GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide

GigaVUE Cloud Suite

Product Version: 5.16

Document Version: 1.0

(See Change Notes for document updates.)

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
5.16.00	1.0	05/26/2022	Original release of this document with 5.16.00 GA.

Contents

GigaVUE Cloud Suite for 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:

About GigaVUE Cloud Suite for AWS

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

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

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

Refer to the following sections for details:

Components of GigaVUE Cloud Suite for AWS

GigaVUE Cloud Suite for AWS includes the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud Suite Cloud for AWS.GigaVUE-FM can be installed on-premises or launched as an Amazon Machine Image (AMI) in AWS. GigaVUE-FM manages the configuration of the following components in your Amazon Virtual Private Clouds (VPC):
  - G-vTAP Controller (only if you are using G-vTAP Agent as the traffic acquisition method)
  - GigaVUE® V Series 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 your VM instance. This agent mirrors the selected traffic from the instances (virtual machines) to the GigaVUE Cloud Suite® V Series node. The G-vTAP Agent is offered as a Debian (.deb) or Redhat Package Manager (.rpm) package. Refer to Install G-vTAP Agents.
- **G-vTAP Controller** manages multiple G-vTAP Agents and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more G-vTAP Controllers to communicate with the G-vTAP Agents. A G-vTAP Controller can only manage G-vTAP Agents that has the same version. For example, the G-vTAP Controller v1.7 can only manage G-vTAP Agents v1.7. So, if you have G-vTAP Agents v1.6 still deployed in the EC2 instances, you must configure both G-vTAP Controller v1.6 and v1.7. While configuring the G-vTAP Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the G-vTAP Agents to the GigaVUE Cloud Suite 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 the V Series node 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

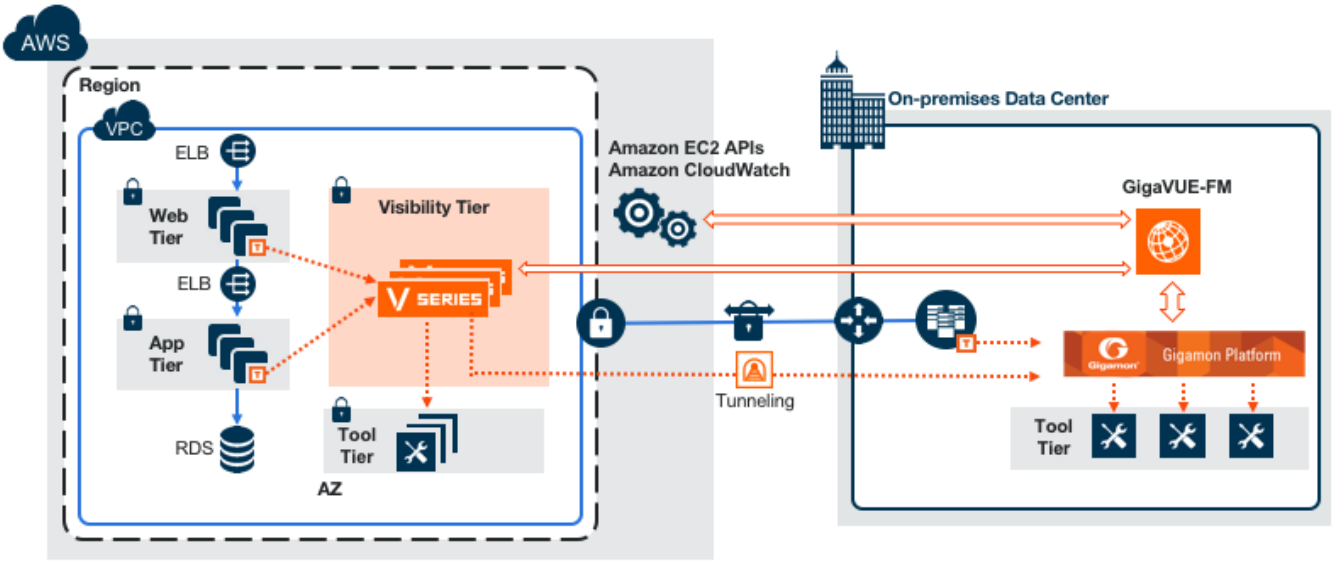
Architecture of GigaVUE Cloud Suite for AWS

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

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

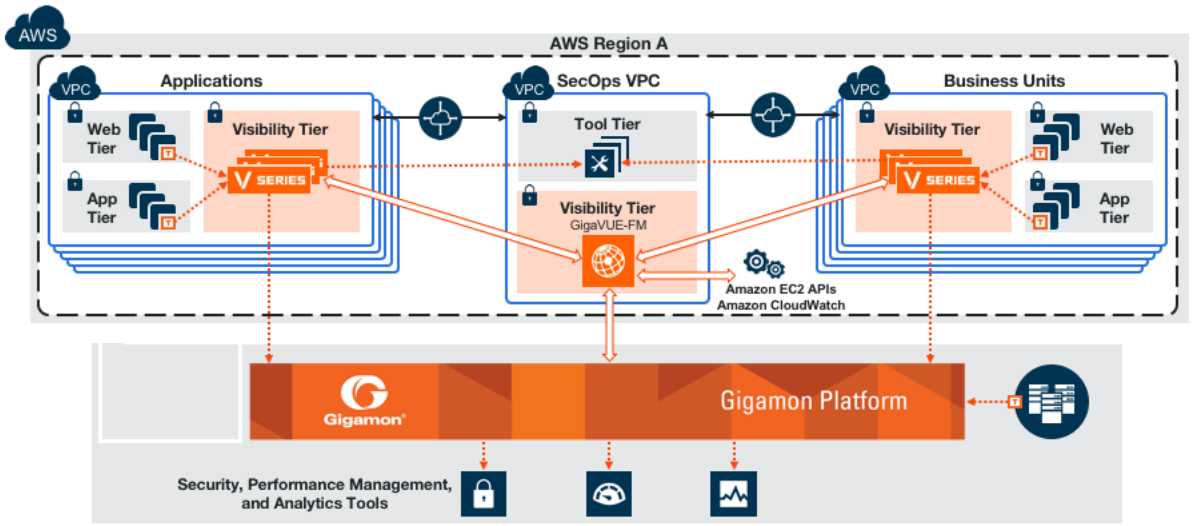
Hybrid Cloud

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.



