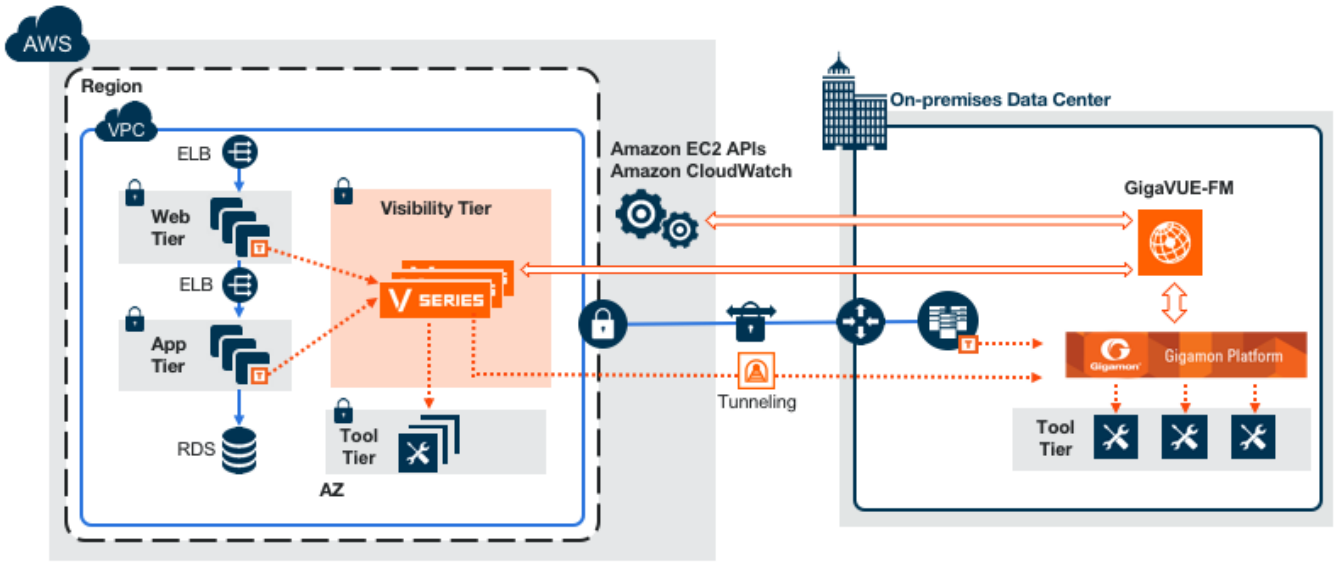
Architecture of GigaVUE Cloud Suite for AWS

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

- Hybrid Cloud
- Multi-VPC Cloud
- Centralized Fabric Controllers and Node Configuration

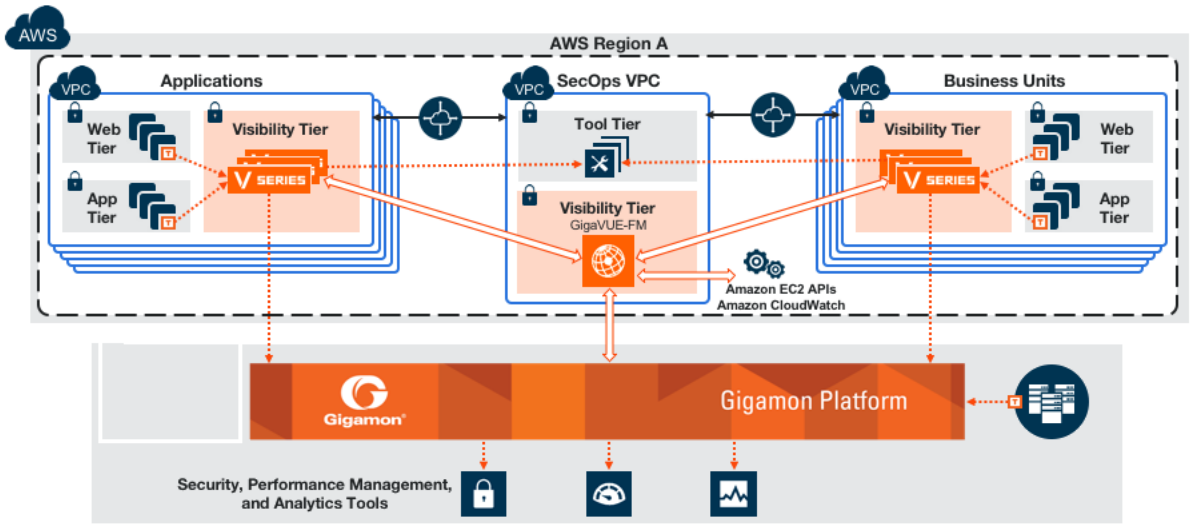
Hybrid Cloud

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.



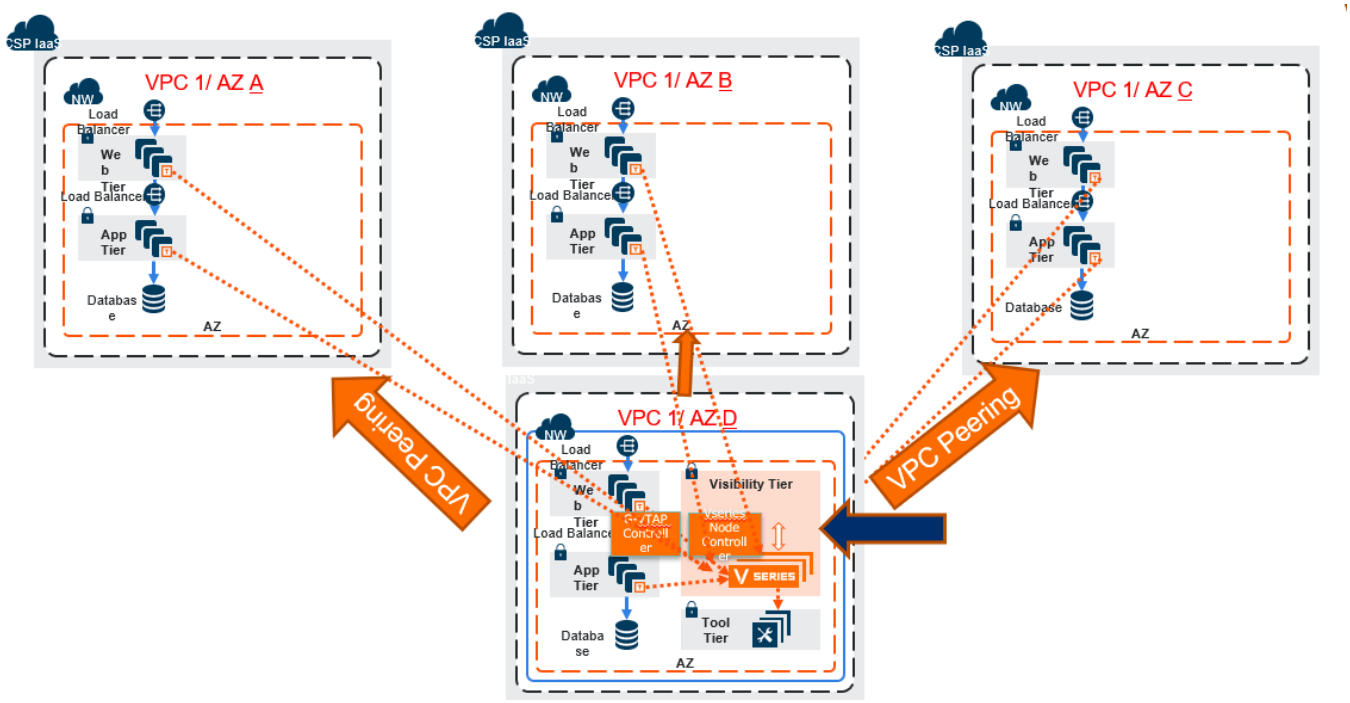
Centralized Fabric Controllers and Node Configuration

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 describeshow to plan and start the GigaVUE Cloud Suite for AWS in your AWS cloud.

Refer to the following sections for details:

- Purchase GigaVUE Cloud Suite using CPPO
- License Information
- Prerequisites
- AMI and Permissions
- Install and Upgrade GigaVUE-FM

Purchase GigaVUE Cloud Suite using CPPO

GigaVUE Cloud Suite is available as an Amazon Machine Image (AMI) product within the AWS Marketplace. When purchasing GigaVUE Cloud Suite using the AWS Marketplace with Consulting Partner Private Offers (CPPO), it comes with a Volume-based license.

The GigaVUE Cloud Suite available on AWS Marketplace via CPPO has only SecureVUEPlus base bundle. The list of SKUs available are:

- VBL-250T-BN-SVP
- VBL-50T-BN-SVP

Refer Volume Based License (VBL) for more detailed information on VBL and the available add-on packages.

License Information

GigaVUE Cloud Suite for AWS supports Volume Based License (VBL) model.

Refer to the following sections for details:

- Volume Based License (VBL)
- Apply License

Volume Based License (VBL)

All the V Series 2 nodes connected to GigaVUE-FM periodically reports statistics on the amount of traffic that flows through the V Series Nodes. The statistics give information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility into the actual amount of data, each licensed application is using on each node, and track the overuse if any. Volume-based licensing has a service period of 1 month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to Contact Sales.

Base Bundles

GigaVUE-FM has the following three base bundles:

- SecureVUEPlus (highest)
- NetVUE (intermediate)
- CoreVUE (lowest)

The number in the SKU indicates the total volume allowance of the SKU. For example, VBL-250T-BN-CORE has a volume allowance of 250 terabytes.

Bundle Replacement Policy

You can always upgrade to a higher bundle but you cannot move to a lower version. You cannot have two different base bundles at the same time however, you can have multiple base bundles of the same type. Once upgraded to a higher bundle, the existing lower bundles will be automatically deactivated.

Add-on Packages

GigaVUE-FM allows you to add additional packages called add-on packages to the base bundles. These add-on packages allow you to add additional applications to your base bundles. Add-on packages have their own start/end date and volume specifications.

Rules for add-on packages:

- Add-on packages can only to be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

The list of the available add-on SKUs are:

- VBL-50T-ADD-5GC
- VBL-250T-ADD-5GC
- VBL-2500T-ADD-5GC
- VBL-25KT-ADD-5GC

How GigaVUE-FM Tracks Volume-Based License Usage

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

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

Manage Volume-Based License

To manage active Volume-Based License:

1. On the left navigation pane, click  .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

   This page lists information like SKUs, Bundles, Start date, End date, Type, and Activation ID of the Volume-Based Licenses that are active. The expired licenses are automatically moved to the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar.

   Click on the individual SKU to view the list of applications available for that particular SKU.

Use the following buttons to manage your active VBL.

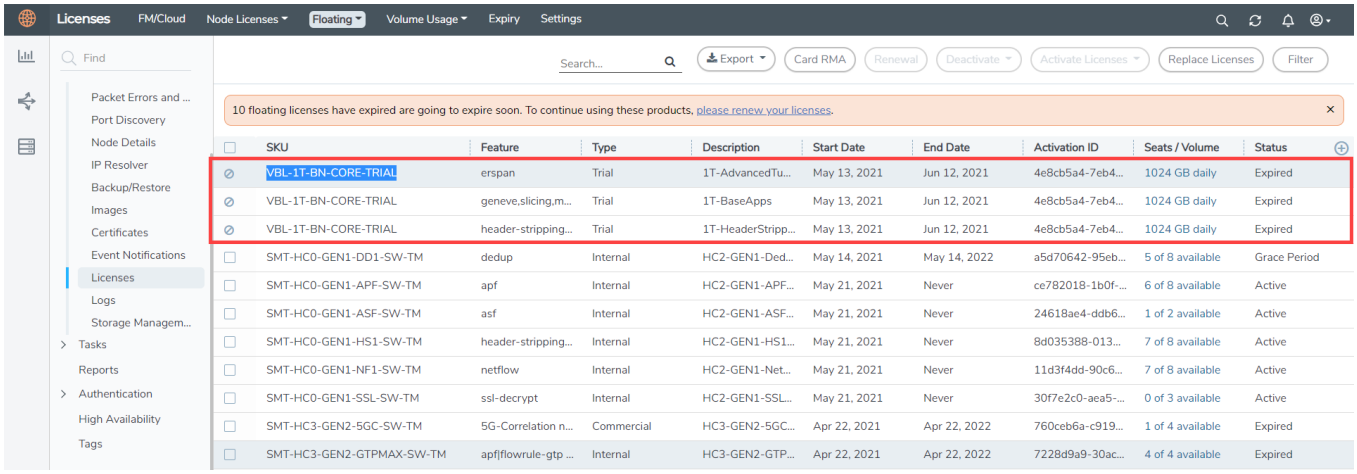
Button	Description
Activate Licenses	Use this button to activate a Volume-Based License. Refer Activate Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this option to narrow down the list of active Volume-Based Licenses that are displayed on the VBL active page.
Export	Use this button to export the details in the VBL active page to a CSV or XLSX file.

For more detailed information on dashboards and reports generation for Volume-Based Licensing refer the following table:

For details about:	Reference section	Guide
How to generate Volume-Based License reports	Generate VBL Usage Reports	GigaVUE Administration Guide
Volume-Based Licensed report details	Volume Based License Usage Report	GigaVUE Administration Guide
Fabric health analytics dashboards for Volume-Based Licenses usage	Dashboards for Volume Based Licenses Usage	GigaVUE-FM User Guide

Default Trial Licenses

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



This license includes the following applications:

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

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

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

Apply License

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

Prerequisites

Refer to the following topics for details:

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. You must also ensure that you are using Customer Managed Policies. 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 Proxies, GigaVUE V Series nodes, and G-vTAP Controllers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

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.

Following is the Network Firewall Requirements for V Series 2 node deployment.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	• HTTPS • SSH	TCP	• 443 • 22	Administrator Subnet	Management connection to GigaVUE-FM

Direction	Type	Protocol	Port	CIDR	Purpose
Inbound	Custom TCP Rule	TCP	5671	V Series 2 Node IP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation G-vTAP Agents to send statistics to GigaVUE-FM.
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Controller to communicate with G-vTAP Agents
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Agents to communicate with G-vTAP Controller
Outbound	• UDP • IP	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
V Series Proxy (optional)					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 node IP	Allows V Series Proxy to communicate with V Series node
V Series 2 node					
Inbound	Custom TCP Rule	TCP	8889	• GigaVUE-FM IP • V Series Proxy IP	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node

Direction	Type	Protocol	Port	CIDR	Purpose
Inbound	• UDP • IP	• UDP (VXLAN) • IP Protocol (L2GRE)	• VXLAN (default 4789) • L2GRE	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	Custom UDP Rule	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	• echo request • echo reply	Tool IP	Allows V Series node to health check tunnel destination traffic

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 Proxy in your VPC.

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

Default Login Credentials

You can login to the GigaVUE V Series Node, GigaVUE V Series proxy, and G-vTAP Controller by using the default credentials.

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is: Username: orchestration Password: Orchestration@123
GigaVUE V Series proxy	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: orchestration

Product	Login credentials
	Password: Orchestration@123
G-VTAP Controller	You can login to the GigaVUE V Series proxy by using ssh. The default username and password is: Username: orchestration Password: Orchestration@123

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

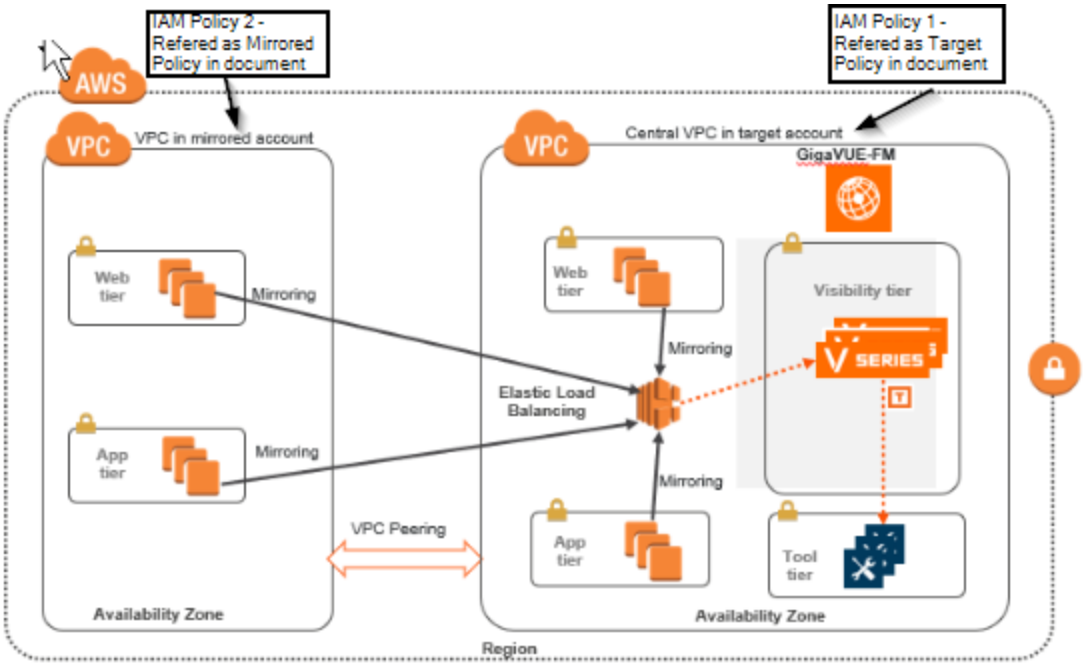
The following IAM policy must be used for VPC mirroring with ELB:

```
{
"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 AWS Credentials
- Create a Monitoring Domain
- Configure GigaVUE Fabric Components in GigaVUE-FM
- Configure GigaVUE Fabric Components in AWS
- Configure an External Load Balancer on GigaVUE Cloud Suite for AWS
- Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS
- Configure a Traffic Pre-filter
- Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

Refer Gaining Application Level Visibility Across Private and Public Cloud Environments for more detailed information.

Deployment Options for GigaVUE Cloud Suite for AWS

This section provides a detailed information on the multiple ways in which GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 can be configured to provide visibility for physical and virtual traffic. There are three different ways in which GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 can be configured based on the traffic acquisition method and the method in which you want to deploy fabric components. For information on the prerequisites and work flow refer the following topics:

- Prerequisites
- Deploy GigaVUE Fabric Components using AWS
- Deploy GigaVUE Fabric Components using GigaVUE-FM
  - Traffic Acquisition Method as G-vTAP
  - Traffic Acquisition Method as VPC Mirroring
  - Traffic Acquisition Method as Tunnel

Deploy GigaVUE Fabric Components using AWS

GigaVUE-FM allows you to use AWS as an orchestrator to deploy GigaVUE fabric nodes and then use GigaVUE-FM to configure the advanced features supported by these nodes. Refer the following table for the step-by-step instructions:

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Install G-vTAP Agents	For Linux: Linux G-vTAP Agent Installation For Windows: Windows G-vTAP Agent Installation
3	Create the AWS Credentials	Create AWS Credentials
4	Create a Monitoring Domain Ensure that the Use FM to Launch Fabric toggle button is disabled.	Create a Monitoring Domain
5	Configure GigaVUE Fabric Components Select G-vTAP as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in GigaVUE-FM
6	Create Monitoring session	Create a Monitoring Session
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Fabric Components using GigaVUE-FM

You can deploy GigaVUE fabric components using GigaVUE-FM using one of the following three traffic acquisition methods:

Traffic Acquisition Method as G-vTAP

In traffic acquisition using G-vTAP Agent, the traffic from Virtual Machines is acquired using the G-vTAP Agents and forwarded to the V Series nodes. To acquire traffic using G-vTAP Agent, perform the following steps:

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Install G-vTAP Agents	For Linux: Linux G-vTAP Agent Installation For Windows: Windows G-vTAP Agent Installation
3	Create the AWS Credentials	Create AWS Credentials
4	Create a Monitoring Domain Ensure that the Use FM to Launch Fabric toggle button is enabled.	Create a Monitoring Domain
5	Configure GigaVUE Fabric Components Select G-vTAP as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in GigaVUE-FM
6	Create Monitoring session	Create a Monitoring Session
7	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
8	Deploy Monitoring Session	Deploy Monitoring Session
9	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as VPC Mirroring

Perform the following steps to use VPC mirroring as your traffic acquisition method:

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Create a Monitoring Domain Ensure that the **Use FM to Launch Fabric** toggle button is enabled.	Create a Monitoring Domain
3	Configure GigaVUE Fabric Components Select VPC Mirroring as the Traffic Acquisition Method. You can configure a prefilter and determine the VPC endpoint traffic that is mirrored. For more information on prefiltering, see Configure a Traffic Pre-	Configure GigaVUE Fabric Components in GigaVUE-FM

Step No	Task	Refer the following topics
	filter.	
4	Create Monitoring session	Create a Monitoring Session
5	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
6	Deploy Monitoring Session	Deploy Monitoring Session
7	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Tunnel

You can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying G-vTAP Agents or G-vTAP controllers. Perform the following steps to use Tunnel as your traffic acquisition method:

Step No	Task	Refer the following topics
1	Install GigaVUE-FM on AWS	Install GigaVUE-FM on AWS
2	Create a Monitoring Domain Ensure that the **Use FM to Launch Fabric** toggle button is enabled.	Create a Monitoring Domain
3	Configure GigaVUE Fabric Components Select Tunnel as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in GigaVUE-FM
4	Create Monitoring session	Create a Monitoring Session
5	Create Ingress and Egress Tunnel Endpoints	Create Ingress and Egress Tunnels
6	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
7	Deploy Monitoring Session	Deploy Monitoring Session
8	View Monitoring Session Statistics	View Monitoring Session Statistics

Install GigaVUE-FM on AWS

You can deploy GigaVUE-FM using the AWS CloudFormation Templates (CFT) found in the AWS Marketplace or deploy the latest GigaVUE-FM instance manually using the public images (AMI) through the AWS EC2.

You can launch GigaVUE-FM in AWS using one of the following methods:

- Launch GigaVUE-FM using CFT
- Launch GigaVUE-FM using an Instance in AMI

Launch GigaVUE-FM using CFT

Refer to the following topics for details:

- Launch GigaVUE-FM from AWS Marketplace
- Configure an AWS CloudFormation Stack

Launch GigaVUE-FM from AWS Marketplace

To launch the GigaVUE-FM instance from the AWS Marketplace:

1. Login to your AWS account.
2. Go to https://aws.amazon.com/marketplace/.
3. In the **Search** field, type Gigamon and click Search.
4. Select the latest GigaVUE Cloud Suite version link from the list for Gigamon products.
5. Click **Continue to Subscribe**. The **Subscribe to this software** page is displayed, where the complete detail about the product is described.
6. Click **Continue to Configuration**. The **Configure this software** page is displayed.
7. In the Configure this software page, select the following:
   a. From the **Fulfillment option** drop-down list, select **Auto Deploy GigaVUE-FM using AWS CFT**.
   b. From the **Software version** drop-down list, select the latest version.
   c. From the **Region** drop-down list, select the appropriate region.
   d. Click **Continue to Launch**. The **Launch this Software** page is displayed.
8. In the Launch this Software page, from the **Choose Action** drop-down, select **Launch CloudFormation**.
9. Click **Launch**. The **Create Stack** page is displayed.

Configure an AWS CloudFormation Stack

To configure CloudFormation Stack:

1. In the **Create Stack** page, enter or select the following details:
   a. Specify a Template and Template source for the Stack.
   b. Click **Next**. The **Specify stack details** page is displayed.

2. In the Specify stack details page, enter or select the following details:
   a. In the **Stack name** field, enter a name for the stack.
   b. Enter or select the following details for the Parameters.

Fields	Action
GigaVUE-FM Instance Configuration	
Instance Type	Select **m4.xlarge** as the minimum instance type for GigaVUE-FM **NOTE:** Do not select the t2 instance types as they are not supported.
Key Pair	Select the name of an existing Amazon EC2 key pair.
Volume Size	The default volume size is 40 GB. You can change the volume size based on your requirement.
GigaVUE-FM Network Configuration	
VPC ID	Select the existing VPC ID.
Subnet	Select the existing public subnet ID.
GigaVUE-FM Security Group Configuration	
SSH Location	Enter the IP address or subnet that requires SSH access to the GigaVUE-FM instance.
CIDR IP	Enter the CIDR block where GigaVUE-FM would be deployed to allow management port access to the other components.

   c. Click **Next**. The **Configure stack options** page is displayed.
3. In the Configure stack options page, enter or select the following details.
   a. In the **Tags** section, enter the key and value pairs. Click **Add tag** to add new tags and click **Remove** to remove tags.
   b. In the **Permissions** section, select the IAM roles for the CloudFormation. Refer to the AMI and Permissions topic in the *GigaVUE Cloud Suite for AWS Guide* for detailed information on the required IAM roles.
   c. In the **Stack failure options** section, select a behavior for stack failures.
   d. In the **Advanced options** section, select the required stack policy and notification options.
   e. Click **Next**. The **Review** page is displayed.
4. In the Review page, review the complete details and then select the **I acknowledge that AWS CloudFormation might create IAM resources** check box.
5. Click **Create Stack** to deploy GigaVUE-FM in AWS.

Launch GigaVUE-FM using an Instance in AMI

To launch GigaVUE-FM using a public image:

1. Login to the AWS EC2.
2. From the navigation pane, select **Images > AMIs**. The **Amazon Machine Images (AMIs)** page appears.
3. Select the latest GigaVUE-FM public image and click **Launch instance from image**. The Instance launch wizard is displayed.
4. In the Instance Launch wizard, select or enter the details in the respective tabs. Refer to the following table for details.

Fields	Action
1. Choose AMI	Select the latest GigaVUE-FM public image.
2. Choose Instance Type	Select **m4.xlarge** as the minimum instance type for GigaVUE-FM **NOTE:** Do not select the t2 instance types as they are not supported.
3. Configure Instance	Select the instance details by your requirements like VPC, Subnet (management network), IAM Role, and more. Refer to the AMI and Permissions topic in the *GigaVUE Cloud Suite for AWS Guide* for detailed information on the required IAM roles. • You can also launch your instance into an Auto Scaling Group. • You can launch multiple instances from the same AMI.
4. Add Storage	Select **Add New Volume**, select a Snapshot, and enter 40 (GiB) as the Size for the new volume in addition to the Root volume 40 (GiB).
5. Add Tags	Enter the key-value pair information for the instances and volumes.
6. Configure Security Group	Select an existing security group or select the protocol type, CIDR IP, and other details for a new security group. For security group values, refer to the Security Group topic in the *GigaVUE Cloud Suite for AWS Guide*.
7. Review	Review your instance launch details.

5. In the Review tab, click **Launch**.

If the page prompts you to specify key pair, select an existing key pair from the drop-down or create a new key pair.

Initial GigaVUE-FM Configuration

It may take several minutes for the GigaVUE-FM instance to initialize. After the initialization is completed, you can verify the instance through the web interface as follows:

1. In your EC2 Instances page, select the launched GigaVUE-FM instance and expand the page in the **Descriptions** tab to view the instance information.
2. Copy and paste the Public IP address into a new browser window or tab.
3. Copy the Instance ID from the **Descriptions** tab.

If GigaVUE-FM is deployed inside AWS, use **admin** as the username and the **Instance ID** as the default password for the admin user to login to GigaVUE-FM, for example i-079173111e2d73753 **(Instance ID)**.

If GigaVUE-FM is deployed outside the AWS, use admin123A!! as the default admin password.

After logging into GigaVUE-FM, you are prompted to change the default password.

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.

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, 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.
   - gvtap-agent_**6.2.00**_x86_64.rpm
   - gvtap.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files 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. 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 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
   ```