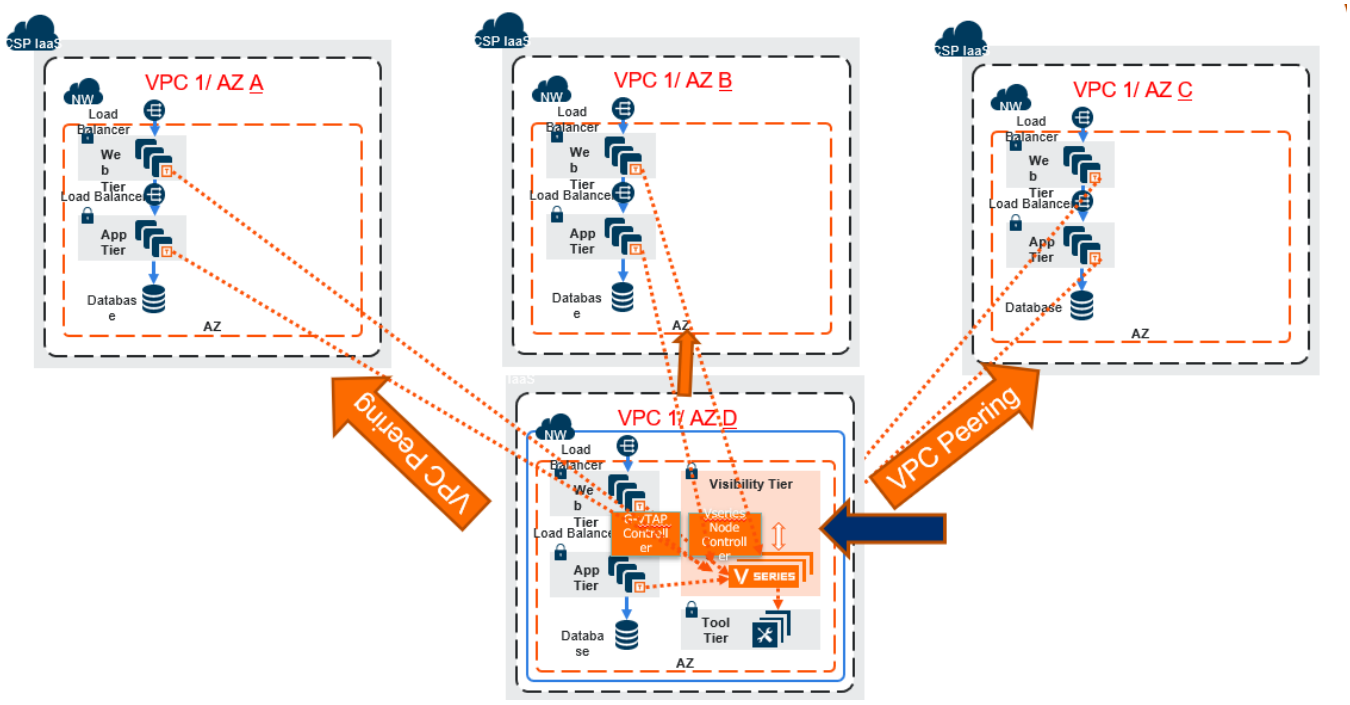
Centralized Fabric Controllers and Node Configuration

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.

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:

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

License Information

GigaVUE Cloud is available in both the public AWS cloud and in AWS GovCloud, and supports the Volume Based License (VBL) model that you can avail from the AWS Marketplace.

Refer to the following sections for details:

- Volume Based License (VBL)
- Apply License

Volume Based License (VBL)

Volume Based License (VBL)

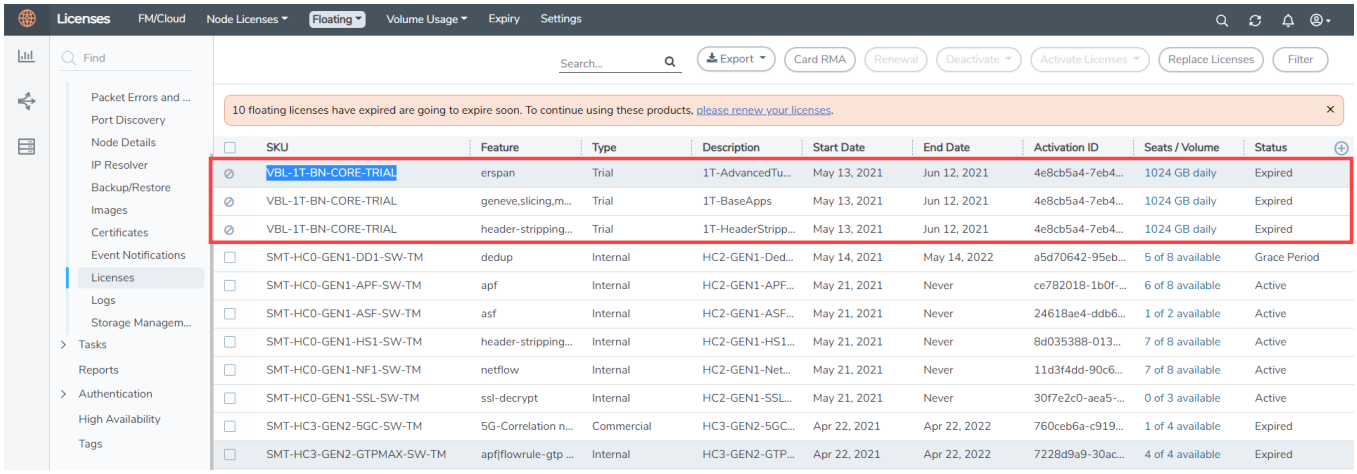
All the V Series 2 nodes connected to GigaVUE-FM reports the stats. All licensed applications, when running on the node, generate usage statistics. In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term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

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

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

Default Trial Licenses

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



This license includes the following applications:

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

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

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

How GigaVUE-FM tracks Volume-based License Usage

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

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

Apply License

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

Prerequisites

Refer to the following topics for details:

- AWS Security Credentials
- Amazon VPC
- Connect GigaVUE-FM to AWS

AWS Security Credentials

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

You need one of the following security credentials:

- **Identity and Access Management (IAM) role**—If GigaVUE-FM is running inside AWS, it is highly recommended to use an IAM role because it can securely make API requests from the instances. Create an IAM role and ensure that the permissions and policies listed in Permissions 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
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 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

Direction	Type	Protocol	Port	CIDR	Purpose
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
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 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.