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.)

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**.

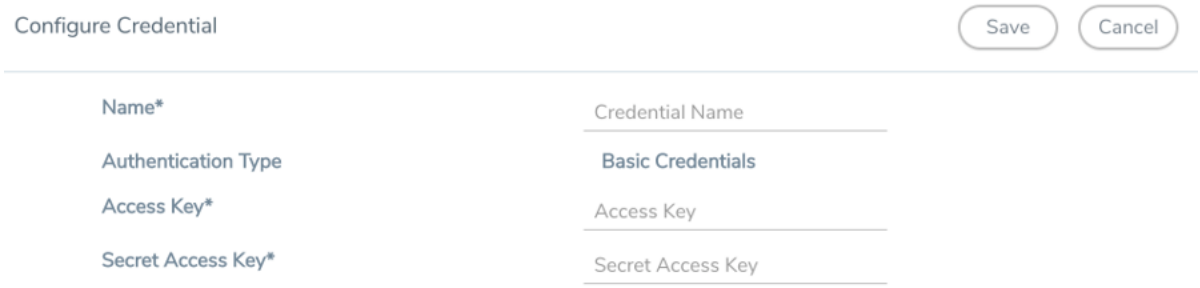
Create AWS Credentials

You can monitor workloads across multiple AWS accounts within one monitoring domain. The GigaVUE fabric nodes can be shared among many AWS accounts to reduce the cost since this was possible only with AWS STS and limited to one region.

- After launching GigaVUE-FM in AWS, the **EC2 Instance Role** authentication credential is automatically added to the AWS Credential page as the default credential.
- You can only add the **Basic Credentials** authentication credentials to the AWS Credential page.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and then click **Settings > Credentials**
2. On the AWS Credential page, click the **Add** button. The **Configure Credential** page appears.



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

Field	Action
Name	An alias used to identify the AWS credential.
Authentication Type	**Basic Credentials** For more information, refer to AWS Security Credentials.
Access Key	Enter your AWS access key. It is the credential of an IAM user or the AWS account root user.
Secret Access Key	Enter your secret access key. It is the AWS security password or key.

4. Click **Save**. You can view the list of available credentials in the AWS Credential page.

Required Policies and Permissions

To add multiple AWS accounts in a monitoring domain, you must add the access and role name of all the additional accounts to your STS policy. Following is a sample STS policy where the *account2* and *account3* are the accesses added to the existing *account1* policy.

```
{
    "Version": "2012-10-17",
    "Statement": {
       "Effect": "Allow",
       "Action": "sts:*",
       "Resource": [
          "arn:aws:iam::account2:role/ROLE-NAME"
          "arn:aws:iam::account3:role/ROLE-NAME"
                   ]
                 }
}
```

For detailed information on the policies attached to GigaVUE-FM, refer to Permissions and Privileges

Following is the required IAM policy to exist in your remote networks:

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

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

Following is the required trust policy to set in your remote account:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Effect": "Allow",
           "Principal": {
               "Service": "ec2.amazonaws.com",
               "AWS": "arn:aws:iam::account:role/ROLE-NAME"
                       },
           "Action": "sts:AssumeRole"
         }
                ]
}
```

Create a Monitoring Domain

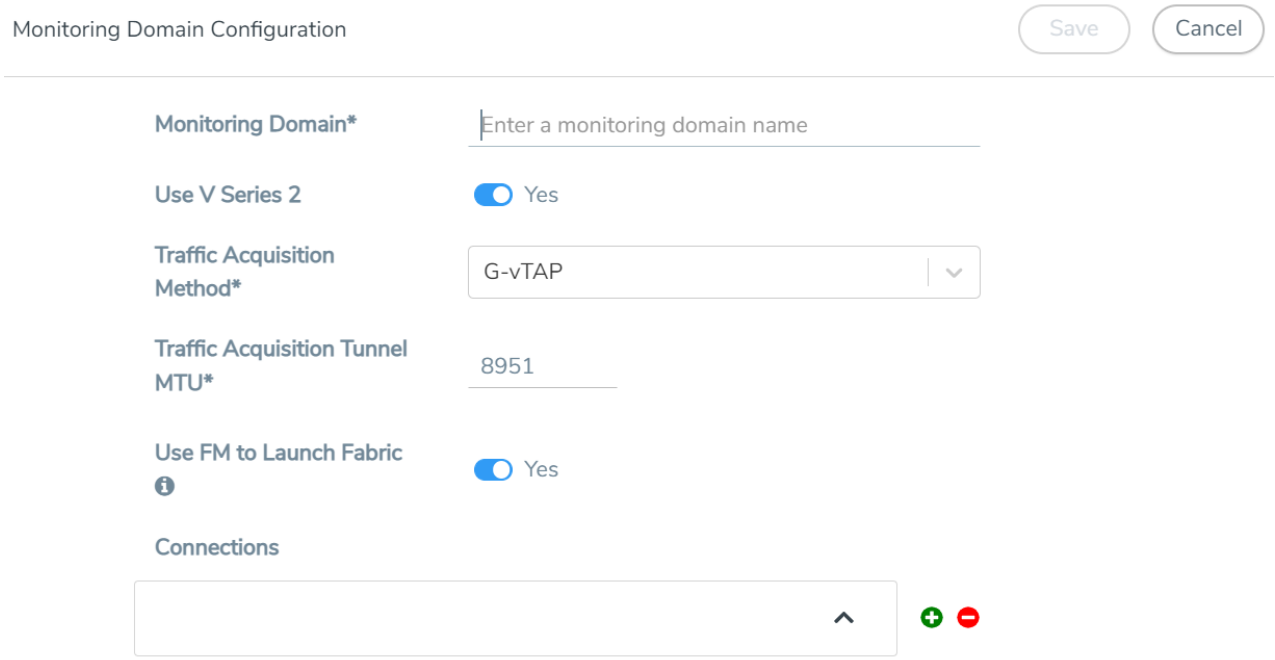
GigaVUE-FM connects to the VPC through the EC2 API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the EC2 API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

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.

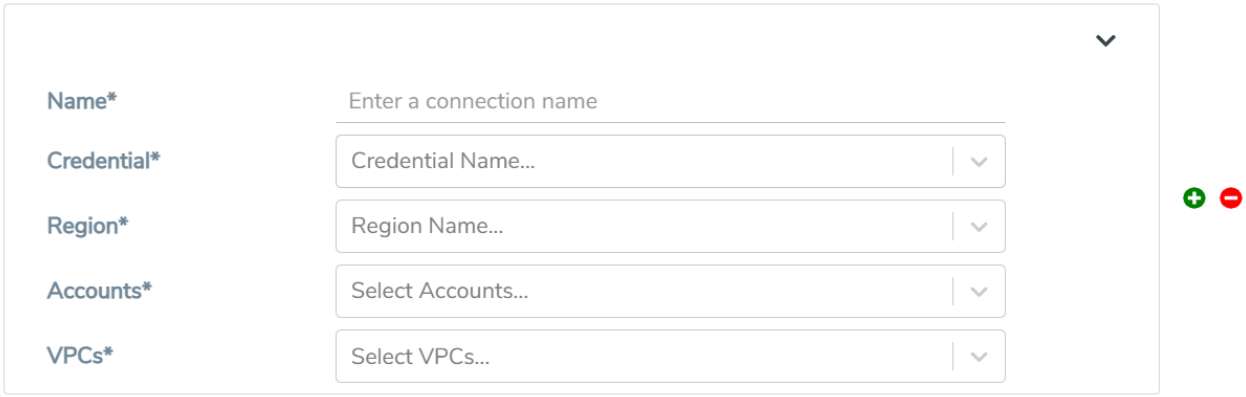
To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > 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	Action
Monitoring Domain	An alias used to identify the monitoring domain.
Use V Series 2	Select **Yes** to configure GigaVUE V Series 2 node.
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. You can also configure the G-vTAP Controller and G-vTAP Agents from your own orchestrator. Refer to Configure GigaVUE Fabric Components using AWS Orchestrator for detailed information. ▪ **VPC Traffic Mirroring**: If you select the VPC Traffic Mirroring option, the mirrored traffic from your workloads is directed directly to 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. Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment. You can choose to use an external load balancer for VPC Traffic Mirroring. Select **Yes** to use load balancer. Refer to Configure an External Load Balancer on GigaVUE Cloud Suite for AWS for detailed information. • G-vTAP Controller configuration is not applicable for VPC Traffic Mirroring. • VPC mirroring does not support cross-account solutions without a load balancer. • For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions and Privileges topic for details. • After deploying the Monitoring Session, a traffic mirror session is created in your AWS VPC consisting of a session, a filter, sources, and targets. For more details, refer to Traffic Mirroring in AWS Documentation. ▪ **Customer Orchestrated Source**: If you use select **Customer Orchestrated Source** as the tapping method, you can use the Customer Orchestrated Source as a source option in the monitoring session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying G-vTAP Agents and G-vTAP Controllers. The user is responsible for creating this tunnel feed and pointing it to the GigaVUE V Series node(s). **NOTE:** When using Observability Gateway (AMX) application, select the **Traffic Acquisition Method** as **Customer Orchestrated Source**.
Traffic Acquisition Tunnel MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP Agent to the GigaVUE V Series node.

Field	Action
	The default value is 8951. The G-vTAP Agent tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.
Use FM to Launch Fabric	Select **Yes** to Configure GigaVUE Fabric Components in GigaVUE-FM or select **No** to Configure GigaVUE Fabric Components in AWS.
Connections Connections  **NOTE:** You can add multiple connections in a monitoring domain. Refer to Create AWS Credentials for more information on adding multiple AWS **Basic Credentials**.	
Name	An alias used to identify the connection.
Credential	Select an AWS credential. For detailed information, refer to Create AWS Credentials.
Region	AWS region for the monitoring domain. For example, US West.
Accounts	Select the AWS accounts
VPCs	Select the VPCs to monitor

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

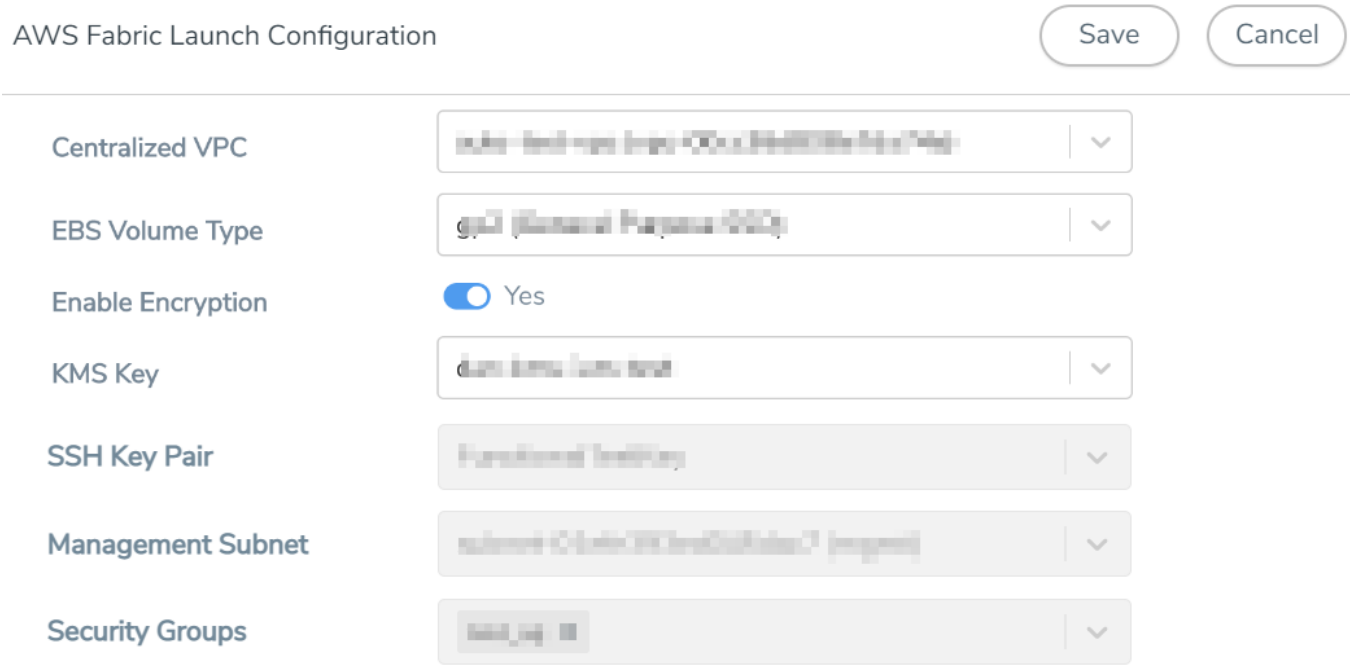
Configure GigaVUE Fabric Components in GigaVUE-FM

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 Proxy
- Configure GigaVUE V Series Node

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



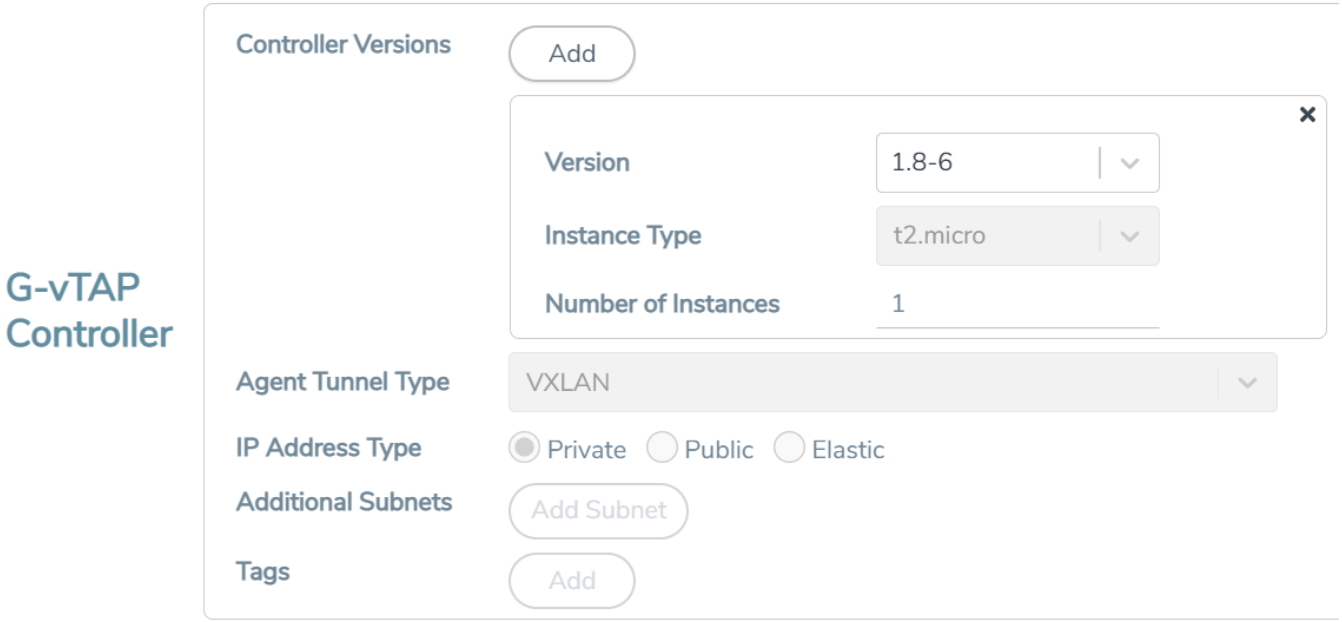
Fields	Description
Centralized VPC	Alias of the centralized VPC in which the G-vTAP Controllers, V Series Proxies and the GigaVUE V Series Nodes are launched.
EBS Volume Type	The Elastic Block Store (EBS) volume that you can attach to the fabric components. The available options are: ▪ gp2 (General Purpose SSD) ▪ io1 (Provisioned IOPS SSD) ▪ Standard (Magnetic)
Enable Encryption	Select **Yes** to enable encryption or select **No** to disable encryption. On selecting Yes to enable encryption, a **KMS Key** field appears. Enter the KMS key for the encryption.
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.

- G-vTAP Controller configuration is not applicable for VPC Traffic Mirroring selected as the traffic acquisition method.
- 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.
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.
IP Address Type	The IP address type. Select one of the following: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the G-vTAP Controller and GigaVUE-FM. ▪ Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. ▪ Select **Elastic** if you want a static public IP address for your instance. Ensure to have the available elastic IP address in your VPC. **NOTE:** The elastic IP address does not change when you stop or start the instance.
Additional Subnet(s)	(Optional) If there are G-vTAP Agents on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the G-vTAP Controller can communicate with all the G-vTAP Agents. Click **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
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.

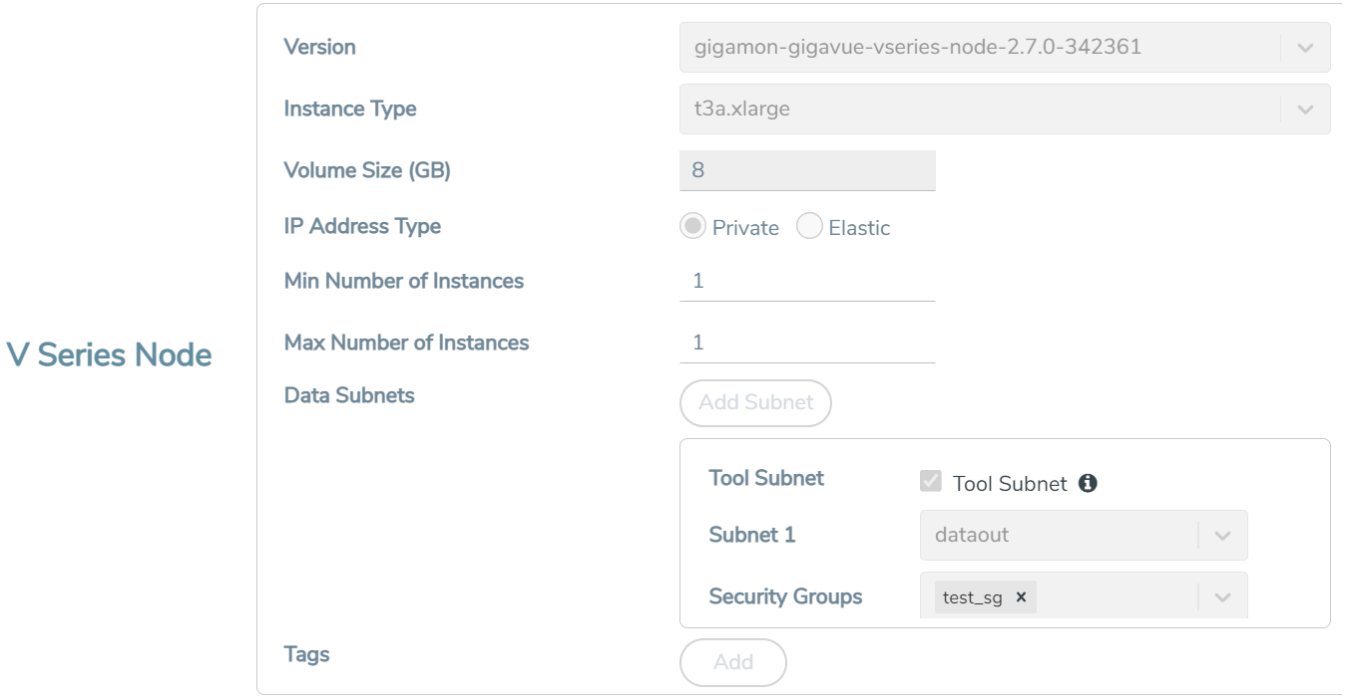
Configure GigaVUE V Series Proxy

Select **Yes** for the Configure a GigaVUE V Series Proxy field. GigaVUE V Series Proxy is optional for the GigaVUE Cloud Suite for AWS.

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

Fields	Description
Version	GigaVUE V Series Proxy version.
Instance Type	Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Number of Instances	Number of GigaVUE V Series Proxy 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 Proxy. 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 Proxy 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 Proxy 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 Proxy instances in your AWS environment.

Configure GigaVUE V Series Node



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

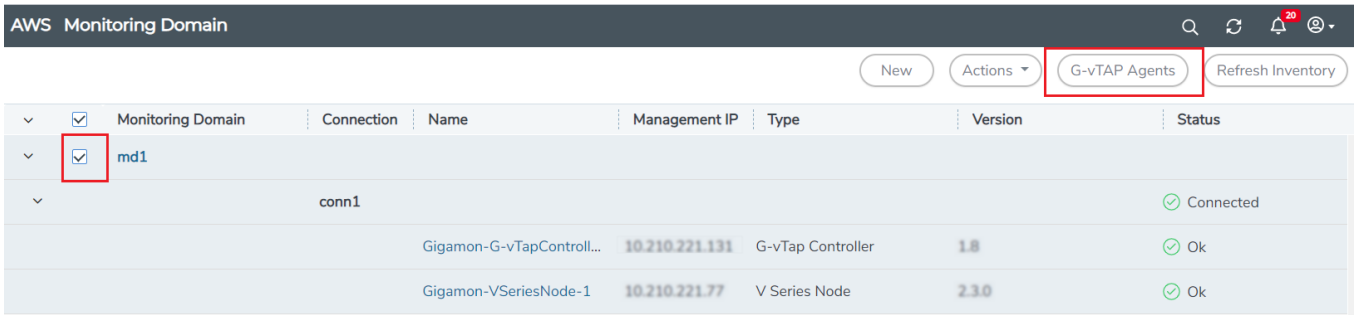
Fields	Description
Version	GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. The default instance type is nitro-based t3a.xlarge. The recommended instance type is c5n.xlarge for 4 vCPU and c5n.2xlarge for 8vcpu. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page. **NOTE:** The GigaVUE V Series 2 Node does not support non-nitro-based instance types.
Volume Size	The size of the storage disk. The default volume size is 8. The recommended volume size is 80. **NOTE:** When using Application Metadata Exporter, the minimum recommended Volume Size is 80GB.
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 **Elastic** if you want a static IP address for your instance. Ensure to have the

Fields	Description
	available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
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.
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 proxy, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

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



Configure Role-Based Access for Third Party Orchestration

Before deploying the fabric components using a third party orchestrator, we must create users, roles and the respective user groups in GigaVUE-FM. The Username and the Password provided in the User Management page will be used in the registration data that can be used to deploy the fabric components in your orchestrator.

Users

The Users page lets you manage the GigaVUE-FM and GigaVUE-OS FM users. You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM.

Add Users

This section provides the steps for adding users. You can add users only if you are a user with **fm_super_admin role** or a user with either read/write access to the FM security Management category.

IMPORTANT: It is recommended to create users through GigaVUE-FM:

- You cannot view or manage users created in GigaVUE-FM CLI using GigaVUE-FM.
- You cannot view changes made to the users in GigaVUE-FM CLI in GigaVUE-FM.

NOTE: Monitor and operator users are not available in GigaVUE-FM. However, if you upgrade from a previous version in which monitor/operator users have been mapped in map default user, then after upgrade:

- **In AAA:** Users authenticated through the external servers will be assigned the fm_user role.
- **In LDAP:** Remote group based DN entry will not be migrated.

To add users perform the following steps:

1. On the left navigation pane, click  and select **Authentication** > **User Management > Users**. The **User Management** page is displayed.

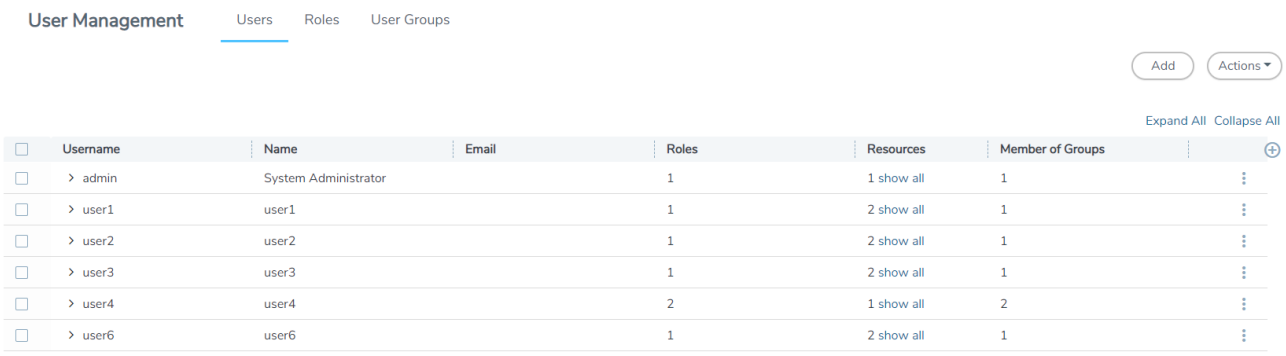


Figure 1 *FM Users Page*

2. Click **Add**. In the Create User wizard that appears perform the following steps. Click **Continue** to progress forward and click **Back** to navigate backward and change details.

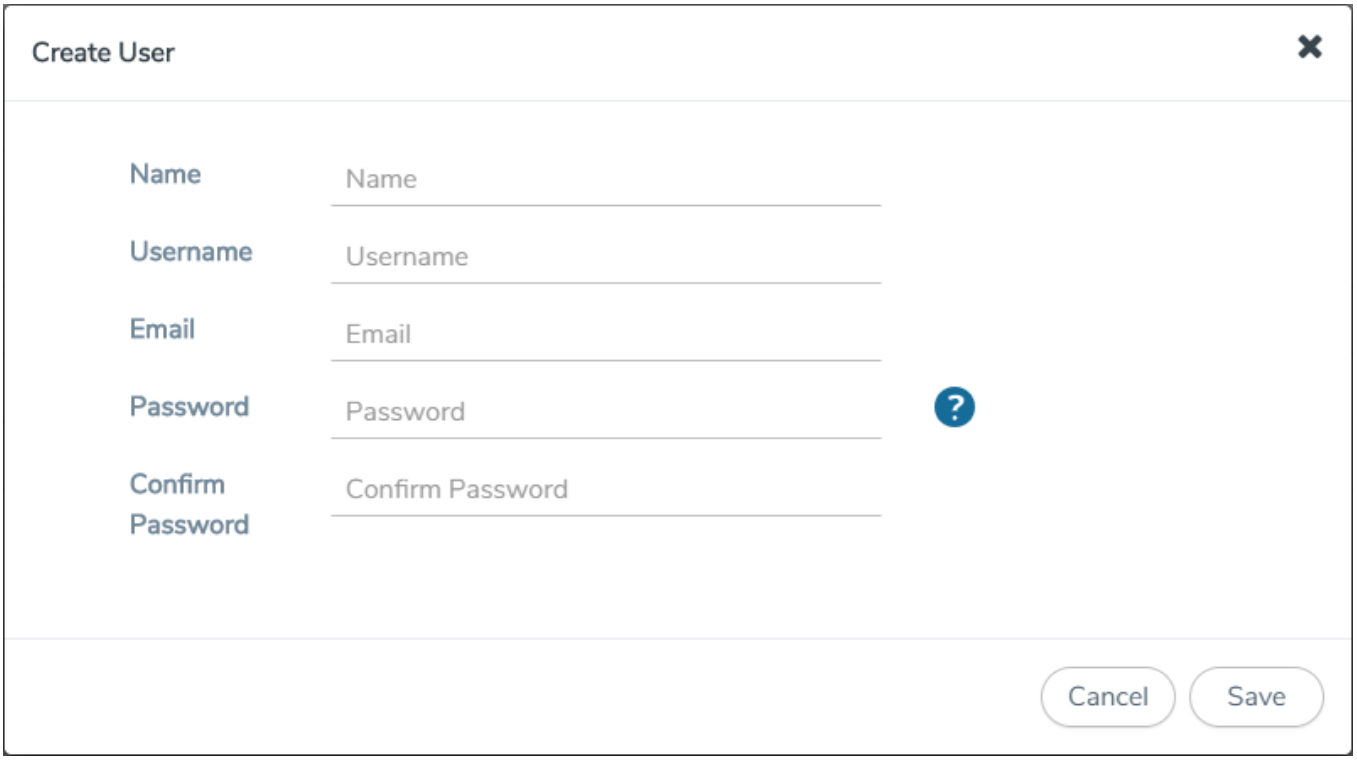


Figure 2 *Create User*

a. In the **User Information** tab, enter the following details:

- **Name:** User's actual name
- **User Name**: User name
- **Email**: Email ID of the user
- **Password/Confirm Password**: Password for the user. Refer to the Change Your Password section.

> **NOTE:** GigaVUE-FM will prompt for your password.

b. Click **Save**.

The new user is added to the summary list view.

You can also assign users to roles and user groups that set the access permissions. For the steps to create roles, refer to Create Roles. For the steps to create groups, refer to Create Groups.

> **NOTE:** If you have logged in as a user with **fm_super_admin** role or a user with either read/write access on FM security Management category, then click on the ellipsis to:

- **Edit:** Edit the user details.
- **Delete:** Delete a user.
- **View Details:** View the user details.

The User name and password provided in this section will be used as the User and Password in the registration data.

After adding User, you must configure roles for third party orchestration.

Create Roles

You can associate a rule with user. Under the **Select Permissions** tab select **Third Party Orchestration** and provide read/write permissions.

Create Roles

This section describes the steps for creating roles and assigning user(s) to those roles.

GigaVUE-FM has the following default roles:

- **fm_super_admin** — Allows a user to do everything in Fabric Manager, including adding or modifying users and configuring all AAA settings in the RADIUS, TACACS+, and LDAP tabs. Can change password for all users.
- **fm_admin** — Allows a user to do everything in Fabric Manager except add or modify users and change AAA settings. Can only change own password.
- **fm_user** — Allows a user to view everything in Fabric Manager, including AAA settings, but cannot make any changes.

> **NOTE:** If you are a user with read-only access you will be restricted from performing any configurations on the screen. The menus and action buttons in the UI pages will be disabled appropriately.

Starting in software version 5.7, you can create custom user roles in addition to the default user roles in GigaVUE-FM. Access control for the default roles and the custom roles is based on the categories defined in GigaVUE-FM. These categories provide the ability to limit user access to a set of managed inventories such as ports, maps, cluster, forward list and so on.

Refer to the following table for the various categories and the associated resources. Hover your mouse over the resource categories in the Roles page to view the description of the resources in detail.

Category	Associated Resources
All	Manages all resources ▪ A user with fm_super_admin role has both read and write access to all the resource categories. ▪ A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	Manages resources such as devices, cards, ports and cloud resources. You can add or delete a device in GigaVUE-FM, enable or disable cards, modify port parameters, set leaf-spine topology. The following resources belong to this category: ▪ **Physical resources:** Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on ▪ **GigaVUE-FM inventory resources:** Nodes, node credentials ▪ **Device backup/restore:** Device and cluster configuration ▪ **Device license configuration:** Device/cluster licensing ▪ **Statistics:** Device, port ▪ **Tags**: Events, historical trending ▪ **Device security**: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings,Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers ▪ **Device maintenance**: Sys Dump, Syslog ▪ **Cloud Infrastructure resources**: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory. **NOTE:** Cloud APIs are also RBAC enabled.
Traffic Control	Manages inline resources, flow maps, GigaSMART applications,

Category	Associated Resources
Management	second level maps, map chains, map groups. The following resources belong to this category: ▪ **Infrastructure resources**: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries ▪ Intent Based Orchestration resources: Policies, rules ▪ **GigaSMART resources:** GigaSMART, GSgroups, vPorts, Netflow exporters ▪ **Map resources**: Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates ▪ **Application intelligence resources**: Application visibility, Metadata, application filter resources ▪ **Tag**: Flow manipulation - Netflow operations, Statistics - device port ▪ Active visibility ▪ **Inline resources**: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile ▪ **Cloud operation resources**: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. **NOTE:** Cloud APIs are also RBAC enabled.
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category: ▪ Backup/restore ▪ Archive server ▪ License ▪ Storage management ▪ Image repo config ▪ Notification target/email
Forward list/CUPS Management	Manages the forward list configuration. The following resources belong to this category:

Category	Associated Resources
	▪ GTP forward list ▪ SIP forward list ▪ Diameter forward list
Third Party Orchestration	Used to deploy fabric components using external orchestrator.
Device Certificate Management	Manages device certificates.
Other Resource Management	Manages virtual and cloud resources

You can associate the custom user roles either to a single category or to a combination of categories based on which the users will have access to the resources. For example, you can create a 'Physical Devices Technician' role such that the user associated with this role can only access the resources that are part of the **Physical Device Infrastructure Management**.

NOTE: A user with **fm_admin** role has both read and write access to all of the categories, but has read only access to the FM Security Management category.

To create a role:

1. On the left navigation pane, click  and select **Authentication > User Management > Roles**.
2. Click **Create**. In the Wizard that appears, perform the following steps. Click **Continue** to progress forward and click **Back** to navigate backward and change details.

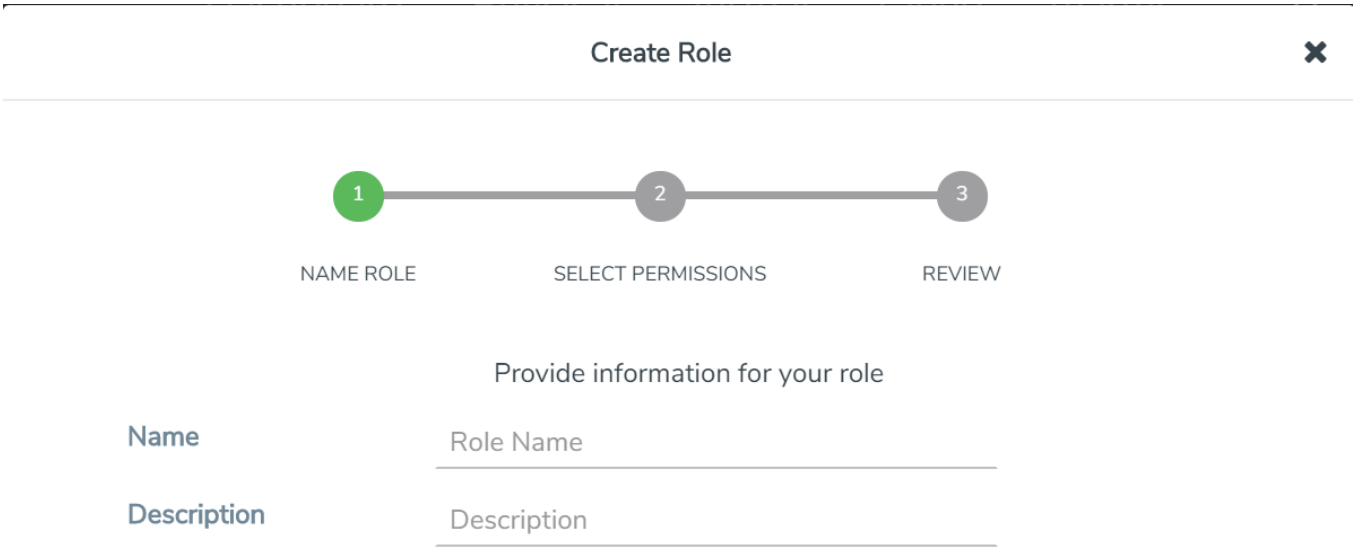


Figure 3 *Create Roles*

a. In the **Name Role** tab enter the following:

- **Name:** Name of the role.
- **Description:** Description for the role.

b. In the **Select Permissions** tab:

- Select the required resources. Hover your mouse over the resource category to get a glimpse of the resource.
- Select the required read and write permissions for the resources selected.

c. In the **Review** tab, review the role created. Click **Save** to create the role.

The new role is added to the summary list view.

The following tables describes how access control is applied to a user who has the required role to access the resources based on:

- RBAC settings in the device
- RBAC mode selected in GigaVUE-FM

Table 1: Access control for a user who has the required role in GigaVUE-FM to access the resources.

RBAC Settings on the Managed Devices	RBAC Mode in GigaVUE-FM	Access control
Allows user to access its resource	Device RBAC	Allow user to access GigaVUE-FM resources
		Allow user to access managed device resources
	GigaVUE-FM RBAC (node credentials has admin privileges)	Allow user to access GigaVUE-FM resources
		Allow user to access managed device resources
Disallows user to access its resource	Device RBAC	Allow user to access GigaVUE-FM resources
		Disallow user to access managed device resources
	GigaVUE-FM RBAC (Node credential has admin privileges)	Allow user to access GigaVUE-FM resources
		Allow user to access managed device resources

Refer to the following notes:

- For users who do not have the necessary role to access the resources, the access controls mentioned above are disallowed irrespective of the RBAC settings on the managed devices and the RBAC mode in GigaVUE-FM.
- For users authenticated using the remote authentication servers such as LDAP or TACACS+, user groups will be assigned to the user based on the mapped-user group configuration. Refer to Authentication for more details about role-mapping in LDAP and TACACS+ based authentication.

Create User Groups

You can use the user group option to associate the users with Roles and Tags. 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 user groups.

Create User Groups

Starting in software version 5.8.00, you can use the user group option to associate the users with Roles and Tags. 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 user groups.

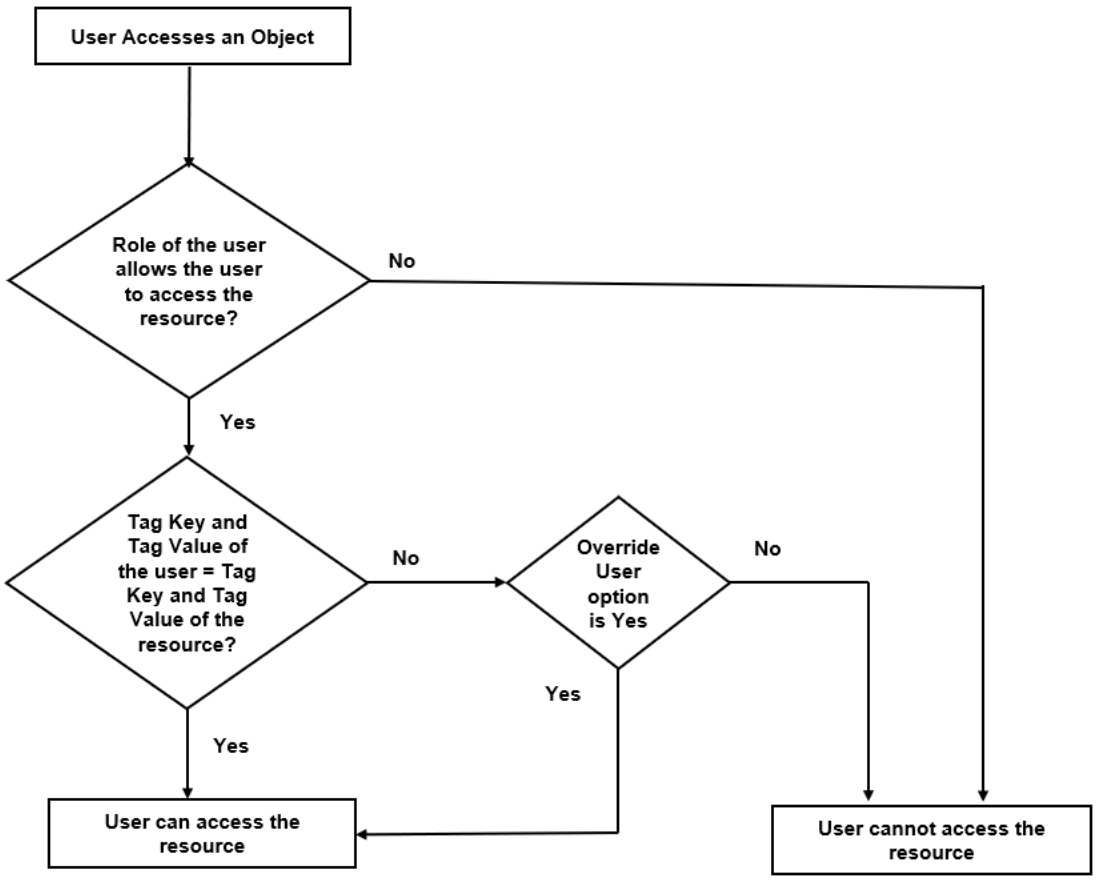
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

User Group	Tag Key and Tag Value	Permission
Super Admin Group	Tag Key = All Tag Value = All	Group with privileges of fm_super_ adminrole.
Admin Group	Tag Key= All Tag Value = All	Group with privileges of fm_admin role.
View only user	Tag Key = All Tag Value = All	Group with privileges of fm_user role.

By creating groups and associating to tags and roles, you can control the users of the following:

- The category of resources which the user can access, such as the clusters, ports, maps and so on. This is defined using the **Roles** option. Refer to the Roles section for more details.
- The physical and logical resources that the user can access, such as the ports in a cluster that belong to a specific department in a location. This is defined using the **Tags** option.

Refer to the following flow chart to see how access control operation occurs when the user accesses a resource:



To create a group:

1. On the left navigation pane, click , and then select **Authentication > User Management > User Groups**.
2. Click **Create**. In the Wizard that appears, perform the following steps. Click **Continue** to progress forward and click **Back** to navigate backward and change details.

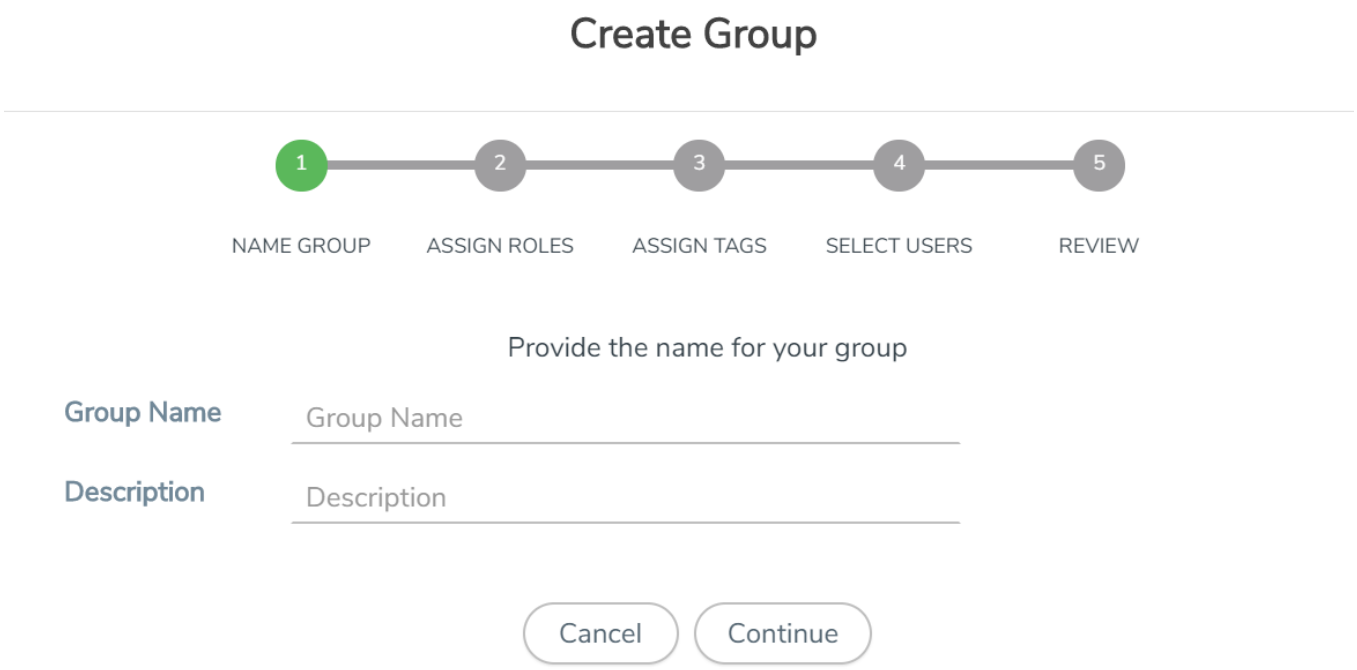


Figure 4 *Create Group*

a. In the **Name Group** tab enter the following:

- **Group Name:** Name of the group.
- **Description:** Description for the group.

b. In the **Assign Roles** tab, select the required role.

c. In the **Assign Tags** tab, select the required tags Id and tag value. Only access control tags will be available for selection.

NOTE: Select the **Override User** option to allow the user to access the resources for which the tag key of the resource does not match the tag key of the user.

d. Select the required users (this step is optional).

e. In the **Review** tab, review the group created. Click **Save** to create the group.

The new group is added to the summary list view. Click on the ellipses to perform the following operations:

- **View Details:** View the details of the group such as the Group Name, Description, Role associated to the group, Tag associated to the group.
- **Assign Users:** Assign groups to users if this step was skipped at the time of creating the group.
- **Remove Users**: Remove existing users from the group.
- **Edit:** Edit an existing group.
- **Delete:** Delete an existing user.

Configure GigaVUE Fabric Components in AWS

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

Keep in mind the following when deploying the fabric components using third party orchestration in integrated mode:

- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- When using VPC mirroring as the traffic acquistion method, add a tag with key **GigamonNode** and value **VSeriesNode** to the V Series Node or Proxy created on the platform.
- You can use AWS as an Orchestrator for deploying GigaVUE fabric components only when using V Series 2 nodes.

In your AWS EC2, you can configure the following GigaVUE fabric components:

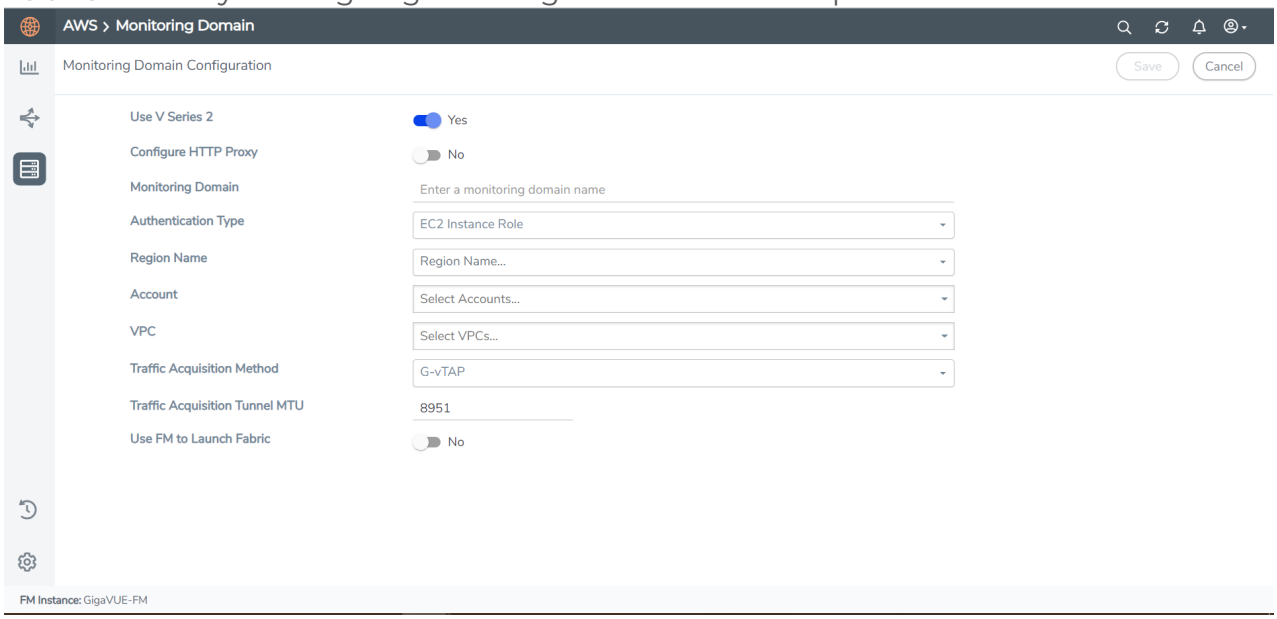
- Configure GigaVUE V Series Nodes and V Series Proxy in AWS
- Configure G-vTAP Controller in AWS
- Configure G-vTAP Agent in AWS

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

To configure GigaVUE V Series Nodes and V Series Proxy in AWS platform:

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

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



3. In your AWS environment, you can deploy GigaVUE V Series Nodes or V Series proxy using the following methods:
   - Register GigaVUE V Series Nodes or Proxy using User Data
   - RegisterGigaVUE V SeriesProxy using a configuration file

Register GigaVUE V Series Nodes or Proxy using User Data

To register GigaVUE V Series Nodes or proxy using the user data in AWS GUI:

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM

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

- You can register yourGigaVUE V Series directly with GigaVUE-FM or you can use V Series proxy to register yourGigaVUE V Series with GigaVUE-FM. If you wish to registerGigaVUE V Series directly, enter the `remotePort` value as 443 or if you wish to deployGigaVUE V Series using V Series proxy then, enter the `remotePort` value as 8891.
- User and Password must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

RegisterGigaVUE V SeriesProxy using a configuration file

To registerGigaVUE V SeriesProxy using a configuration file:

1. Log in to theGigaVUE V SeriesProxy.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

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

3. Restart theGigaVUE V Seriesproxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps restart
     ```

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

Configure G-vTAP Controller in AWS

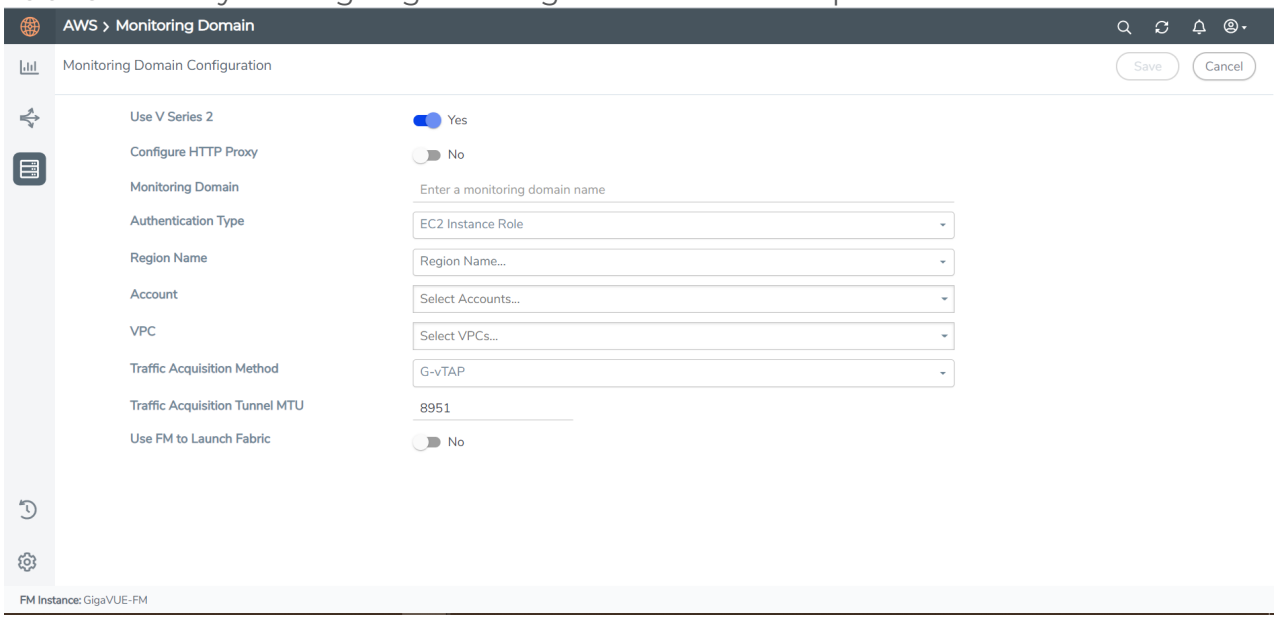
You can configure more than one G-vTAP Controller in a monitoring domain.

To configure G-vTAP Controller in AWS platform:

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

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

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

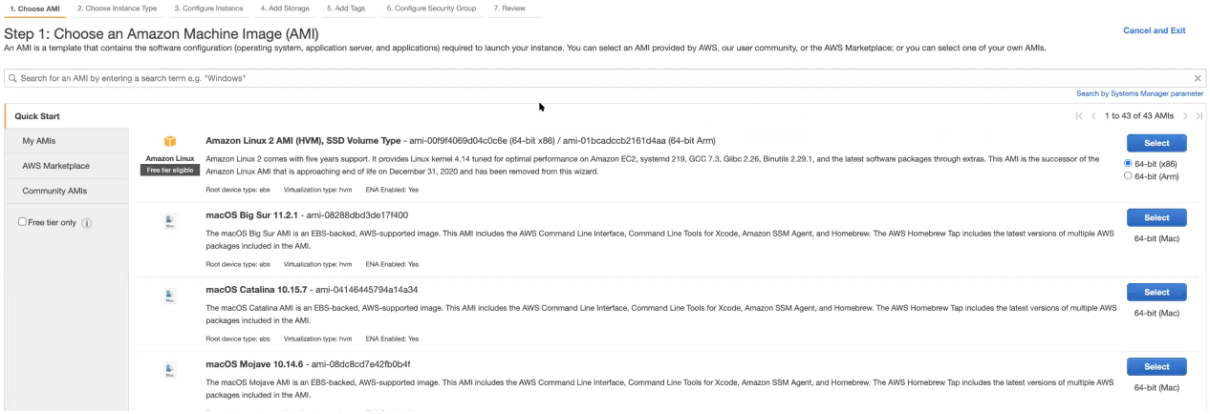


3. In your AWS environment, launch the G-vTAP Controller AMI instance using any of the following methods:
   - Register G-vTAP Controller using User Data
   - Register G-vTAP Controller using a configuration file

Register G-vTAP Controller using User Data

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

a. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.



b. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The G-vTAP Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

> - User and Password must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

The G-vTAP Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Monitoring Domain	Connection	Fabric	Management IP	Fabric Version	Status
MD1					
	[redacted]vpc				Connected
		G-vTapController	[redacted]	1.7-304	Ok
		Gigamon-VSeriesProxy-1	[redacted]	2.1.0	Ok
		Gigamon-VSeriesNode-1	[redacted]	2.2.0	Ok

Register G-vTAP Controller using a configuration file

To register G-vTAP Controller using a configuration file:

a. Log in to the G-vTAP Controller.

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

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

c. Restart the G-vTAP Controller service.

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

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

Configure G-vTAP Agent in AWS

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

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

To register G-vTAP Agent using a configuration file:

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

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

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the G-vTAP Controller 1>,
                  <IP address of the G-vTAP Controller 2>
        remotePort: 8891
```

   - User and Password must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

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

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

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

Keep in mind the following when upgrading the GigaVUE-FM to 6.1.00 (when using third party orchestration to deploy fabric components):

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM

with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure that there is no existing user in GigaVUE-FM, with the username **orchestration**.

It is recommended to change the password in the Users page, once the upgrade is complete. Refer to Configure Role-Based Access for Third Party Orchestration for detailed steps on how to change password in the user page.

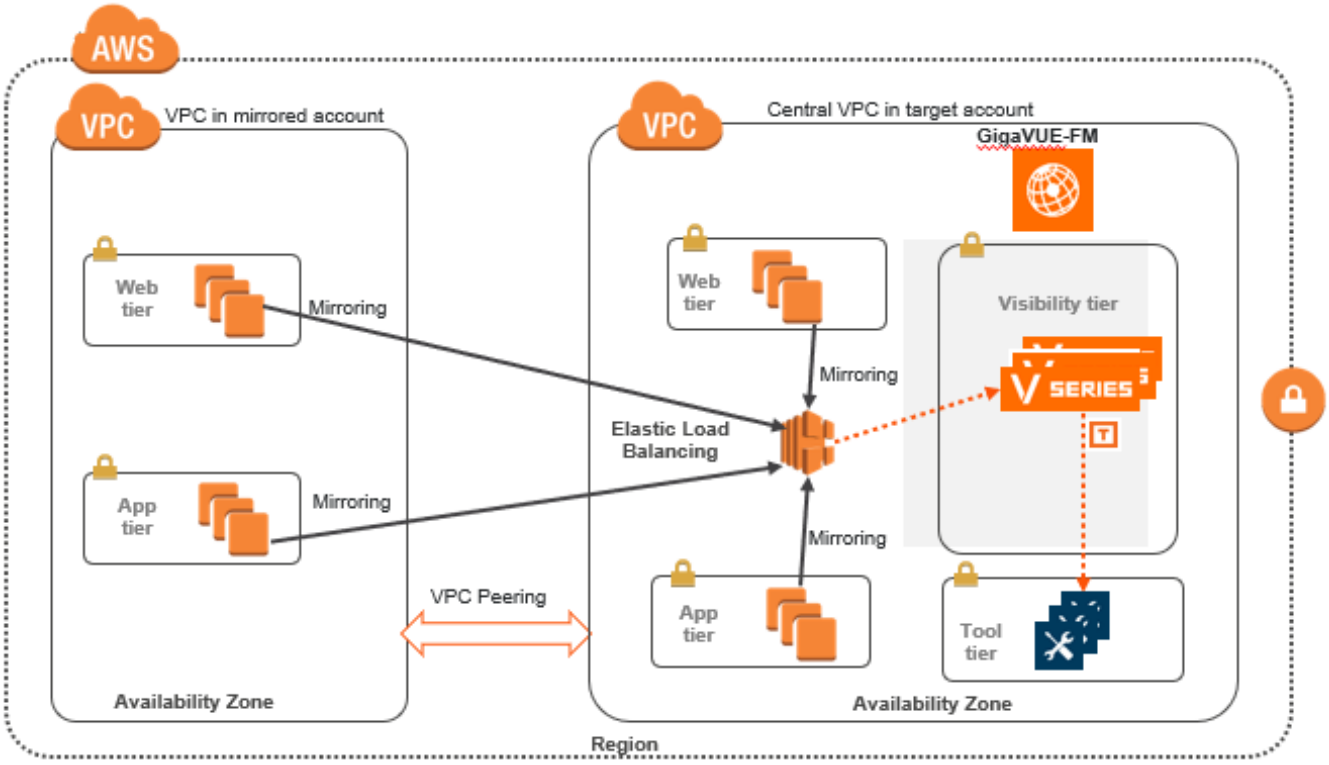
Configure an External Load Balancer on GigaVUE Cloud Suite for AWS

You can use your own load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series 2 nodes. The load balancer distributes the traffic to the GigaVUE V Series 2 nodes and the GigaVUE-FM auto-scales the GigaVUE V Series Nodes based on the traffic. GigaVUE-FM creates a traffic mirror from the target VMs to the load balancer that all the targets must have the same traffic load balancer destination. Load balancer forwards the traffic to the GigaVUE V Series 2 nodes and the AWS Auto Scaling group monitors the load of all GigaVUE V Series nodes. AWS Auto Scaling group can add or remove nodes if the traffic load is heavy or low.

Refer to the following topics for detailed information.

- Architecture
- Prerequisites
- Configure an External Load Balancer in AWS
- Deploy GigaVUE V Series Solution with Elastic Load Balancing

Architecture



The design depicts deploying GigaVUE Cloud Suite fabric components in a centralized VPC where the target VMs of mutiple 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. The load balancer deploys or deletes additional GigaVUE V Series 2 nodes and distributes the traffic among them to aggregate, filter, and forward the traffic to the tools over the tunnel endpoint. In AWS, the Auto Scaling group monitors the load among all the GigaVUE V Series 2 nodes and adds or removes them via RESTful API integration with the GigaVUE-FM when the traffic load crosses or drops below a pre-defined threshold.

A typical AWS deployment to support the external load balancer requires the following components:

- GigaVUE-FM (Fabric Manager
- GigaVUE V Series 2 node
- AWS Network Load Balancer (uniformly distributes traffic from AWS target VMs to GigaVUE V Series nodes)

Prerequisites

- Create or update Security Group polices of GigaVUE Cloud Suite components. Refer to Security Group topic for detailed information.
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Network Load Balancer is deployed. Refer to Amazon VPC for more information.

  NOTE: The target account VPC is considered as the centralized VPC by GigaVUE-FM and the connections towards all other mirrored account VPCs either through 1 : 1 VPC peering or via 1 : M transit gateway (that connects all participating VPCs across mirrored AWS accounts). VPC peering has no bandwidth limitation and no additional cost within the same region (recommended). Transit gateway costs more and it also has a limitation of 50 Gbps burst per VPC.

- Create or update existing IAM role for GigaVUE-FM in the centralized VPC. Additionally trust relationship needs to be created between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. Refer to AMI and Permissions section for detailed information.

Configure an External Load Balancer in AWS

To configure an external load balancer in AWS:

1. In the **Target Groups** page, click **Create target group** and the Create target group wizard appears. Enter or select the following values and create the target group.
   a. Select **IP addresses** as the target type.
   b. Enter a name for the target group.
   c. Select the **UDP** as the Protocol and **4789** as the port number.
   d. Select the VPC of your target group where the targets are registered.
   e. Select **TCP** as the Health check protocol in port number **8889** with **10 seconds** health check interval.

   NOTE: For detailed instructions, refer to Create a target group for your Network Load Balancer topic in the AWS Elastic Load Balancing document.

2. Navigate to the **Load Balancer** page and click **Create Load Balancer** the Create elastic load balancer wizard appears. Enter or select the following values and create the load balancer.
   a. Select **Network Load Balancer** as the load balancer type and click **Create**.
   b. Enter a name for the Network Load Balancer.
   c. Select **Internal** load balancer as the Scheme.
   d. Select the **VPC** for your targets (GigaVUE V Series Nodes).
   e. Select the regions/zones and the corresponding subnets.
   f. Select **UDP** as the Listener Protocol with Port number **4789**.

   NOTE: For detailed instructions, refer to Create a Network Load Balancer topic in the AWS Elastic Load Balancing document.

3. Navigate to the **Launch Templates** page and click **Create launch template** the Create launch template wizard appears. Enter or select the following values and create the launch template.
   a. Enter a name for the launch template.
   b. Select the AMI of the GigaVUE V Series node.
   c. Select **t3a.xlarge** as the instance type.
   d. Select a Key pair for the instance.
   e. Select **VPC** as the Networking platform and don't specify the security group.
   f. Add 2 Network Interfaces for the GigaVUE V Series node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces, select the appropriate security group.

   NOTE: For detailed instructions, refer to Creating a launch template for an Auto Scaling group topic in the AWS EC2 Auto Scaling document.

4. Navigate to the **Auto Scaling groups** page, and click **Create an Auto Scaling group** the Create Auto Scaling group wizard appears. Enter or select the following values and create the Auto Scaling group.
   a. Enter a name for the Auto Scaling group.
   b. Select an existing launch template.
   c. Select the VPC and subnet.
   d. In the Group size section, enter the value for minimum and maximum capacity.
   e. In the Scaling policies section, select **Target tracking scaling policy** and choose Average network in (bytes) for the Metric type with **1000000000 (bytes)** as target value and **300** seconds warm up value.
   f. (optional) Add **Tags** to the instances.