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

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
- STS AssumeRole Policies

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.

An example of the above permissions is to associate the following policies to your IAM role before launching the GigaVUE-FM instance (you can attach this IAM at any time the instance exists):

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeKeyPairs",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTrafficMirrorFilters",
"ec2:DescribeTrafficMirrorSessions",
"ec2:DescribeTrafficMirrorTargets",
"ec2:DescribeVpcs"
],
"Resource": "*"
```

```
},
{
"Effect": "Allow",
"Action": [
"ec2:RunInstances",
"ec2:TerminateInstances"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
"ec2:CreateTrafficMirrorFilterRule",
"ec2:CreateTrafficMirrorSession",
"ec2:CreateTrafficMirrorFilter",
"ec2:DeleteTrafficMirrorFilter",
"ec2:DeleteTrafficMirrorSession",
"ec2:CreateTrafficMirrorTarget",
"ec2:DeleteTrafficMirrorTarget"
],
"Resource": "*"
}
]
}
---EC2 Permissions
"ec2:Describe*",
"ec2:RebootInstances",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"ec2:ReportInstanceStatus",
"ec2:Disassociate*",
"ec2:CreateTags",
"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*"
```

If you choose Amazon CloudWatch integration in GigaVUE-FM, you may also associate the following optional policies to your IAM role:

```
---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
```

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

Amazon STS Support and AssumeRole 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 *GigaVUE-FM Installation and Upgrade Guide*.
- 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
- Upgrade GigaVUE fabrics in GigaVUE-FM

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

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

```
$ ls gvtap-agent_1.8-5_amd64.deb
$ sudo dpkg -i gvtap-agent_1.8-5_amd64.deb
```

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

> NOTE: Any changes to the 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 **1.8-5** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

   ```
   $ ls gvtap-agent_1.8-5_x86_64.rpm
   $ sudo rpm -i gvtap-agent_1.8-5_x86_64.rpm
   ```
3. Modify the **/etc/gvtap-agent/gvtap-agent.conf** file to configure and register the source and destination interfaces.The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

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

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

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

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

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

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

   ```
   # eth0   mirror-src-ingress mirror-src-egress# eth1   mirror-src-
   ingress mirror-src-egress mirror-dst
   ```
4. Save the file.

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

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

6. Reboot the instance.

Check the status with the following command:

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

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

1. Launch the RHEL/CentOS agent AMI image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**1.8-5**_x86_64.rpm
   - gvtap.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te

```
semodule_package -o gvtap.pp -m gvtap.mod
sudo semodule -i gvtap.pp
```

5. Install G-vTAP Agent package:

```
sudo rpm -ivh gvtap-agent_1.8-5_x86_64.rpm
```

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

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

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

7. Install strongSwan:

```
tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
cd strongswan-5.7.1-1.el7.x86_64
sudo sh ./swan-install.sh
```

8. Reboot the instance.

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent **`1.8-5`** MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator** and the G-vTAP Agent service starts automatically.

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

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

   Following are the rules to modify the G-vTAP configuration file:
   - Interface is selected by matching its CIDR address with config entries.
   - For the VMs with single interface*(.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 **`1.8-5`** ZIP package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Extract the contents of the .zip file into a convenient location.
3. Run 'install.bat' as an **Administrator** and the G-vTAP Agent service starts automatically.

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

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

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

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

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

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

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

5. Save the file.

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

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

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

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

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

Install IPSec on G-vTAP Agent

If IPSec is used to establish secure connection between G-vTAP Agents andGigaVUE V Seriesnodes, then you must install IPSec on G-vTAP Agent instances. To install IPSec on G-vTAP Agent you need the following files:

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

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

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

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

Install G-vTAP from Ubuntu/Debian Package

1. Launch the Ubuntu/Debian image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**1.8-5**_amd64.deb
   - gvtap-ipsec_**1.8-5**_amd64.deb
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.
4. Install the G-vTAP Agent package file:
   ```
   sudo dpkg -i gvtap-agent_1.8-5_amd64.deb
   ```
5. Modify the **/etc/gvtap-agent/gvtap-agent.conf** file to configure and register the source and destination interfaces:

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

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

   NOTE: You can view the G-vTAP log using **cat /var/log/gvtap-agent.log** command.
6. Install strongSwan:
   ```
   tar -xvf strongswan5.3.5-1ubuntu3.8_amd64-deb.tar.gz
   cd strongswan-5.3.5-1ubuntu3.8_amd64/
   sudo sh ./swan-install.sh
   ```
7. Install IPSec package:
   ```
   sudo dpkg -i gvtap-ipsec_1.8-5_amd64.deb
   ```

Install G-vTAP from Red Hat Enterprise Linux and CentOS

1. Launch RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**1.8-5**_x86_64.rpm
   - gvtap-ipsec_**1.8-5**_x86_64.rpm
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.

4. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_1.8-5_x86_64.rpm
   ```
5. Edit the gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   # sudo /etc/init.d/gvtap-agent restart
   ```
6. Install strongSwan:
   ```
   tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
   cd strongswan-5.7.1-1.el7.x86_64
   sudo sh ./swan-install.sh
   ```
7. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_1.8-5_x86_64.rpm
   ```

NOTE: You must install IPSec package after installing StrongSwan.