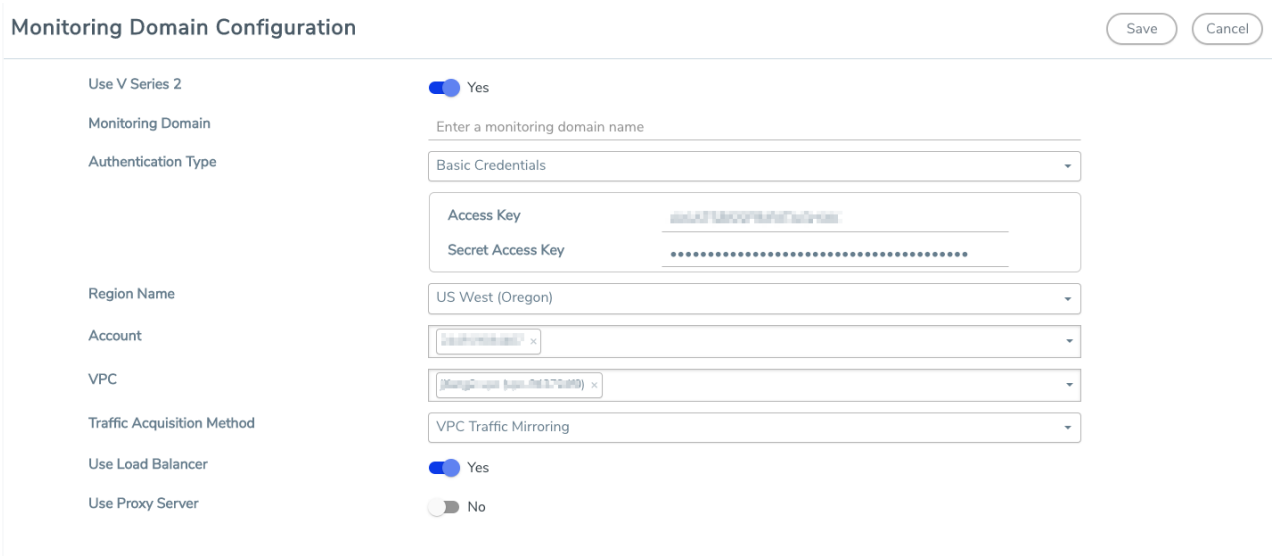
   NOTE: For detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in the AWS EC2 Auto Scaling document.

In the Instances page, you can view the GigaVUE V Series 2 node instance deployed by the load balancer and use the same

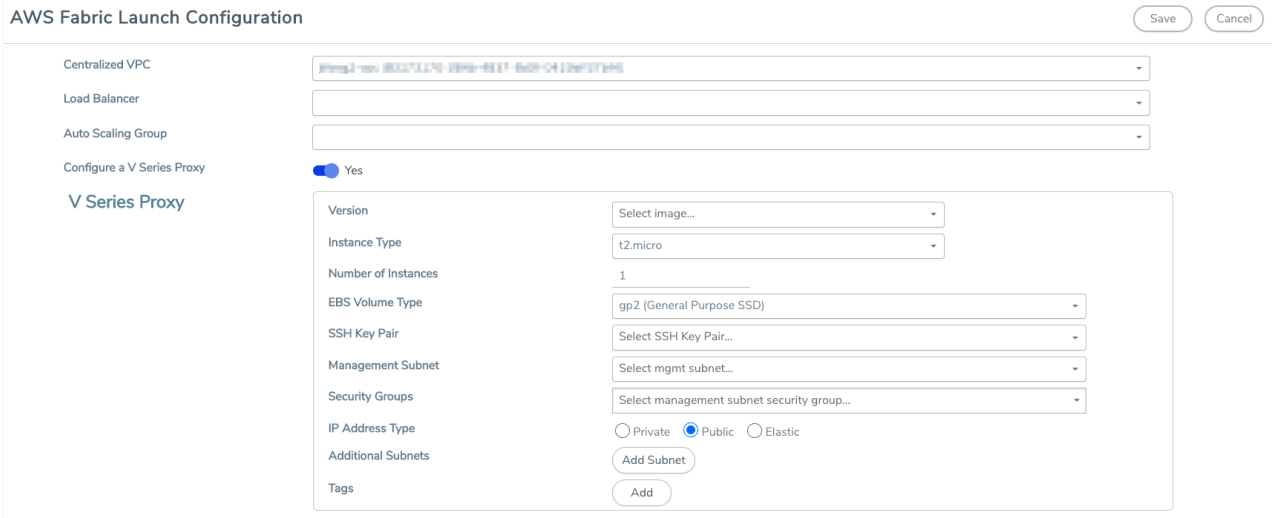
Deploy GigaVUE V Series Solution with Elastic Load Balancing

To deploy GigaVUE V Series solution across the AWS accounts with Elastic Load Balancing in GigaVUE-FM:

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** as the Traffic Acquisition method. Refer to Create a Monitoring Domain for detailed information.



2. For the **Use Load Balancer** field, select **Yes**.
3. Click **Save** and the AWS Fabric Launch Configuration page appears.



4. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
   - Select the Load Balancer configured in AWS
   - Select the Auto Scaling Group configured in AWS

   For the remaining field description, refer to Configure GigaVUE Fabric Components in GigaVUE-FM.
5. Click **Save** to save the configuration.

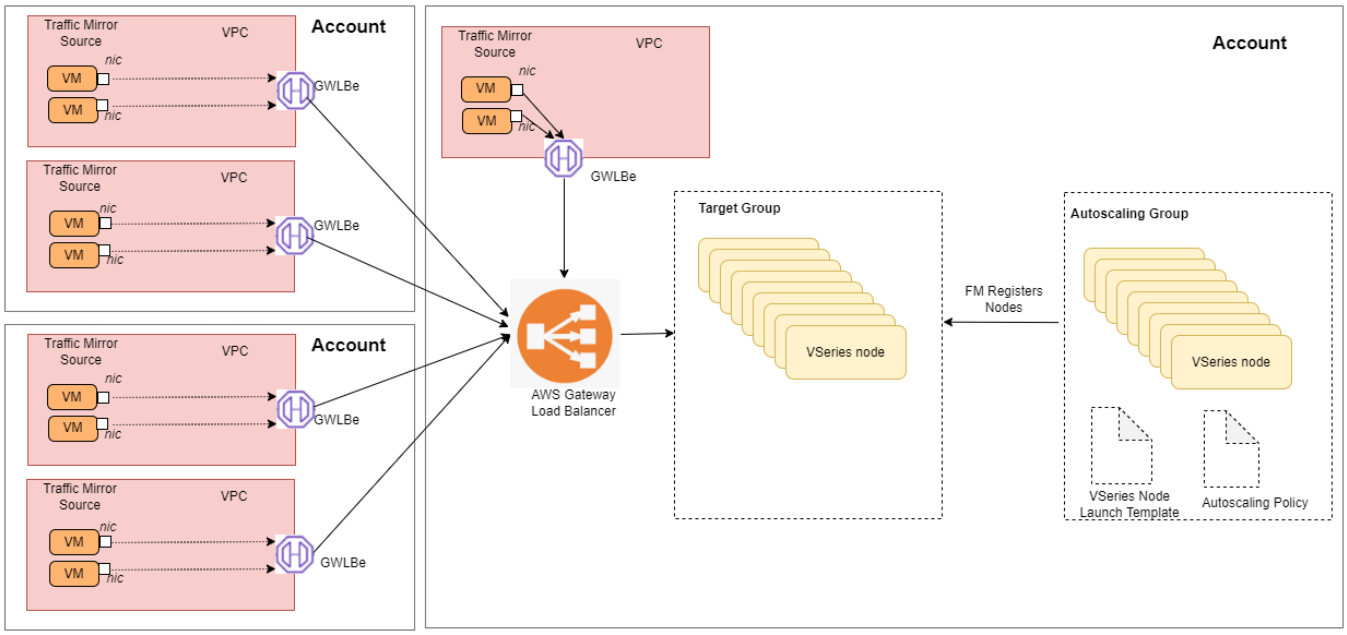
Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS

The gateway load balancer (GWLB) uses the gateway load balancer end points to distribute the traffic across the end points. It is a VPC endpoint that provides connectivity in between virtual machines. With GWLB Endpoint as a target, mirrored traffic can be forwarded from any subnet. You can monitor network traffic across multiple VPCs and accounts, with centralized traffic inspection in a single VPC across their entire organization.

Refer to the following topics for detailed information.

- Architecture
- Prerequisites
- Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS
- Deploy GigaVUE V Series Solution with Gateway Load Balancer

Architecture



In the architecture, you can see the deployment of GigaVUE Cloud Suite for AWS environments that have GWLB implementation for the security appliances, such as firewalls. In such deployments, the applications and your appliances are in different VPCs. The workload VPC is configured with the Gateway load balancer endpoint while the service VPC is configured with the Gateway load balancer. Gigamon deployed VPC has the solution components, such as GigaVUE FM, V Series Nodes, and the OOB tools which consume the mirrored and decapsulated data.

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. Refer to Security Group topic for detailed information.
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Gateway Load Balancer is deployed. Refer to Amazon VPC for more information.
- Create or update existing IAM role for GigaVUE-FM in the centralized VPC. Additionally trust relationship needs to be created between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. Refer to AMI and Permissions section for detailed information.

- For more information on AWS recommended design for Gateway Load Balancer implementation with inline services, such as firewall. see Getting started with Gateway Load Balancers - Elastic Load Balancing (amazon.com)
- You must create a VPC endpoint and endpoint service. For more information, see Create endpoint service
- Create a routing table. For more information, see Amazon documentation.

Configure a Gateway Load Balancer in AWS

To configure an external load balancer in AWS:

1. In the **Target Groups** page, click **Create target group** and the Create target group wizard appears. Enter or select the following values and create the target group.
   a. Select **IP addresses** as the target type.
   b. Enter a name for the target group..
   c. Select the VPC of your target group where the targets are registered.
   d. Select **TCP** as the Health check protocol in port number **8889** with **10 seconds** health check interval.

   NOTE: You must select GENEVE protocol and port 6081 while creating the targets groups. For detailed instructions, refer to Target groups for your Gateway Load Balancers.

2. Navigate to the **Load Balancer** page and click **Create Load Balancer** the Create elastic load balancer wizard appears. Enter or select the following values and create the load balancer.
   a. Select **Gateway Load Balancer** as the load balancer type and click **Create**.
   b. Enter a name for the Gateway Load Balancer.
   c. Select the **VPC** for your targets (GigaVUE V Series Nodes).
   d. Select the regions/zones and the corresponding subnets.
   e. Associate the load balancer to the target group.
   f. By default, **GENEVE** as the Listener Protocol with Port number **6081** is selected.

   NOTE: For detailed instructions, refer to Create a Gateway Load Balancer topic in the AWS Elastic Load Balancing document

3. Navigate to the **Launch Templates** page and click **Create launch template** the Create launch template wizard appears. Enter or select the following values and create the launch template.
   a. Enter a name for the launch template.
   b. Select the AMI of the GigaVUE V Series node.
   c. Select **c5n.xlarge** as the instance type.
   d. Select a Key pair for the instance.
   e. Select **VPC** as the Networking platform and don't specify the security group.
   f. Add 2 Network Interfaces for the GigaVUE V Series node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces, select the appropriate security group.

   NOTE: For detailed instructions, refer to Creating a launch template for an Auto Scaling group topic in the AWS EC2 Auto Scaling document.

4. Navigate to the **Auto Scaling groups** page, and click **Create an Auto Scaling group** the Create Auto Scaling group wizard appears. Enter or select the following values and create the Auto Scaling group.
   a. Enter a name for the Auto Scaling group.
   b. Select an existing launch template.
   c. Select the VPC and subnet.
   d. In the Group size section, enter the value for minimum and maximum capacity.
   e. In the Scaling policies section, select **Target tracking scaling policy** and choose Average network in (bytes) for the Metric type with **1000000000 (bytes)** as target value and **300** seconds warm up value.
   f. (optional) Add **Tags** to the instances.

   NOTE: For detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in the AWS EC2 Auto Scaling document.

In the Instances page, you can view the GigaVUE V Series 2 node instance launched by the auto scaling group.

Deploy GigaVUE V Series Solution with Gateway Load Balancer

To deploy GigaVUE V Series solution across the AWS accounts with Gateway Load Balancing in GigaVUE-FM:

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** as the Traffic Acquisition method. Refer to Create a Monitoring Domain for detailed information.
2. For the **Use Load Balancer** field, select **Yes**.
3. Click **Save** and the AWS Fabric Launch Configuration page appears.

4. In the AWS Fabric Launch Configuration page, select the following for the load balancer.
   - Select the Load Balancer configured in AWS
   - Select the Auto Scaling Group configured in AWS

   For the remaining field description, refer to Configure GigaVUE Fabric Components in GigaVUE-FM.
5. Click **Save** to save the configuration.

To monitor the traffic, you must create a monitoring session. For more information on creating a monitoring session, see Configure Monitoring Session.

For more information on the best practices and architectures, see the following links:

- Getting started with Gateway Load Balancers
- Scaling network traffic inspection using AWS Gateway Load Balancer

Configure a Traffic Pre-filter

When you create a monitoring session, GigaVUE-FM creates a traffic mirror filter with a "Pass All" rule and associates it with the traffic mirroring session. The Pass All filter forwards all the traffic without filtering.

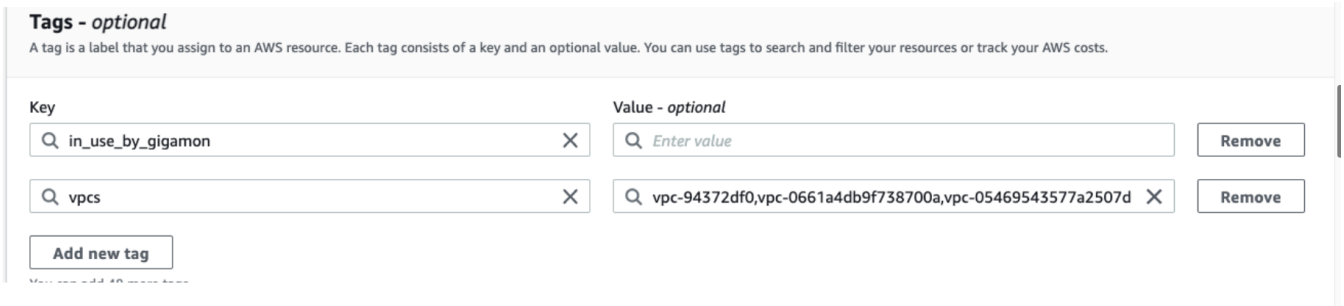
If you want to filter the traffic, then you can create a traffic mirror filter on AWS and add rules to determine the traffic that is mirrored. This traffic mirror filter acts as a pre-filter and pass only the filtered traffic to the GigaVUE V Series Nodes.

To apply the filter to the traffic mirror session that is created by the FM, you must add the tag "in_use_by_gigamon" to the traffic mirror filter. The GigaVUE-FM collects all the traffic mirror filters that has the tag "in_use_by_gigamon". It then applies these filters on the traffic mirror sessions to replace the default Pass All filter.

In addition to "in_use_by_gigamon" tag, you can add the tag "vpcs" to apply specific VPCs. The tag value is a list of vpc separated by comma ",".

You can apply filters at two levels. The two level filters can work together. The VPC level filter overrides the Account level filter for the VPC defined in VPC level filter.

1. Account level: You can define a filter (only one filter) which applies on every VPC in an account. The filter should be tagged with "in_use_by_gigamon" only. The "vpcs" tag should not be used.
2. VPC level: To filter the traffic at VPC level, in addition to the tag "in_use_by_gigamon" , add the tag "vpcs" .



NOTE: A filter can be defined for multiple VPCs. Two filters should not have intersection on VPC. If there is an intersection on VPC, then the FM will pick a random filter and no error will be displayed.

For more information on creating a traffic mirror, refer to the AWS documentation.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes. For more detailed information about G-vTAP Agent, G-vTAP Controller, GigaVUE V Series Proxy and Node Version refer GigaVUE-FM Version Compatibility Matrix.

Refer to the following topic for more information:

- Prerequisite
- Upgrade G-vTAP Controller
- Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes, you must upgrade GigaVUE-FM to software version 5.13 or above.

Upgrade G-vTAP Controller

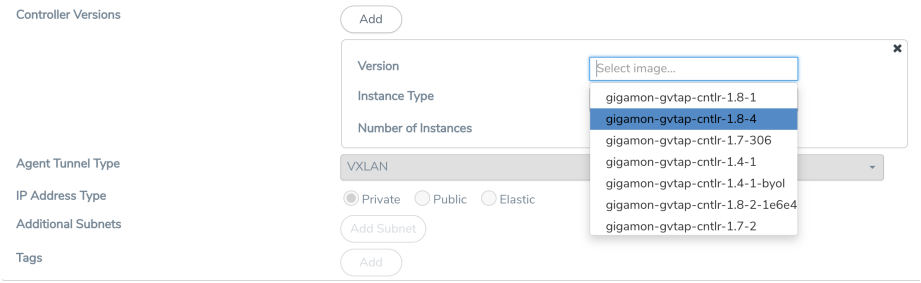
NOTE: G-vTAP Controllers cannot be upgraded. Only a new version that is compatible with the G-vTAP Agent's version can be added or removed in the **AWS Fabric Launch Configuration** page.

To change the G-vTAP Controller version follow the steps given below:

To change G-vTAP Controller version between different major versions

NOTE: You can only add G-vTAP Controllers which has different major versions. For example, you can only add G-vTAP Controller version 1.8-x if your existing version is 1.7-x.

a. Under **Controller Versions**, click **Add**.
b. 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.
c. From the **Instance Type** drop-down list, select a size for the G-vTAP Controller.
d. In **Number of Instances**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.



You cannot change the IP Address Type and the Additional Subnets details, provided at the time of G-vTAP Controller configuration.

After installing the new version of G-vTAP Controller, follow the steps given below:

1. Install G-vTAP Agent with the version same as the G-vTAP Controller.
2. Delete the G-vTAP Controller with older version.

To change G-vTAP Controller version with in the same major version

This is only applicable if you wish to change your G-vTAP Controller version from one minor version to another within the same major version. For example, from 1.8-2 to 1.8-3.

a. From the **Version** drop-down list, select a G-vTAP Controller image with in the same major version.
b. Specify the **Number of Instances**. The minimum number you can specify is 1.
c. Select the **Subnet** from the drop-down.

- You cannot modify the rest of the fields.
- After installing the new version of G-vTAP Controller, install the G-vTAP Agent with the same version.

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes at a time.

There are two ways to upgrade the GigaVUE V Series Proxy and Nodes. You can:

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

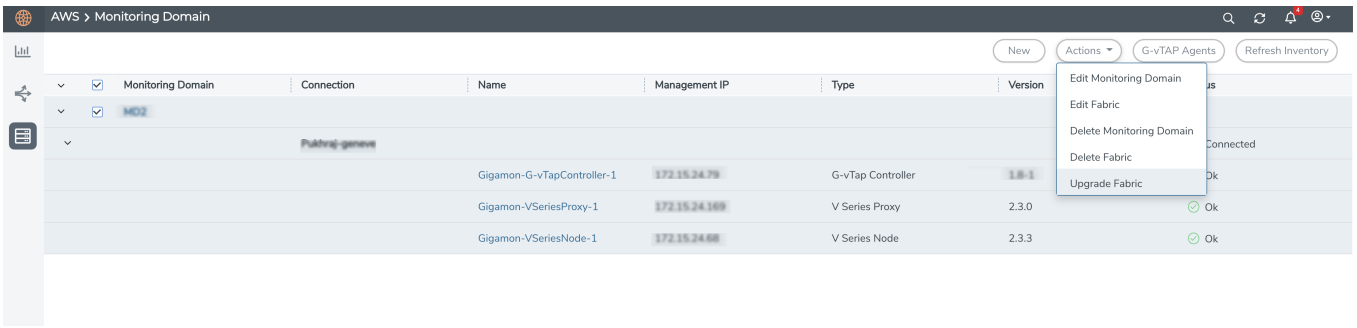
  For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and Nodes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

  NOTES:
  - When the new version of nodes and proxy are launched, the old version is not deleted by GigaVUE-FM until the new version of node and proxy is launched and the status is changed to **Ok**. Make sure that the instance type of the node and proxy selected during the configuration can accommodate the total number of new and old fabric nodes present in the VPC. If the instance type cannot support so many Virtual Machines, you can choose to upgrade the fabric nodes in multiple batches.
  - If there is an error while upgrading the complete set of proxy and nodes present in the VPC, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
  - Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of free addresses are available in the respective subnets. Otherwise, the upgrade will fail.
- Launch and replace the nodes and proxy in multiple batches.

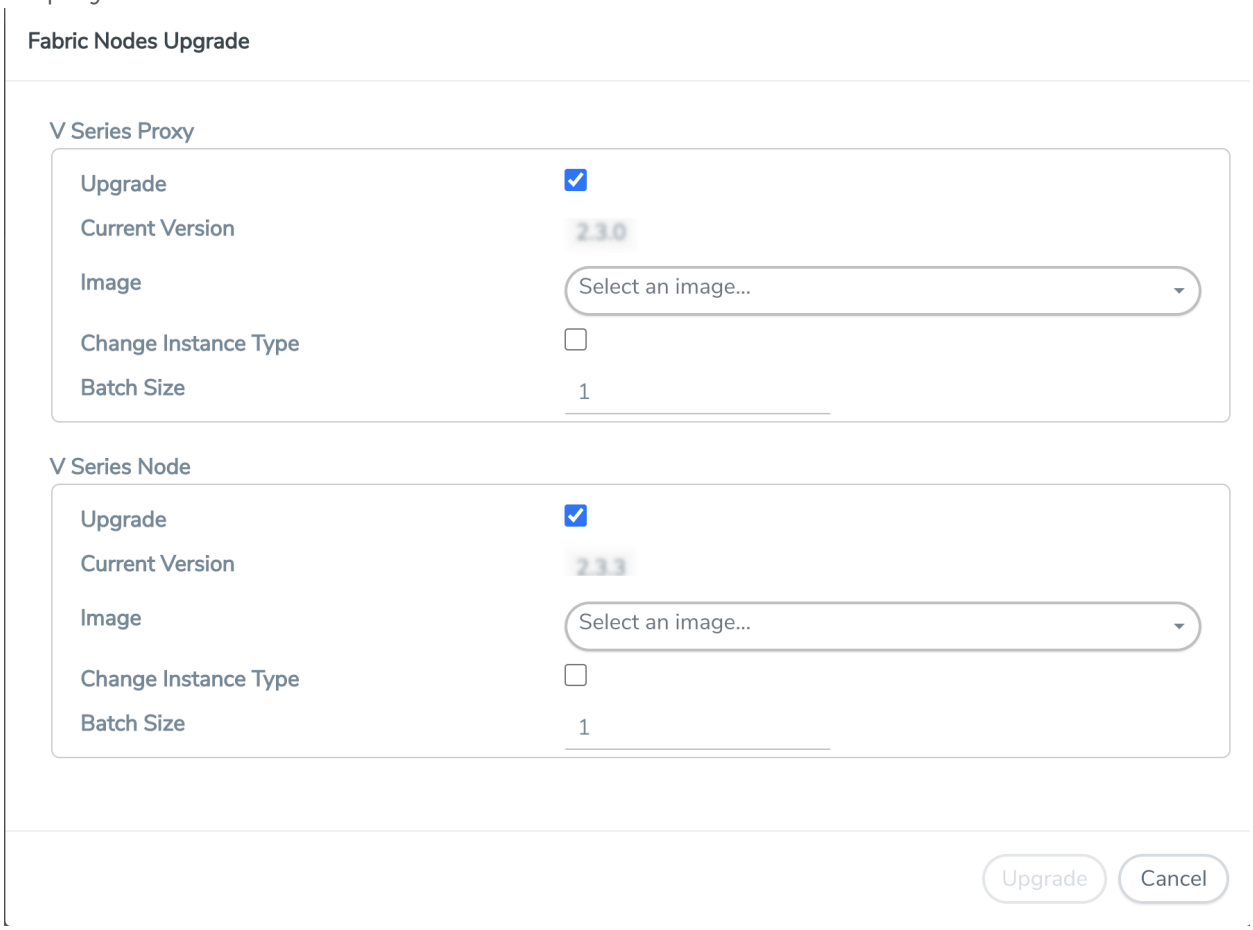
  For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

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

1. Go to **Inventory > VIRTUAL > AWS** , and then click **Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The Fabric Nodes Upgrade page is displayed.



4. To upgrade the GigaVUE V Series Nodes/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy/Nodes.
6. Select the **Change Instance Type** checkbox to change the instance type of the nodes/proxy, only if required.
7. To upgrade the GigaVUE V Series Nodes/Proxy, specify the batch size in the **Batch Size** box.

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

The upgrade process takes a while depending on the number of GigaVUE V Series Proxy and Nodes upgrading in your AWS environment. First, the new version of the GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. In the V Series Proxy page, click the link under Progress to view the upgrade status.

Once the nodes are upgraded successfully, the monitoring session is re-deployed automatically.

Configure Monitoring Session

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

Refer to the following sections for details:

Create a Monitoring Session

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.

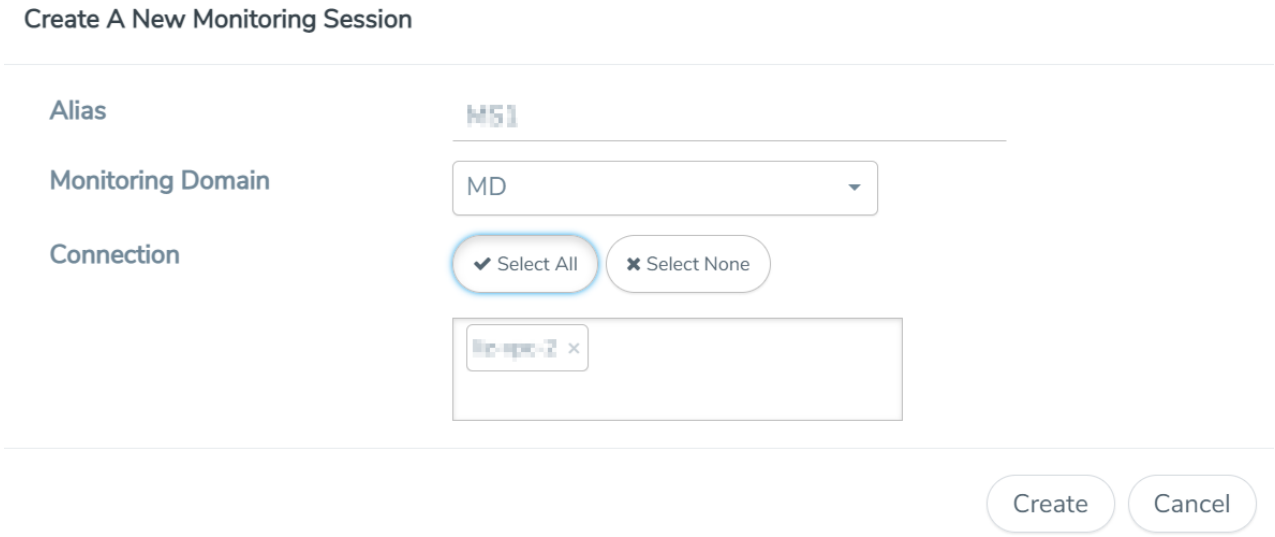
For the connections without G-vTAPs there is no targets that are automatically selected. You can use Customer Orchestrated Source in the monitoring session to accept a tunnel from anywhere.

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.

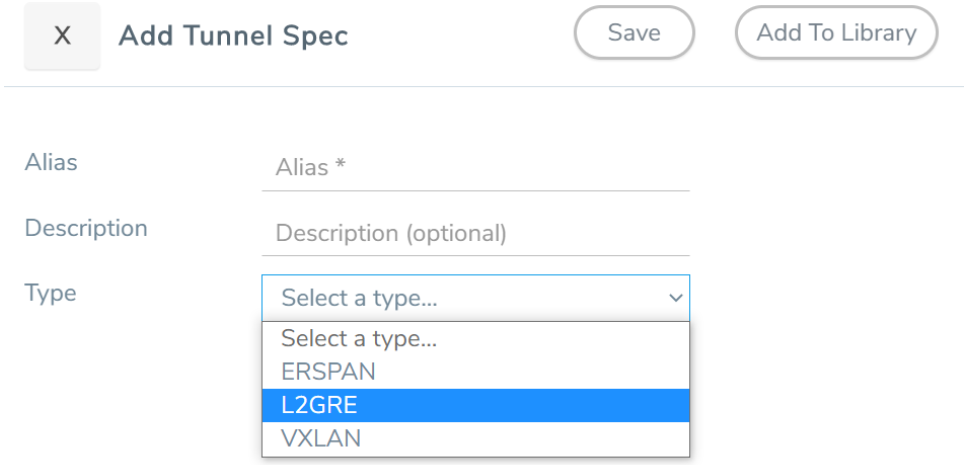
Create Ingress and Egress Tunnels

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

NOTE: ERSPAN is not supported for AWS solution.

To create a new tunnel endpoint:

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



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

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

4. Click **Save**.

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

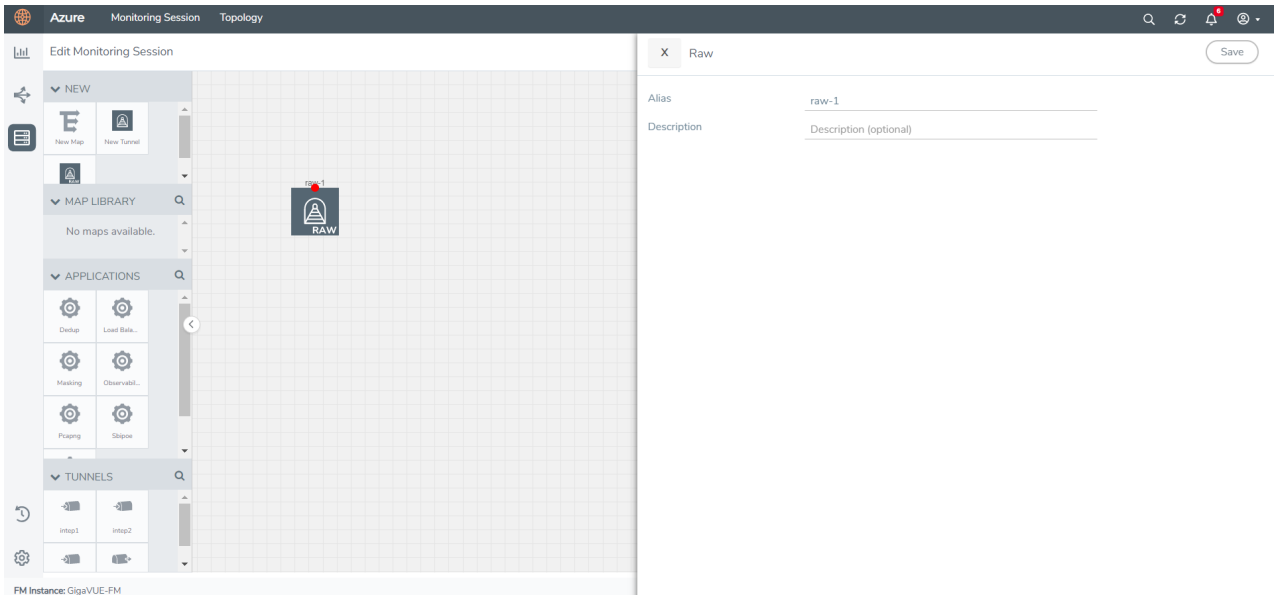
After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

Create Raw Endpoint

Raw End Point (REP) is used to pass traffic from an interface. You can optionally use this end point to send traffic to the applications deployed in the monitoring session.

To add Raw Endpoint to the monitoring session:

1. Drag and drop **New RAW** from **NEW** to the graphical workspace.
2. Click the **New RAW** icon and select **Details**. The **RAW** quick view page appears.
3. Enter the alias and description. In the **Alias** field, enter a name for the Raw End Point and click **Save**.



4. To deploy the monitoring session after adding the Raw Endpoint click the **Deploy** button in the edit monitoring session page.
5. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the V Series Nodes for which you wish to deploy the monitoring session.
6. After selecting the V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual V Series Nodes. Then, click **Deploy**.

Create a New Map

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

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

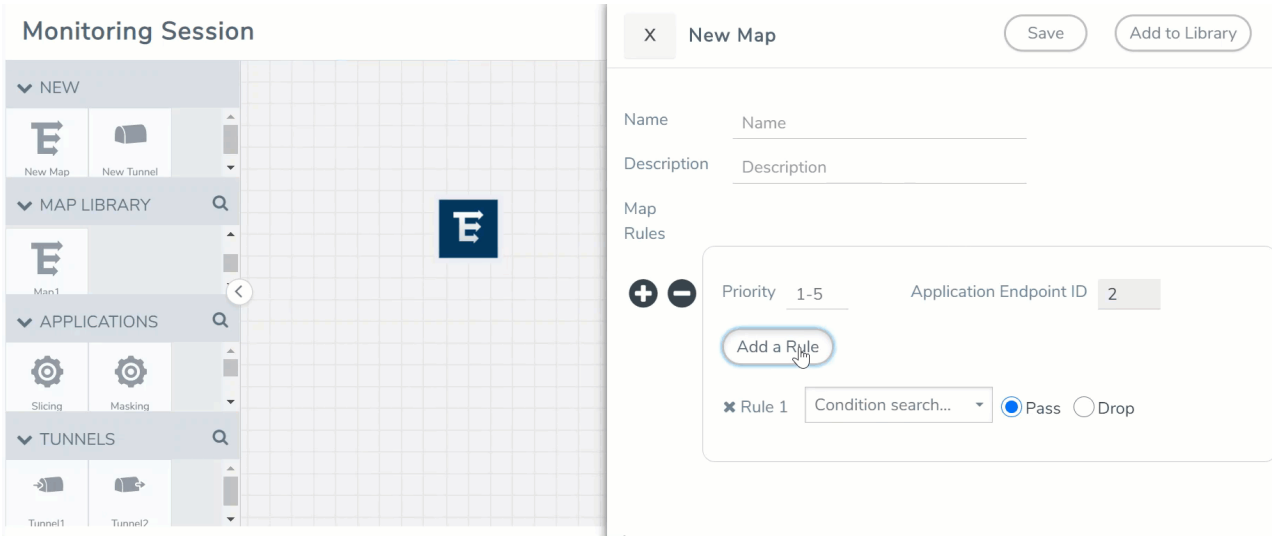
A map is used to filter the traffic flowing through the GigaVUE V Series Nodes. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.

Keep in mind the following when creating a map:

Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.
Priority	A priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
Pass	The traffic from the virtual machine will be passed to the destination.
Drop	The traffic from the virtual machine is dropped when passing through the map.
Traffic Filter Maps	A set of maps that are used to match traffic and perform various actions on the matched traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the monitoring session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps**
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

To create a new map:

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



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

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

Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
- Traffic Map—Only Pass rules for ATS
- Inclusion Map—Only Pass rules for ATS
- Exclusion Map—Only Drop rules for ATS

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

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

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

Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a windows agent.

You can also perform the following action in the Monitoring session canvas.

- Click a map and select **Details** to edit the map or select **Delete** to delete the map.
- Click the **Show Targets** button to view the monitoring targets highlighted in orange.
- Click  to expand the **Targets** dialog box. Click  to change the view from the list view to topology view. To view details about a GigaVUE V Series Node, click the arrow next to the VM.
- In the Instances window, click  to filter the list of instances.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a monitoring session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. Enter the name as Map 1 and enter the description. Enter the priority and Application Endpoint ID.
3. Select the condition as VM Name and enter the **target**. This includes the instances, target-1-1, target-1-2, target-1-3, target-2-1, and target-2-2.
4. Click on the Expand icon on the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps sections appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description for the map.
   a. Enter the name as Inclusionmap1 and enter the description. Enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1**. Then the instance with VM name **target-1-1, target-1-2,** and **target-1-3** will be included.

6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in above section.
   a. Enter the name as Exclusionmap1 and enter the description. Enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then the instance **target-1-3** will be excluded.

   Based on this configuration, the Automatic Target Selection will select the instances target-1-1 and target-1-2 as target.

Add Applications to Monitoring Session

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

- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Application Metadata Exporter

For more detailed information on how to configure these application, refer to *GigaVUE V Series Applications Guide*.

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

- Application Metadata Intelligence
- Application Filtering Intelligence

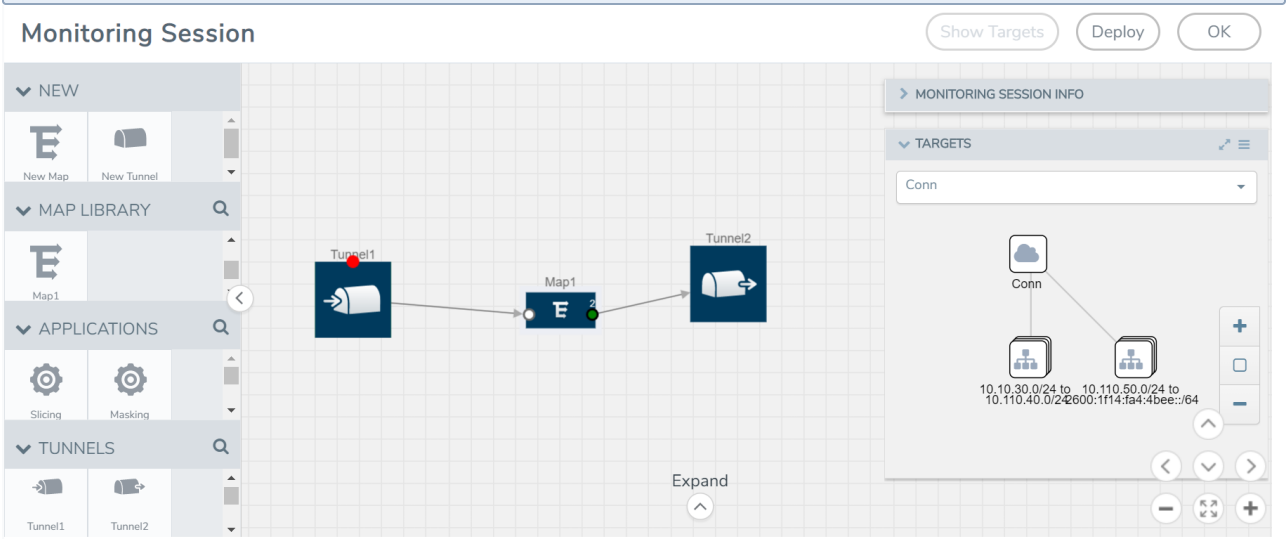
For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop the following items to the canvas as required:
   - Ingress tunnel (as a source) from the **NEW** section
   - Maps from the **MAP LIBRARY** section
   - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART apps from the **APPLICATIONS** section
   - Egress tunnels from the **TUNNELS** section
2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

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



3. (Not applicable for Tunnel traffic acquisition method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.
4. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.

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

The Monitoring Session page also has the following options under the **Actions** button:

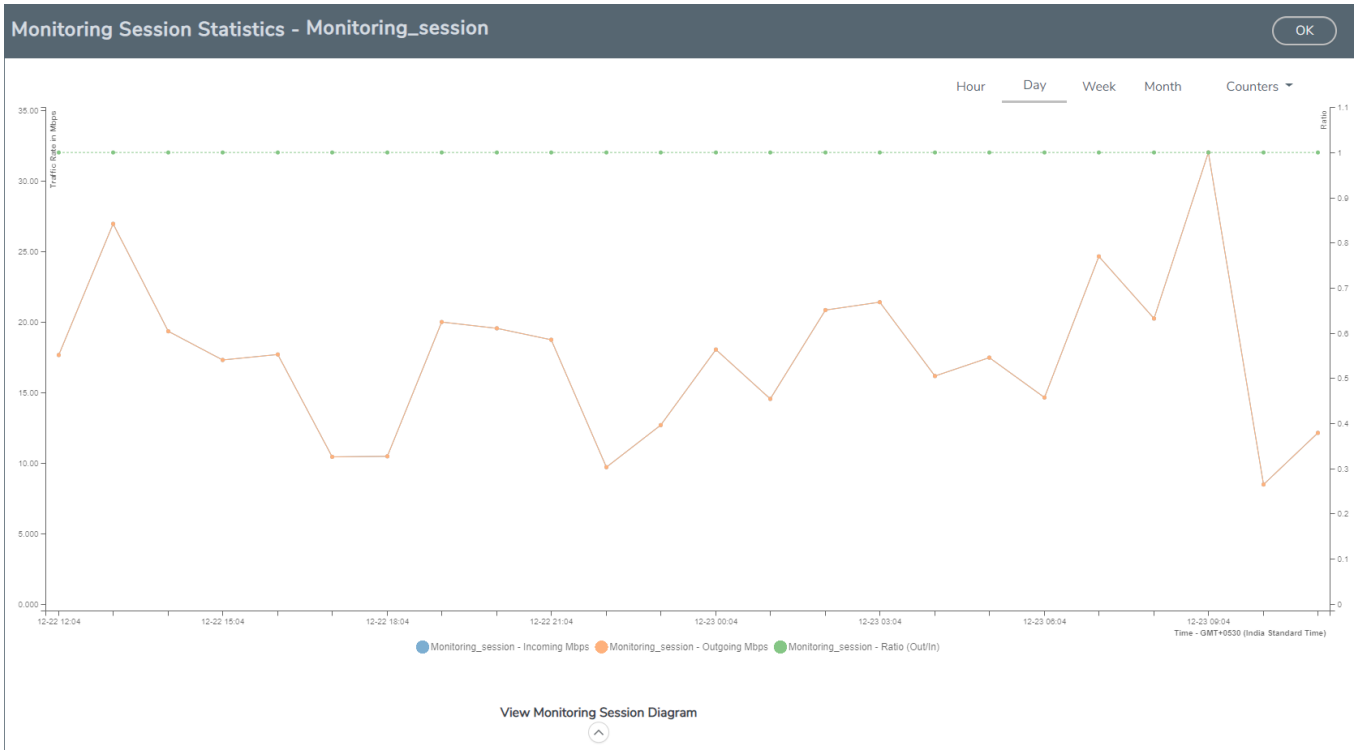
Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again..
Delete	Deletes the selected monitoring session.

View Monitoring Session Statistics

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

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

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



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

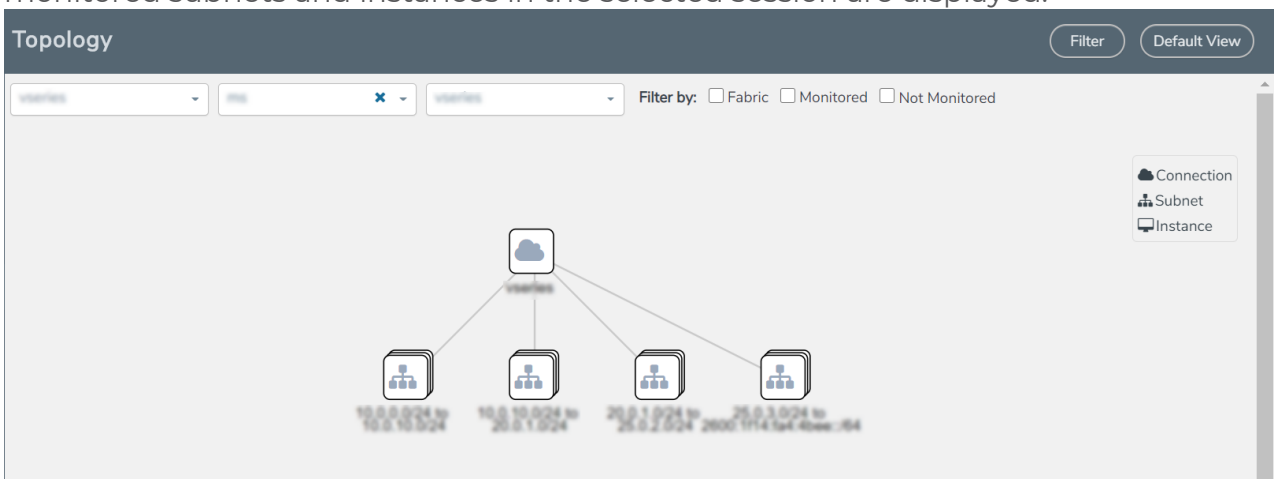
- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view 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.

Configure Application Intelligence Solutions on GigaVUE V Series Nodes for AWS

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow. Refer the following topics for step by step instructions on how to configure Application Intelligence solution for GigaVUE V Series Nodes:

- Configure Environment
- Create Credentials
- Connect to AWS
- Create Source Selectors
- Create Tunnel Specifications
- Configure Application Intelligence Session

Important Notes:

- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **V Series Node API Proxy Server** (VPS) to scale and manage multiple V Series Nodes. Refer to the GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide for detailed information.
- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- Prior to configuring the Application Intelligence solution, refer to the Prerequisites topic for the minimum requirements.
- When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to Configuration Settings section in the *GigaVUE Administration Guide* for configuration details.
- To delete a GigaVUE V Series Node deployed in a Application Intelligence solution, you must delete the resources in the following order:
  1. Delete the Application Intelligence solution.
  2. Delete the GigaVUE V series Node and Connection.
  3. Delete the Environment.