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

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

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

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

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

8. Install strongSwan:
   ```
   tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
   cd strongswan-5.7.1-1.el7.x86_64
   sudo sh ./swan-install.sh
   ```
9. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_1.8-5_x86_64.rpm
   ```
10. Reboot the instance.

Create Images with Agent Installed

If you want to avoid downloading and installing the G-vTAP Agents every time there is a new instance to be monitored, you can save the G-vTAP Agent running on an instance as a private AMI.

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

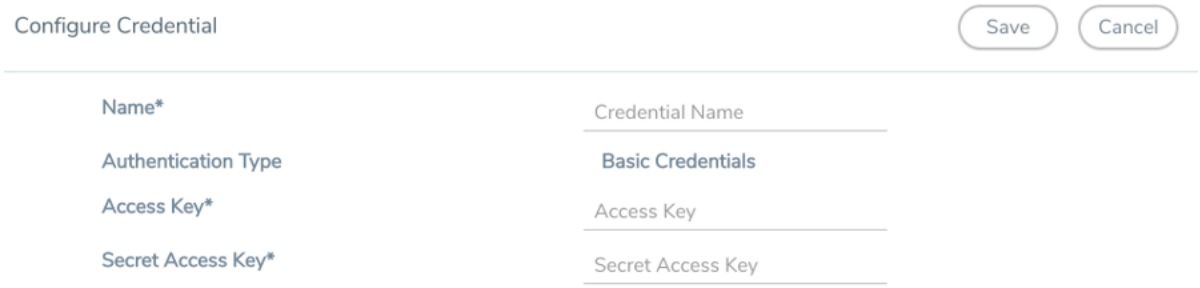
Create AWS Credentials

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. From the left navigation pane, click **Inventory > VIRTUAL > AWS > Credential**.
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

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

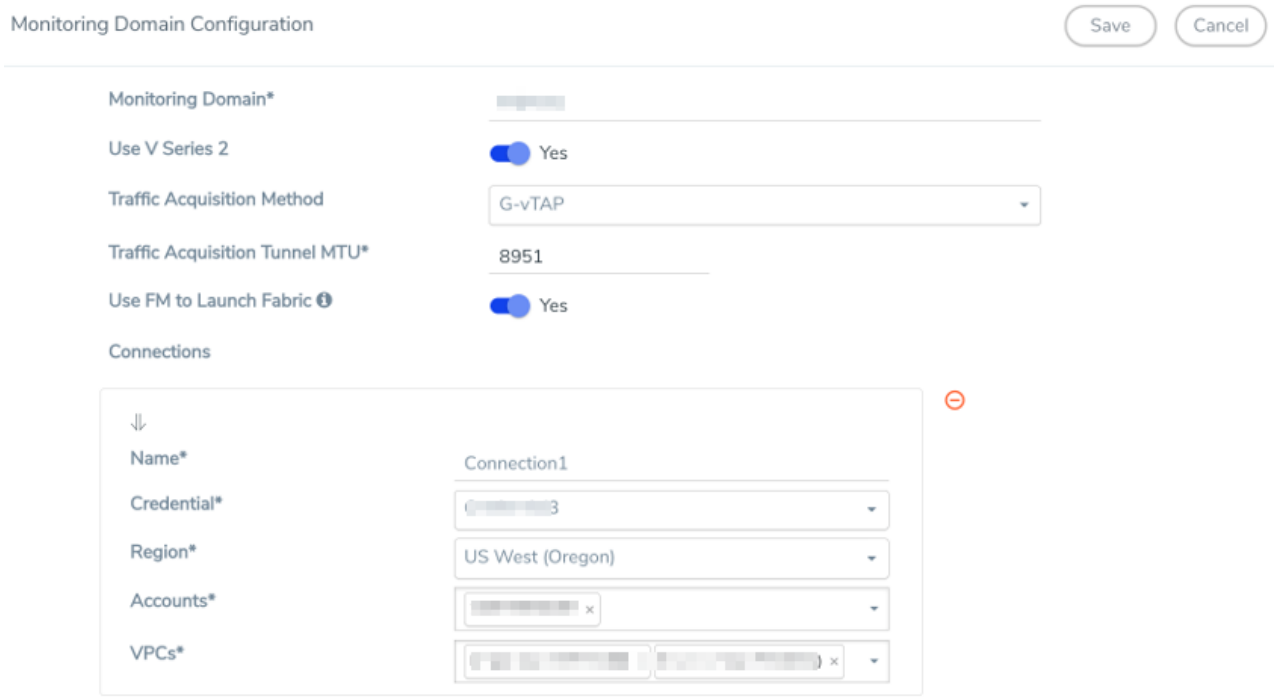
GigaVUE-FM connects to the VPC through the EC2 API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the EC2 API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