Configure Environment

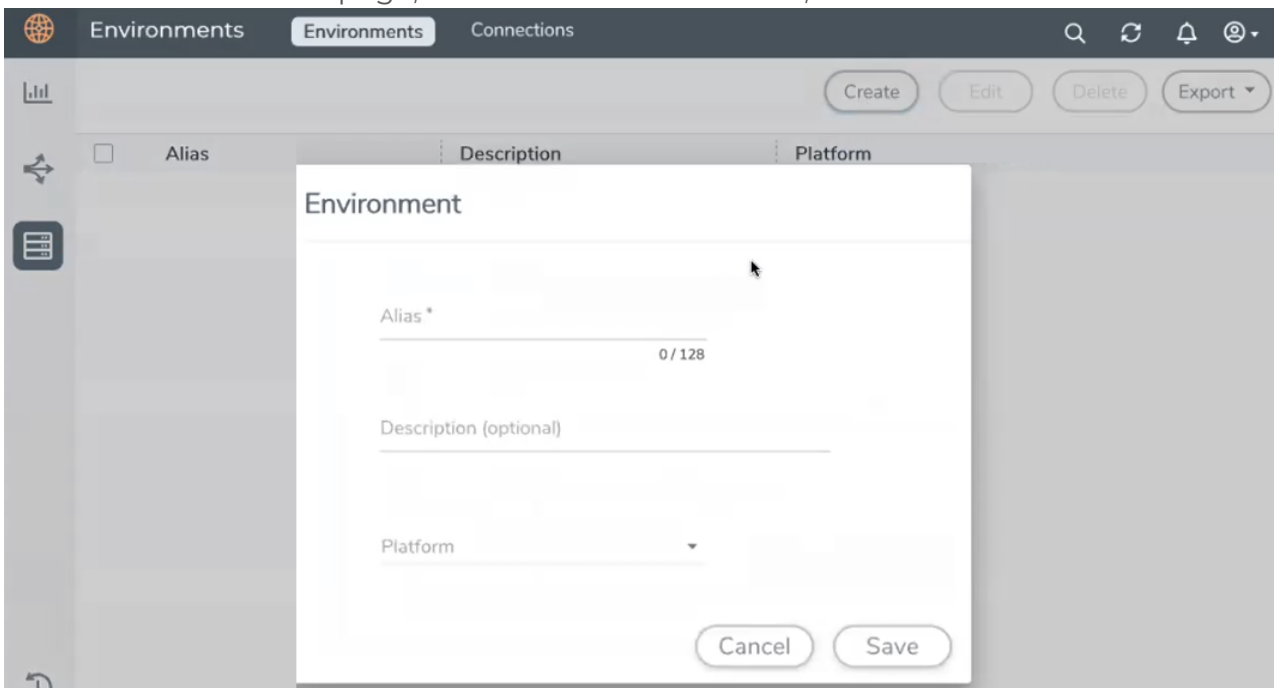
The Environments page allows you to create the following:

- **Environments**: The physical or the virtual environment in which the Application Intelligence solution is to be deployed.
- **Connections**: Connection between GigaVUE-FM and the cloud platform.

Create Environment

To configure the Environment:

1. Select **Inventory** > **Resources** > **Environments**.
2. On the **Environments** page, on the **Environments** tab, click **Create**.



3. Select or enter the following details:

Field	Description
Alias	Alias name used to identify the Environment.
Description	Brief description about the Environment.
Platform	Select the cloud platform.

4. Click **Save**. The environment is added to the list view.

Use the following buttons to manage your environment:

Button	Description
Delete	Use to delete an Environment.
Edit	Use to edit the details in an Environment.
Export	Export the details from the Environment page in an XLS or CSV file.

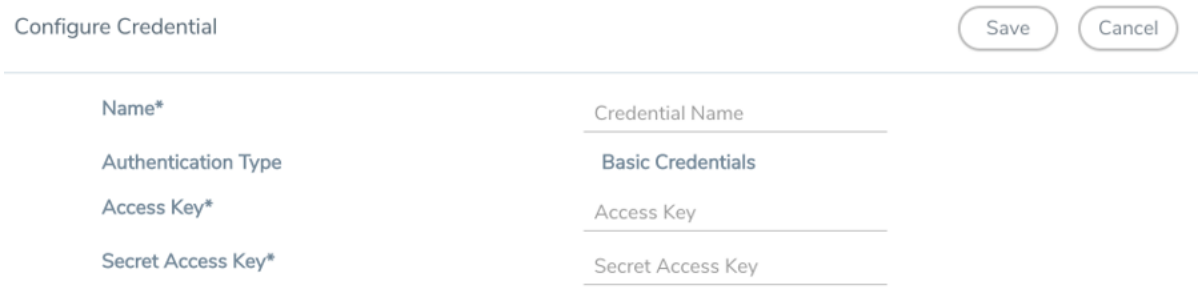
Create Credentials

You must configure your AWS Credentials for configuring the Application Intelligence solution.

Create AWS Credentials

To create AWS credentials:

1. From the left navigation pane, click **Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Credentials** tab, select **AWS** from the drop-down menu.
3. On the AWS Credential page, click **Add**. The **Configure Credential** page appears.



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

Field	Action
Name	An alias used to identify the AWS credential.
Authentication Type	**Basic Credentials** For more information, refer to AWS Security Credentials.
Access Key	Enter your AWS access key. It is the credential of an IAM user or the AWS account root user.
Secret Access Key	Enter your secret access key. It is the AWS security password or key.

5. Click **Save**.

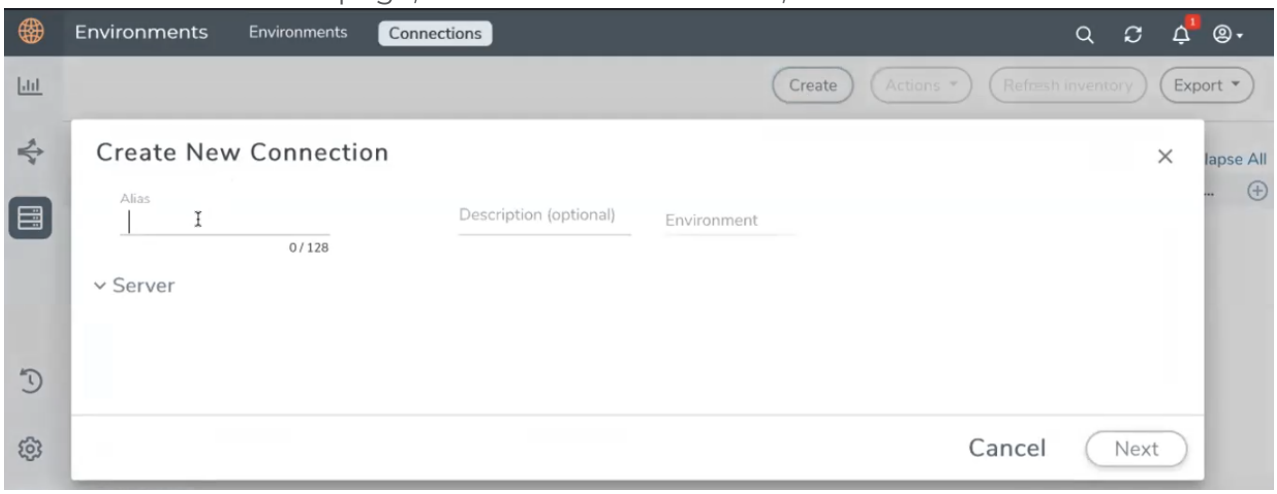
Connect to AWS

After creating a environment create a connection between the AWS and GigaVUE-FM. Refer to the following step given below for detailed information on how to create a new connection.

Create Connection

To create a new Connection:

1. Select **Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Connections** tab, click **Create**.



3. The **Create New Connection** dialog box opens. Enter the details as mentioned in the below section.

> **NOTE:** When creating a connection in the connections page, the corresponding monitoring domain created for internal use in GigaVUE-FM will not be displayed in the Monitoring Domain list page.

> **NOTE:** For Application Intelligence solution, you must add the UDP port 2056 for GigaVUE-FM in your AWS security group.

To connect to AWS, select or enter the following details:

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials for detailed information on how to create credentials.
Secret	The AWS region for the connection. For example, EU (London).

Field	Description
Region	**NOTE:** If the region you want to choose is not available in the Region Name list, you can add a custom region. **Adding a Custom Region** To add a custom region: **a.** In the Region Name drop-down list, select **Custom Region**. **b.** In the Custom Region Name field, enter the name of the region that is not available in the list.
Select Account	Select the AWS account name/id.
Select VPCs	Select the VPC
Traffic Acquisition Method	Select a Tapping method. The available options are: ▪ **G-vTAP**: If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP Agents. You can also configure the G-vTAP Controller and G-vTAP Agents using your own orchestor. Refer to Configure GigaVUE Fabric Components using AWS Orchestrator for detailed information. ▪ **VPC Traffic Mirroring**: If you select VPC Traffic Mirroring option as tapping method, only nitro-based agent is support. If you wish to use an external load balancer (optional). Select **Yes** to use a load balancer. Refer to Configure an External Load Balancer on GigaVUE Cloud Suite for AWS and Configure a Gateway Load Balancer on GigaVUE Cloud Suite in AWS for detailed information. G-vTAP Controller configuration is not required for VPC Traffic Mirroring. ▪ **Tunnel**: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series Nodes without deploying G-vTAP Agents or G-vTAP controllers.. **NOTE:** For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions and Privileges for details.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. **NOTE:** The default MTU is 1450. You can edit the MTU value according to your requirements. The valid range is between 1450 to 9000.

In the AWS Virtual Node Deployment page, select or enter the following details and click **Next**:

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	The Elastic Block Store (EBS) volume that you can attach to the fabric components. The

Fields	Description
Type	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.
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.

Enable the **Configure a V Series Proxy** toggle button if you wish to deploy V Series nodes using a proxy. In the V Series Proxy section, select or enter the values for the fields as described in the below table.

Fields	Description
Version	GigaVUE V Series Proxy version.
Instance Type	Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Number of Instances	Number of GigaVUE V Series Proxy 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 Proxy. Refer to Security Group for more details.

Fields	Description
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 Proxy 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 Proxy 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 Proxy instances in your AWS environment.

In the G-vTAP Configuration section, select or enter the following details:

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: An older version of G-vTAP Controller can be deleted once all the G-vTAP Agents are upgraded to the latest version.
Instance Type	The instance type for the G-vTAP controller. The recommended minimum instance type is nitro-based starting from t2.micro. **NOTE:** V Series 2 solution does not support non-nitro-based instance types.
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.
G-vTAP Agent MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP Agent to the GigaVUE V Series node. • In AWS, the default value is 9000.

Fields	Description
	• For VXLAN, the default value is 8951. The G-vTAP Agent tunnel MTU must be at least 50 bytes less than the agent's destination interface MTU size. • For GRE, the default MTU setting must be at least 42 bytes less than the default MTU. AWS Platform MTU is 9000 ▪ With agent tunnel type L2GRE and 'Secure Mirror Traffic' option enabled, G-vTAP Agent Tunnel MTU should be set as (9000-42-53) = 8905. ▪ With agent tunnel type L2GRE and 'Secure Mirror Traffic' option disabled, G-vTAP Agent Tunnel MTU should be configured as (9000-42) = 8958. ▪ With agent tunnel type VXLAN and 'Secure Mirror Traffic' option enabled, G-vTAP Agent Tunnel MTU should be (9000-50-53) = 8897. ▪ With agent tunnel type VXLAN and 'Secure Mirror Traffic' option disabled, G-vTAP Agent Tunnel MTU should be 8951.
IP Address Type	The IP address type. Select one of the following: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the G-vTAP Controller and GigaVUE-FM. ▪ Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. ▪ Select **Elastic** if you want a static public IP address for your instance. Ensure to have the available elastic IP address in your VPC. **NOTE:** The elastic IP address does not change when you stop or start the instance.
Additional Subnet(s)	(Optional) If there are G-vTAP Agents on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the G-vTAP Controller can communicate with all the G-vTAP Agents. Click **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
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.

In the V Series Node configuration section, select or enter the following:

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. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
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 **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.
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.
Max Number of Instances	The maximum number of GigaVUE V Series Nodes that can be deployed in the monitoring domain.
Tunnel MTU	The Maximum Transmission Unit (MTU) on the outgoing tunnel endpoints of the GigaVUE V Series Node when a monitoring session is deployed. The G-vTAP Agent and controller tunnel MTU should be 50 bytes less than the agent's destination interface MTU size. The default value is 9001.
Data Subnets	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the G-vTAP Agents. **NOTE:** Using the Tool Subnet checkbox you can indicate the subnets to be used by theGigaVUE V Series to egress the aggregated/manipulated traffic to the tools.

Use the following buttons to manage your AWS connections :

Button	Description
Create	Use to create new connection.
Actions	Provides the following options: • **Edit Connection** - Use to edit a connection. You can also use this option to deploy your node after creating the connection.

Button	Description
	• **Edit Node** - If you have already deployed your node, then use this option to edit your node. You can also use this option to add more nodes into your existing connection. • **Delete Connection** - Use to delete a connection. • **Delete Node** - Use to delete a node. • **Force Delete** - This option is enabled when an upgrade fails due to infrastructure issues. Use this option to force delete the connection. • **Upgrade Fabric** - Use to upgrade your fabric components.
Refresh Inventory	Use to refresh the entire connections page.
Export	Use to export the details from the Connections page into an XLS or a CSV file.

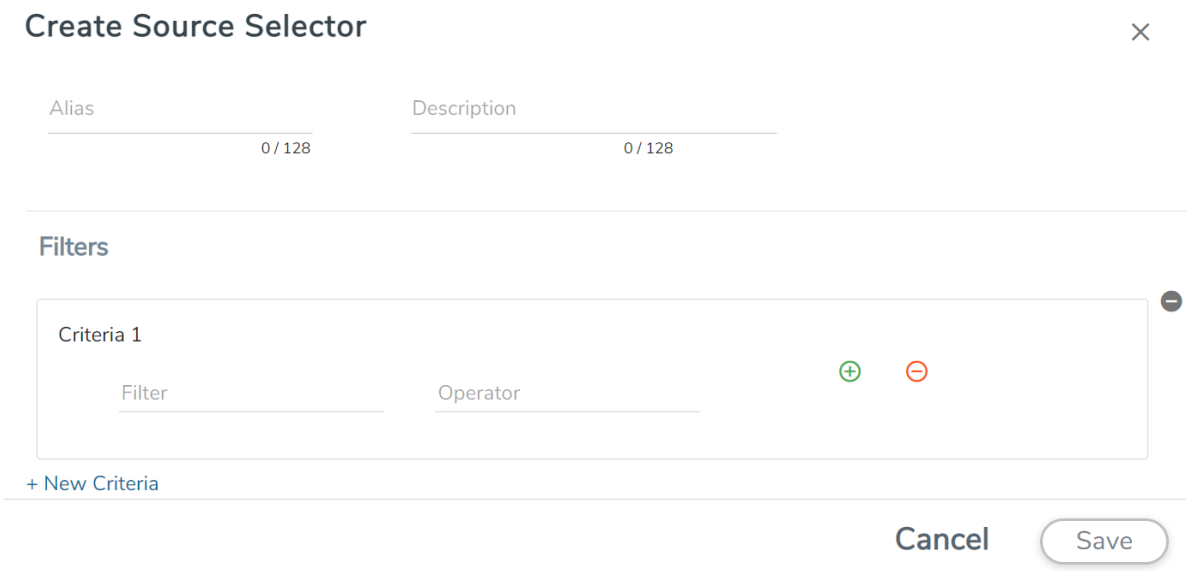
Create Source Selectors

When setting up a traffic flow, it is important to define the selection criteria for the source of traffic. Use the Source Selectors page for configuring the source of traffic to the GigaVUE V Series nodes.

NOTE: When deploying the Application Intelligence suing Source Selector, if the GigaVUE V Series Node is down, you will not be able to view the Selected Targets and G-vTAP Agents.

To configure the Source Selectors:

1. Select **Inventory** > **Resources> Source Selectors**.
2. On the **Source Selectors** page, on the **VM** tab, click **Create**. The **Create Source Selector** wizard appears.



3. Enter or select the required information:

Field	Description
Alias	Name of the source
Description	Description of the source
Filters	You can create a filter template from the Filters option
Criteria 1	Criteria to filter the traffic source. **NOTE:** You can create multiple criteria.
Filter	The criteria based on which the traffic is filtered. Select from the list of available filters. **NOTE:** Ensure that the registered traffic agents match the filter criteria.
Operator	Select the required operator based on the filter selected. Options are: • Starts with • Ends with • excludes • equals • between
Values	The values for the filter.

4. Click Save to save the source selector.

Note: You can create multiple filter criteria. Within each criterion, you can configure multiple filters.

- If you have configured multiple filters in a criterion, then the traffic will be filtered only if all the filter rules are true.
- If you have configured multiple criteria, then the traffic will be filtered even if one of the criteria is true.

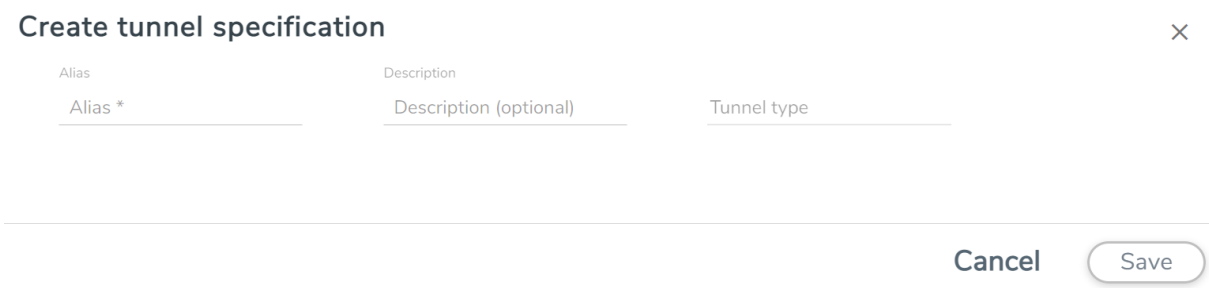
Create Tunnel Specifications

A tunnel endpoint can be created using a standard L2GRE, VXLAN, or ERSPAN tunnel. The tunnel can be an ingress tunnel or an egress tunnel.

NOTE: VXLAN is the only supported tunnel type for Azure.

To configure the tunnels:

1. Select **Inventory** > **Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **VM** tab and click **Create**. The Create Tunnel Specification wizard appears.



3. Enter or select the following information:

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

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

User Defined Application

This feature gives you the ability to classify applications not classified automatically by the DPI engine. This allows unclassified TCP, UDP, HTTP, and HTTPS applications to be identified and named with the help of user defined application signatures.

To configure User Defined Application signatures :

Step Number	Task	Refer the following
1	Create rules under User Defined Application Section	Create rules under User Defined Application
2	Configure Application Intelligence Session	For Physical: Application Intelligence Session For Virtual: Configure Application Intelligence Session
3	Monitor User Defined Application	View the Application Intelligence Dashboard

Create Rules under User Defined Application

1. Click **Inventory**.

2. Click **User Defined Applications** to create rules based on a set of **Supported Protocols and Attributes**. For information on **Supported protocols and Attributes** refer **User Defined Application** topic. This helps the physical or virtual node to classify the traffic based on the protocols and attributes selected in the created rule.

3. Click **New** in the **User Defined Applications** screen to create a new rule.

4. Enter **Application Name**.

5. Enter **Priority**. The value must be between 1 and 120.

Note: The least value will have the highest priority.

6. In the created rule:

   a. Choose the **Protocol** from the list of protocols.

   b. Choose the **Attributes** from the list of attributes.

   c. Choose the **Values** from the list of values.

7. Click **Apply**. The rule is now created. For information on the limitations for creating rules refer Configuration Limitations section.

8. Click the application listed under the **Applications** column.

9. Click the **Rule** tab.

10. Select a rule to view its protocol details.

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regex patterns, refer Supported RegExp Syntax

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file|new_slice|upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for	Client to Server	REGEXP	mozilla

			request	Only		
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http:\/\/gigamon.com\/
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\/football\/.*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
ssl	common_name	Domain Name	Domain name from Client Hello message or the certificat		REGEXP	(.*\.)?gigamon\.com

			e			
	stc-subject_alt_name	Subject Alt Name (s)	List of host names which belong to the same certificate	Server to Client Only	REGEXP	(.*\.)?gigamon\.com
rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http:\/\/www.music.tv\/recorded\/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a packet, excluding the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata

	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
sip	user_ agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Messa ge Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Messa ge Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addres s	IP address of the server		IPV4 as REGEXP String	62.132.12.30\/24
	dscp	DSCP Value	DSCP from Different ia ted Service (DS) Field in		UINT8 as REGEXP String	33

			IP header			
	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentia ted Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that

	precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
( ) [ ]	Groups a series of expressions together Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
| [<start>-<end>]	Separates values contained in ( ). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog | cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_ number>	Matches for a direct binary with octal input
\x<hexadecimal-number>\x	Matches for a direct binary with hexadecimal input
\[<character-set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Configure Application Intelligence Session

Application Visualization (earlier known as Application Monitoring) gathers the application statistics, and sends this information to GigaVUE-FM, which acts as an application monitor. The monitoring reports are sent to GigaVUE-FM through the destination port 2056. The application statistics appear as an array of monitoring reports that provide application-usage data in an easy-to-read graphical interface. This provides you with greater insight and control over how your network is being used and what applications are utilizing the most resources. To perform Application Monitoring, you must create the required application intelligence sessions on the nodes managed by GigaVUE-FM.

Prerequisites

- The environment on which the Application Intelligence solution is to be deployed must already be created and the nodes must be deployed on it.
- In virtual environment, the destination tunnels for the Application Filtering Intelligence Map must already be created.