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. From the left navigation pane, click **Inventory > VIRTUAL > AWS > 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**: 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 using 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 for detailed information. • G-vTAP Controller configuration is not applicable for VPC Traffic Mirroring. • For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions 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. ▪ **Tunnel**: If you use select Tunnel as the tapping method, you can use the tunnel 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).
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. 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 NOTE: You can add multiple connections in a monitoring domain. Refer to Create AWS Credentials for more information on adding multiple AWS **Basic Credentials**.	

Field	Action
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
VPC	Select the VPCs to monitor

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

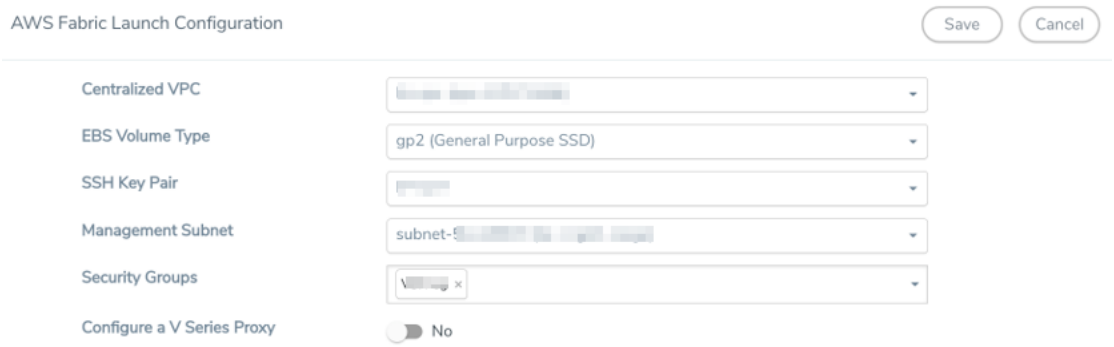
Configure GigaVUE Fabric Components in GigaVUE-FM

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:

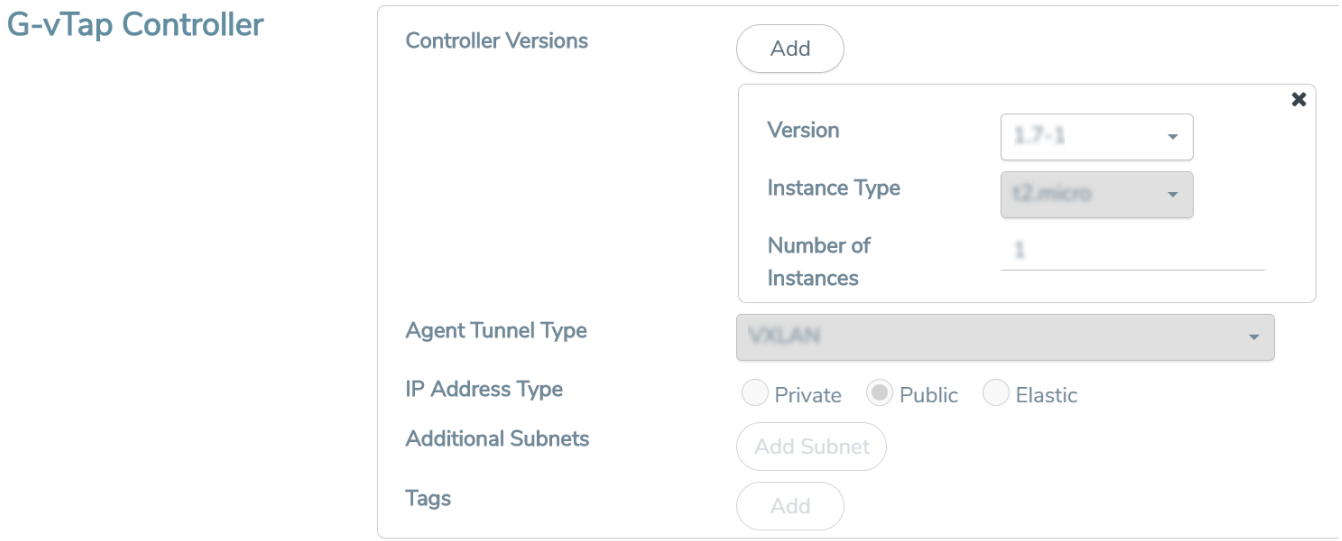
Fields	Description
	▪ gp2 (General Purpose SSD) ▪ io1 (Provisioned IOPS SSD) ▪ Standard (Magnetic).
SSH Key Pair	The SSH key pair for the GigaVUE fabric nodes. For more information on Key Pairs, refer to Key Pair.