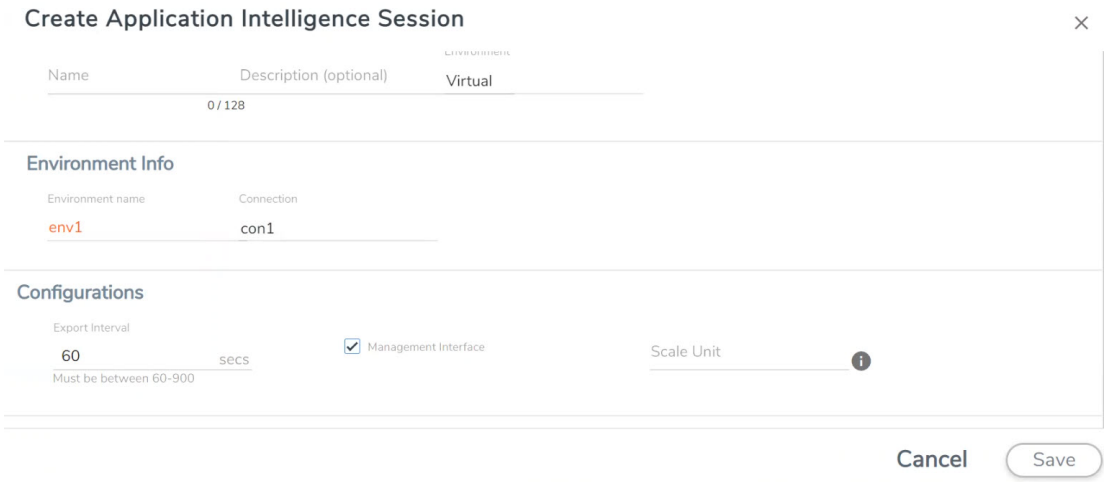
> **NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

Complete the following prerequisites before creating an Application Intelligence solution in the virtual environment:

To create an Application Intelligence Session:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**.
2. Click **Create New**. The **Create Application Intelligence Session** page appears.



3. In the **Basic Info** section, enter the name and description, and in the Environment select **Virtual** for the session to be created:
   - Virtual- connects to the specific environment.
4. In the Environment section, select the **Environment Name**, and the **Connection Name.** To create an Environment and connection, refer to Configure Environment.
5. In the **Configurations** section, complete the following:
   a. Select an **Export Interval** during which you want the Application Intelligence session to generate the reports for application visualization. The valid range is 60–900 seconds.
   b. Select the required interface. By default, **Management Interface** is enabled. To export the data through tunnel interface, uncheck the Management Interface check box.
   c. Enter a value for the **Scale Unit**. The scale unit represents the number of flows supported by the application. If the scale unit value is 1, the maximum active flow limit will be 100k.
   Refer to the following table for the maximum scale unit supported for VMware, AWS, and Azure platforms.

   NOTE: Scale Unit is not applicable for the OpenStack platform.

Cloud Platform	Instance Size	Maximum Scale Unit
VMware	Large (8 vCPU and 16 GB RAM)	3
	Medium (4 vCPU and 8 GB RAM)	1
AWS	Large (c5n.2xlarge)	4
	Medium (t3a.xlarge)	3
Azure	Large (Standard_D8s_V4)	9
	Medium (Standard_D4s_v4)	3

6. In the **Source Traffic** section, select anyone of the following:

- **Source Selector**- Select the source from the drop-down list box. To create new source, select **New Source Selector** and add the filters. For more information on creating a New Source Selector, refer to Create Source Selectors.

  NOTE: You cannot configure Source Selectors when you deploy the GigaVUE V Series Nodes using the Third Party Orchestration in VMware ESXi host.

- **Tunnel Specification**- Select the tunnel from the drop-down list box. To create new tunnel, select **New Source Tunnel Spec** and add the details for the tunnel. For more information on creating a new tunnel, refer to Create Tunnel Specifications.

> **NOTE:** Select the ens192 interface for the Tunnel Specifications from the drop-down menu when using third party orchestration.

- **Raw End Point**- Select the Raw End Point Interface from the drop-down menu which will trap the traffic for application monitoring.

  > **NOTE:** This field is applicable only when you deploy your GigaVUE V Series Nodes using third party orchestration in VMware ESXi Host, Nutanix and Google Cloud Platform.

> - Tunnel Specification for the source must always be configured with Traffic Direction as IN, to indicate that it is an ingress tunnel.
> - For Azure Connection, VXLAN is the only supported Tunnel Type.

7. Click **Save**. The session created is added in the list view.
8. In the **User Defined Applications** section, select the template from the list.For information on **Supported protocols and Attributes** and **Limitations** refer **User Defined Application** topic.

The total applications participating in the network traffic are displayed in the Application Intelligence Dashboard. For more information about the dashboard, refer to the View the Application Intelligence Dashboard.

Select the session from the Application Intelligence Sessions pane and click on the ⋮ icon and select **View Details** from the drop-down menu, to view the deployed G-vTAP Agents, their status and more information about source selectors, selected target.

If the session configuration is unsuccessful, troubleshoot the error notified (refer to View the Health Status of a Solution). Click the **Reapply all pending solutions** button in the dashboard to redeploy the configuration.

> **NOTE:** GigaVUE-FM takes few minutes to display the application statistics.

> **NOTE:** The option **Reapply all pending solutions** is applicable for physical solution only.

When the Application Intelligence solution is in suspended state, you cannot delete the session. You can click on the ⋮ icon and select **View Details** from the drop-down menu, to view the details.

You can also filter the traffic based on the applications. For more information, see Create Application Filtering Intelligence.

Cloud Health Monitoring

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components.

Configuration Health Monitoring

The configuration health status provides us detailed information about the configuration and deployment status of the deployed monitoring session.

This feature is supported for the following fabric components and features on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For G-vTAP Agents:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

To view the configuration health status, refer to the View Health Status section.

Traffic Health Monitoring

GigaVUE-FM allows you to monitor the traffic health status of the entire monitoring session and also the individual V Series Nodes for which the monitoring session is configured. Traffic health monitoring focuses on identifying any discrepancies (packet drop or overflow etc) in the traffic flow. When any such discrepancies are identified, GigaVUE-FM propagates the health status to corresponding monitoring session. GigaVUE-FM monitors the traffic health status in near real-time. GigaVUE V Series Node monitors the traffic, when the traffic limit goes beyond the upper or lower threshold values that is configured, it notifies GigaVUE-FM, based on which traffic health is computed.

This feature is supported for GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware

The following section gives step-by-step instructions on creating, applying, and editing threshold templates across a monitoring session or an application, and viewing the traffic health status. Refer to the following section for more detailed information:

- Create Threshold Template
- Apply Threshold Template
- Edit Threshold Template
- Clear Thresholds
- Supported Resources and Metrics

Keep in mind the following points when configuring a threshold template:

- By default Threshold Template is not configured to any monitoring session. If you wish to monitor the traffic health status, then create and apply threshold template to the monitoring session.
- Editing or redeploying the monitoring session will reapply all the threshold policies associated with that monitoring session.
- Deleting or undeploying the monitoring session will clear all the threshold policies associated with that monitoring session.
- After applying threshold template to a particular application, you need not deploy the monitoring session again.

Create Threshold Template

To create threshold templates:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.
2. The **Threshold Template** page appears. Click **Create** to open the **New Threshold Template** page.
3. Enter the appropriate information for the threshold template as described in the following table.

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Monitored Objects	Select the resource for which you wish to apply the threshold template. Eg: TEP, REP, Maps, Applications like Slicing, Dedup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that needs to be monitored. For ex, Tx Packets, Rx Packets etc
Type	**Difference**: The difference between the stats counter at the start and end time of an interval, for a given metric. **Derivative**: Average value of the stats counter in a time interval, for a given metric.
Condition	**Over**: Checks if the stats counter value is greater than the 'Set Trigger Value'. **Under**: Checks if the stats counter value is lower than the 'Set Trigger Value'.
Set Trigger Value	Value at which a traffic health event is raised, if stats counter goes below/ above this value. Based on the condition configured.
Clear Trigger Value	Value at which a traffic health event is cleared, if stats counter goes below/ above this value. Based on the condition configured.

4. Click **Save**. The newly created threshold template is saved, and it appears on the **Threshold Template** page.

Apply Threshold Template

You can apply your threshold template across the entire monitoring session and also to a particular application.

Apply Threshold Template to Monitoring Session

To apply the threshold template across a monitoring session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. To apply a threshold template across a monitoring session, select the template you wish to apply across the monitoring session from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Done**.

Apply Threshold Template to Applications

To apply the threshold template to a particular application in the monitoring session follow the steps given below:

NOTE: Applying threshold template across monitoring session will not over write the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it over writes the existing threshold value for that particular application.

1. On the **Monitoring Session** page. Click **Actions > Edit**. The Edit Monitoring Session page with canvas page appears.
2. Click on the application for which you wish to apply or change a threshold template and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Save**.

Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appear.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

NOTE: Editing a threshold template does not automatically apply the template to monitoring session. You must apply the edited template to monitoring session for the changes to take effect.

Clear Thresholds

You can clear the thresholds across the entire monitoring session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the monitoring session follow the steps given below:

1. On the **Monitoring Session** page. Click **Actions > Edit**. The Edit Monitoring Session page with canvas page appears.
2. Click on the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Click **Clear All** and then Click **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a monitoring session follow the steps given below:

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. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds page appears**. Click **Clear**.

NOTE: Clearing thresholds at monitoring session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application refer to Clear Thresholds for Applications

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors	1. Difference 2. Derivative	1. Over 2. Under

	8. Rx Errors		
Raw End Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
Map	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Slicing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Header Stripping	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Tunnel Encapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Load Balancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSL Decryption	1. Tx Packets 2. Rx Packets	1. Difference 2. Derivative	1. Over 2. Under

	3. Packets Dropped		
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMI Exporter	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

View Health Status

You can view the health status of the monitoring session on the Monitoring Session details page. The health status of the monitoring session is healthy only if both the configuration health and traffic health are healthy.

View Health Status of the Entire Monitoring Session

To view the health status of a monitoring session:

1. On the Monitoring Session details page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed, click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

This displays the configuration health and traffic health of the monitoring session and also the thresholds applied to that monitoring session.

View Health Status of an Application

To view the health status of an application across an entire monitoring session:

1. On the Monitoring Session page, click on the health status displayed in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

This displays the configuration health and traffic health of the application and also the thresholds applied to that particular application.

View Health Status for Individual V Series Nodes

You can also view the health status of the view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu and then click on the Status displayed in the top left-corner above the canvas. The quick view page appears.

View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, click on the health status in the **Status** column of the monitoring session.
2. The monitoring session diagram is displayed. Select the V Series Node from the **View By** drop-down menu.
3. To view application health, click on the application for which you wish to see the health status. The quick view page appears.
4. Click on the **Status** tab.

The subsession toggle button available in the top-left corner of the canvas allows you to view the statistics of individual paths in the monitoring session. If the traffic health is not configured for monitoring session or a particular application, the traffic health is displayed as **Not Applicable**.

View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page.

The following columns in the monitoring session page are used to convey the health status:

Health

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy then the health status is moved to unhealthy.

V Series Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

You can view the health status of the individual V Series Nodes by clicking on the V Series Node Health column.

NOTE: V Series Node health only displays the health status therefore even if the V Series Node is down it will not be reflected in the monitoring session page.

Target Source Health

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

Fabric Health Analytics for Virtual Resources (BETA)

Fabric Health Analytics is delivered as BETA in software version 5.16.00 and is subject to change in the upcoming release(s).

Fabric Health Analytics (FHA) in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using FHA[1] you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using FHA. Dashboards, Visualizations and Search Objects are called FHA objects. Refer to Fabric Health Analytics BETA topic in *GigaVUE Fabric Management Guide* for more detailed information on Fabric Health Analytics.

Rules and Notes:

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the Clone Dashboard section for more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.

Virtual Inventory Statistics and Cloud Applications Dashboard

Fabric Health Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. Refer to the Fabric Health Analytics section in *GigaVUE Fabric Management Guide* for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

To access the dashboards:

1. Go to  -> **Analytics -> Dashboards.**
2. Click on the required dashboard to view the visualizations.

The following table lists the various virtual dashboards:

[1]FHA uses the Kibana front-end application to visualize and analyze the data in the Elasticsearch database of GigaVUE-FM. Kibana is an open source data visualization plugin for Elasticsearch.

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: • Platform • Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the V Series node in 5 minutes interval, for the past one hour. **NOTE:** The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the V

Dashboard	Displays	*Visualizations*	Displays
			Series node for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Rx Trend	Receiving trend of the V Series node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the V Series network interface for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Tunnel Rx Packets/Errors	Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation.
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload.

Dashboard	Displays	*Visualizations*	Displays
	• VSeries Node	*Dedup Packets Detected/Dedup Packets Overload Percentage*	Percentage of the dedup packets received against the dedup application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session**: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V-series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • **V series node**: Management IP of the V Series node. Choose the required V-series node from the drop-down. • **Tunnel:** Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. The following statistics are displayed for the tunnel: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.

Dashboard	Displays	*Visualizations*	Displays
	• Transmitted Errored Packets • Transmitted Dropped Packets	*Tunnel Packets*	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V series node. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V series node** • **Application**: Select the required application. By default, the visualizations displayed includes all the applications. By default, the following statistics are displayed: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
		App Packets	Displays received traffic vs transmitted traffic, as the number of packets.
End Point (Virtual)	Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V-series nodes. The following statistics that are shown for Endpoint (Virtual): • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets The endpoint drop-down shows *<V-series Node Management IP address : Network Interface>* for each endpoint. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V Series node** • **Endpoint:** Management IP of the V Series node followed by the Network Interface (NIC)	*Endpoint Bytes*	Displays received traffic vs transmitted traffic, in Bytes.
		Endpoint Packets	Displays received traffic vs transmitted traffic, as the number of packets.

NOTE: The Tunnel (Virtual), App (Virtual) and Endpoint (Virtual) dashboards do not show data from the previous releases if the *Monitoring Session [Platform : Domain : Connection]* dashboard filter is applied. This is because, this filter relies on the new attributes in the Elasticsearch database, which are available only from software version 5.14.00 and beyond.

Administer GigaVUE Cloud Suite for AWS

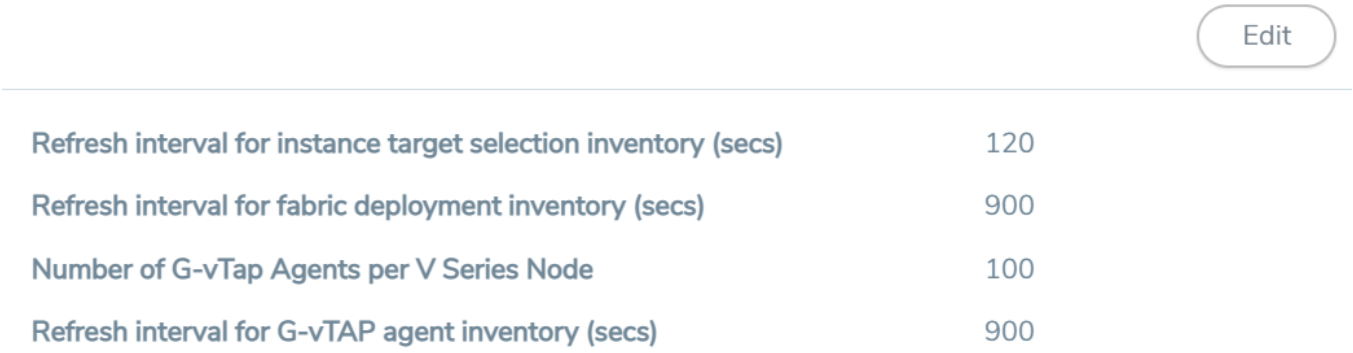
You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

- 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-

Settings	Description
	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.

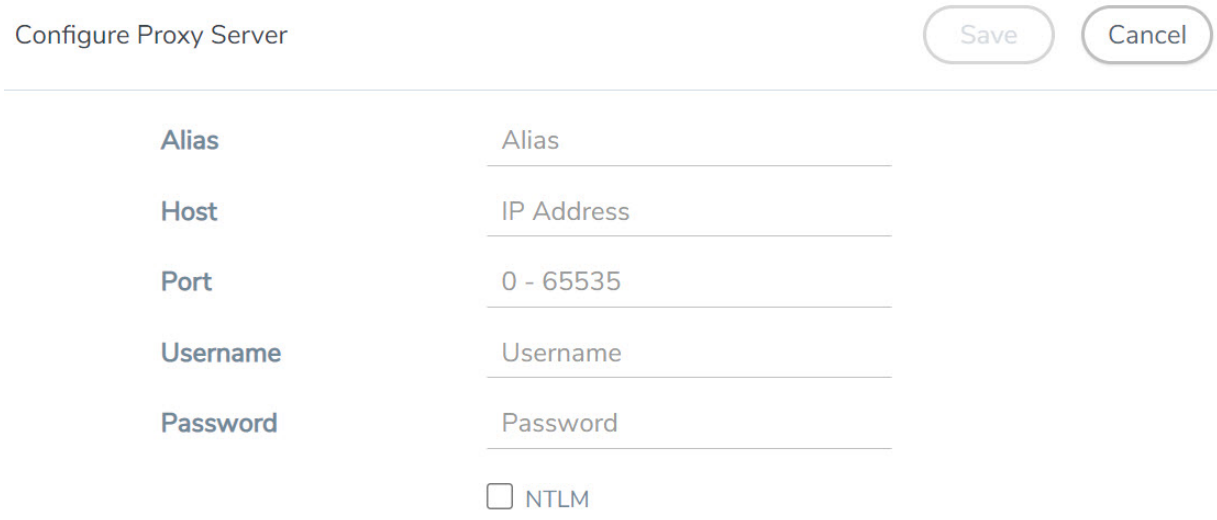
Configure Proxy Server

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

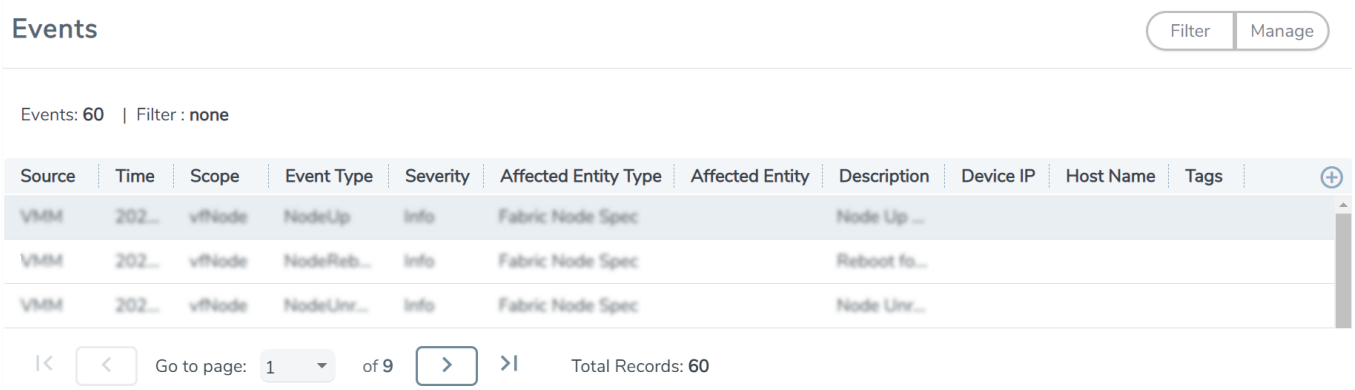
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- 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.

Controls/ Parameters	Description
Scope	The category to which the alarms or events belong. Alarms and events can belong to the following category: Virtual Fabric Node, VM Domain, VM Manager.
Event Type	The type of event that generated the alarms and events.
Severity	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when GigaVUE V Series nodes are installed, such a message is displayed as Info.
Affected Entity Type	The resource type associated with the alarm or event.
Affected Entity	The resource ID of the affected entity type.
Description	The description of the event, which includes any of the possible notifications with additional identifying information where appropriate.
Device IP	The IP address of the device.
Host Name	The host name of the device.

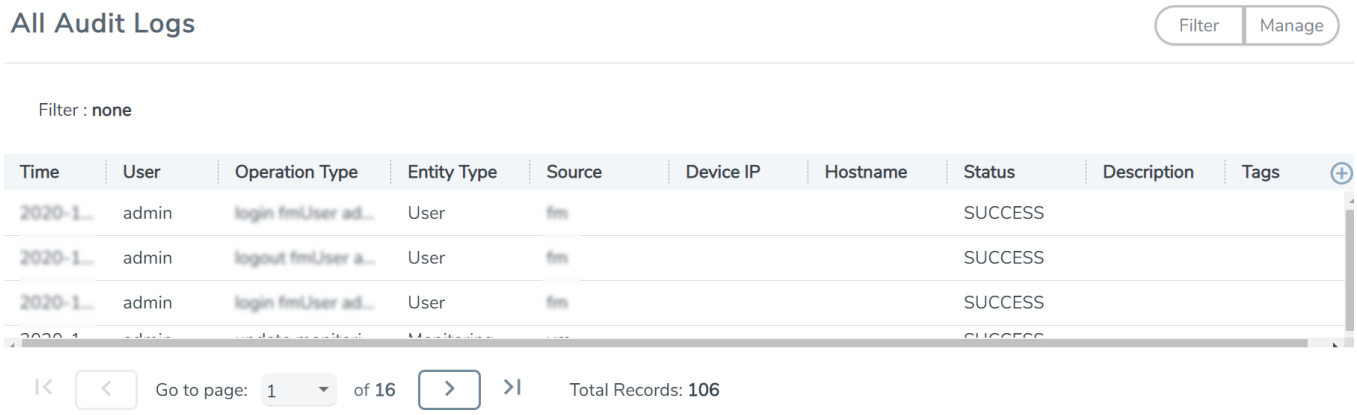
To filter the alarms and event:

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

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.
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 Suite fabric components available for the 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 2 Configuration

GigaVUE-FM	G-vTAP Agent Version	Next GenerationG-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series 2 Nodes
6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00	v6.2.00
6.1.00	v6.1.00	N/A	v6.1.00	v6.1.00	v6.1.00
6.0.00	v1.8-7	N/A	v1.8-7	v2.7.0	v2.7.0
5.16.00	v1.8-5	N/A	v1.8-5	v2.6.0	v2.6.0
5.15.00	v1.8-5	N/A	v1.8-5	v2.5.0	v2.5.0
5.14.00	v1.8-4	N/A	v1.8-4	v2.4.0	v2.4.0
5.13.01	v1.8-3	N/A	v1.8-3	v2.3.3	v2.3.3
5.13.00	v1.8-2	N/A	v1.8-2	v2.3.0	v2.3.0
5.12.01	v1.8-1	N/A	v1.8-1	v2.2.0	v2.2.0
5.12.00	v1.7-1	N/A	v1.7-1	v2.1.0	v2.1.0

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 Cloud Suite 6.2 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA10 Hardware Installation Guide
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 6.2 Hardware and Software Guides
***GigaVUE Cloud Suite for Third Party Orchestration**
GigaVUE Cloud Suite for AnyCloud Guide
Universal Container Tap Guide
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
GigaVUE Cloud Suite for AWS Secret Regions 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 Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
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 Cloud Suite 6.2 Hardware and Software Guides
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)