Management Subnet	The subnet that is used for communication between the controllers and the nodes, as well as to communicate with GigaVUE-FM. This is a required field.
Security Groups	The security group created for the GigaVUE fabric nodes. For more information on security groups, refer to Security Group

Configure G-vTAP Controller

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

- 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.



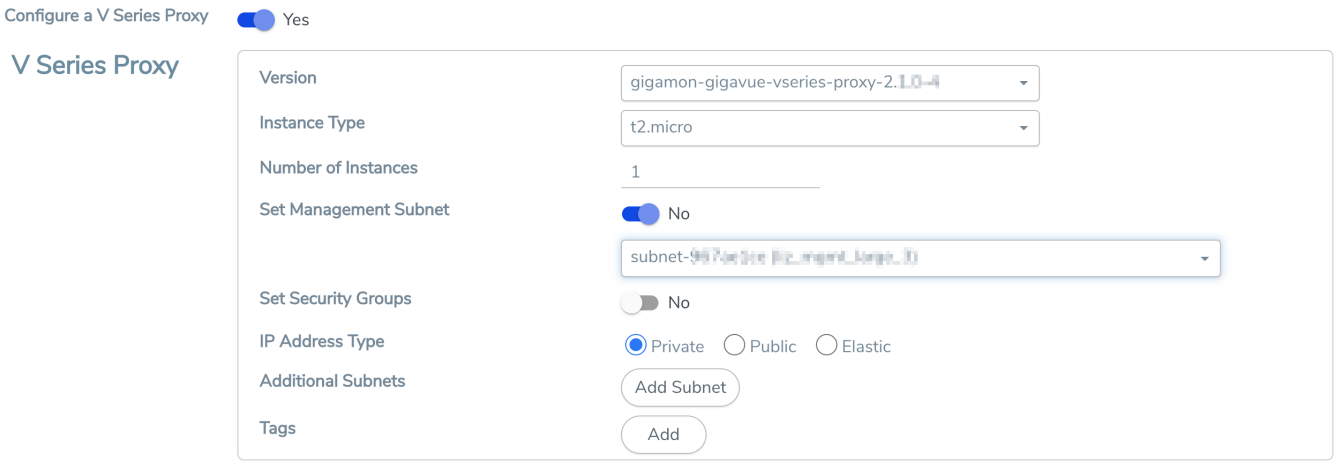
Enter or select the required information in the G-vTAP Controller section as described in the following table.

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.
Instance Type	The instance type for the G-vTAP controller. The recommended instance type is t2.micro.
Number of Instances	The number of G-vTAP Controllers to deploy in the monitoring domain.
Agent Tunnel Type	The type of tunnel used for sending the traffic from G-vTAP Agents to GigaVUE Cloud Suite 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.

Fields	Description
	▪ 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

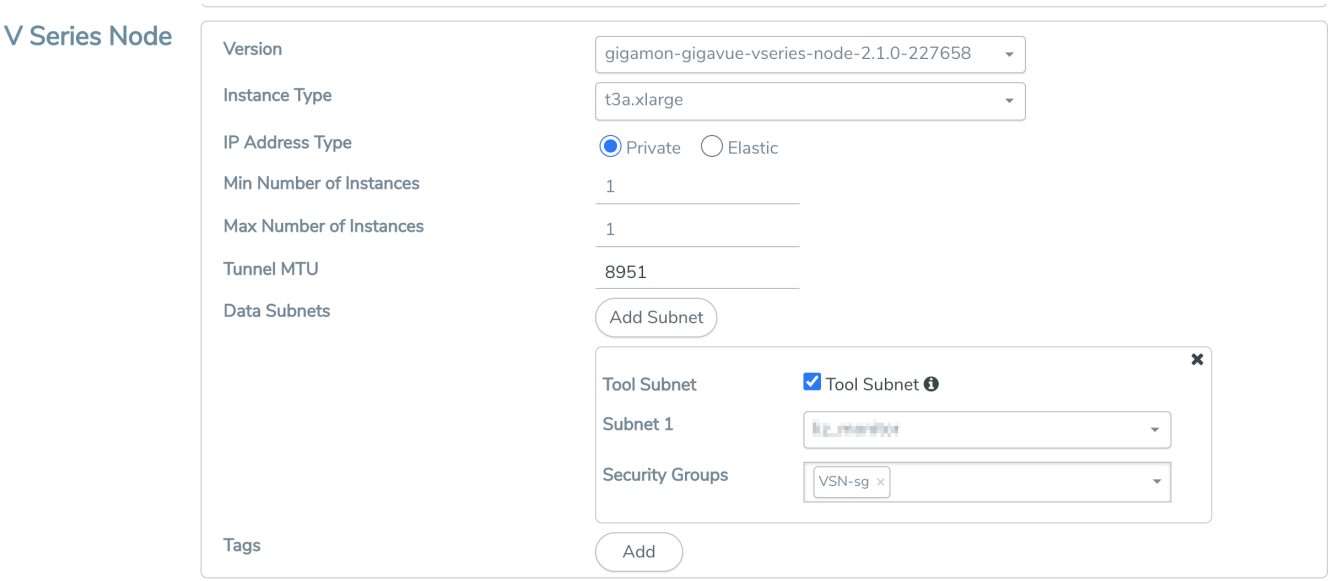
Select **Yes** for the Configure a GigaVUE V Series Proxy field. GigaVUE V Series Proxy is optional for the GigaVUE Cloud Suite for AWS.



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.

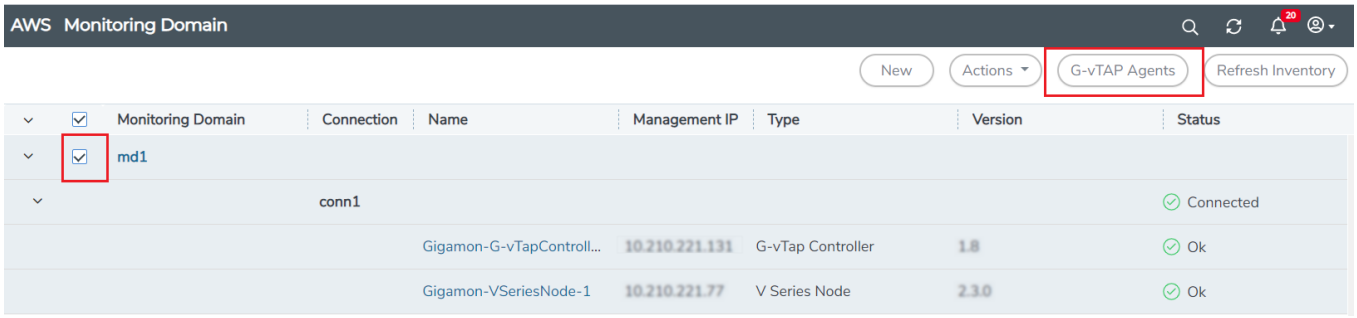
Fields	Description
Version	GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. The default instance type is nitro-based t3a.xlarge. The recommended instance type is c5n.xlarge for 4 vCPU and c5n.2xlarge for 8vcpu. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
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

Fields	Description
	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 the V Series Node to egress the aggregated/manipulated traffic to the tools.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your AWS environment. For example, you might have GigaVUE V Series Node deployed in many regions. To distinguish these GigaVUE V Series Node based on the regions, you can provide a name that is easy to identify such as us-west-2-vseries. To add a tag: a. Click **Add tag**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-vseries.

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 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.

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

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

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

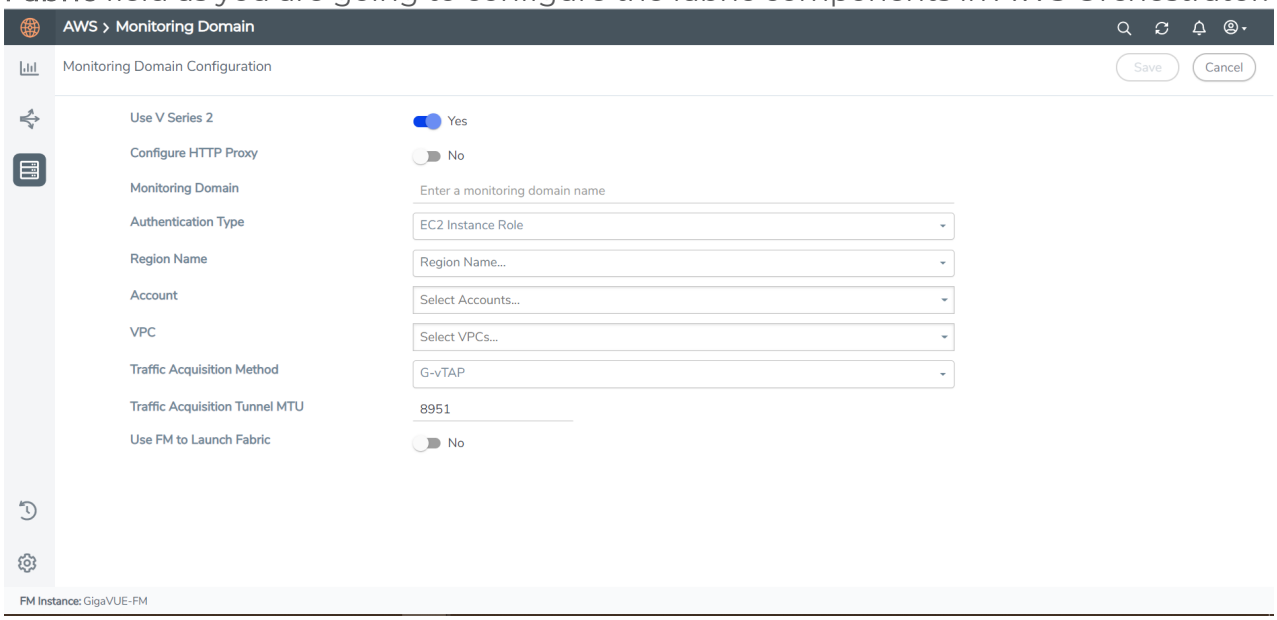
Configure V Series Nodes and V Series Proxy in AWS

To configure 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.

   > **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.



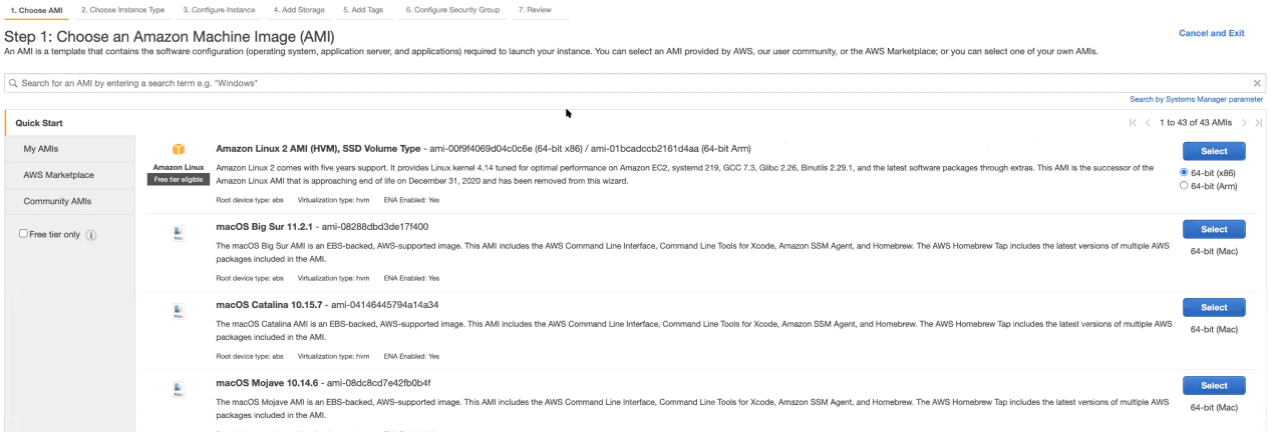
3. In your AWS environment, you can deploy V Series nodes or V Series proxy using the following methods:
   - Register V Series Nodes or Proxy using User Data
   - Register V Series Node or Proxy using a configuration file

NOTE: 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.

Register V Series Nodes or Proxy using User Data

To register 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.

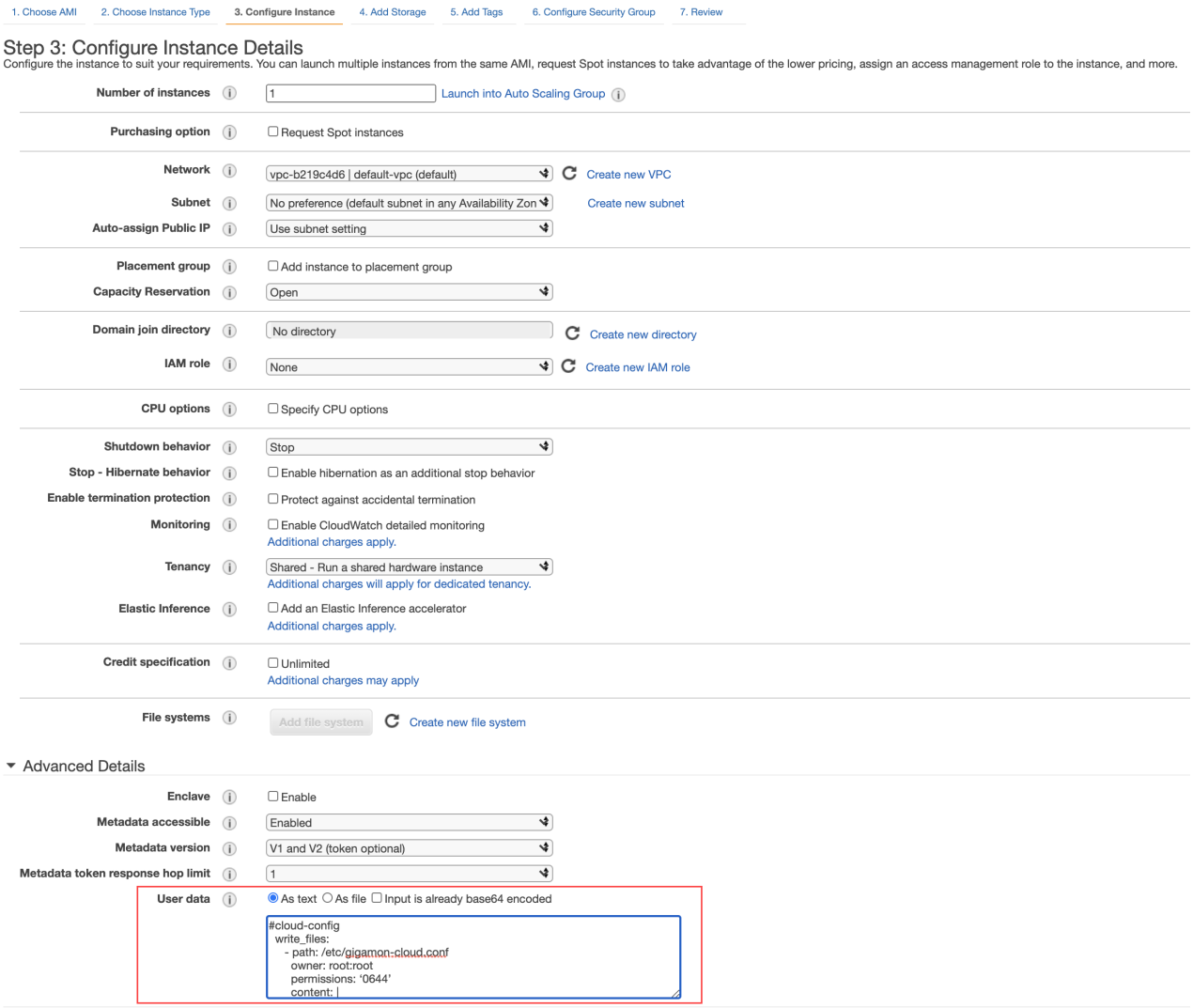


2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The V Series nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

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



Register V Series Node or Proxy using a configuration file

To register V Series Node or Proxy using a configuration file:

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

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

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

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

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

Configure G-vTAP Controller in AWS

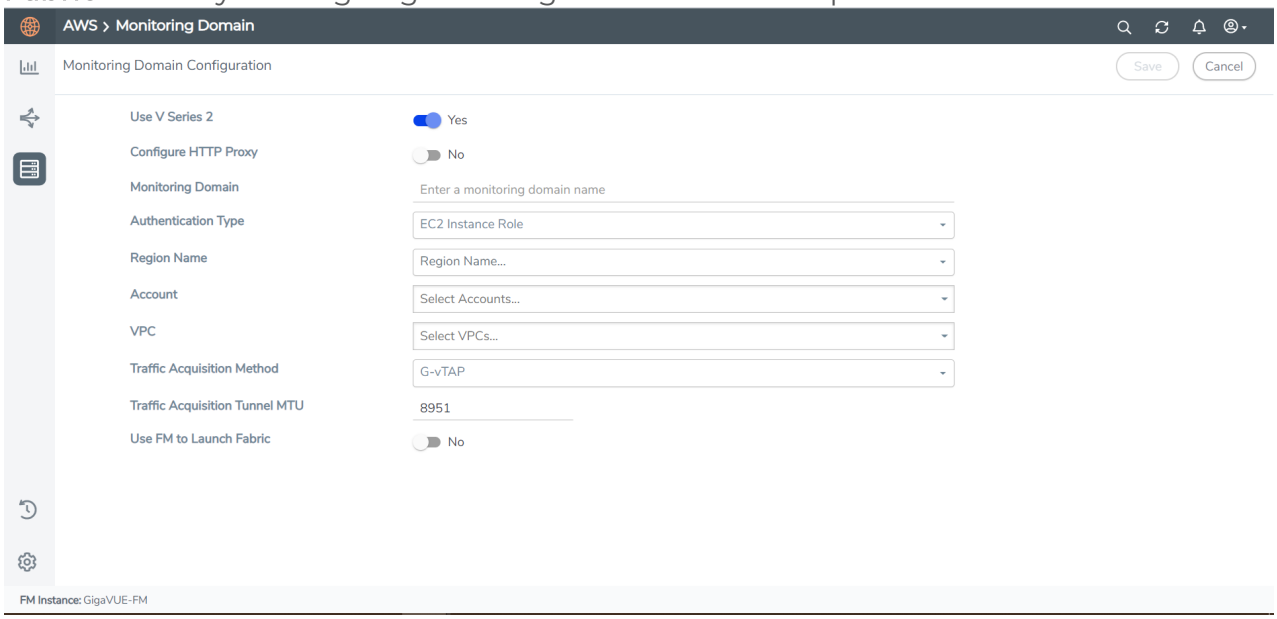
You can configure more than one G-vTAP Controller in a monitoring domain.

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.

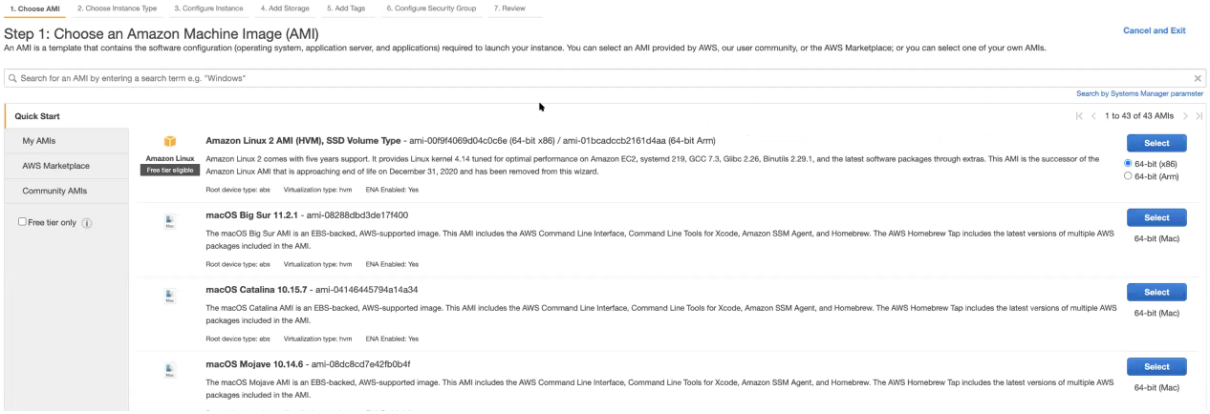


3. In your AWS environment, launch the G-vTAP Controller AMI instance using any of the following methods:
   - Register G-vTAP Controller using User Data
   - Register G-vTAP Controller using a configuration file

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.

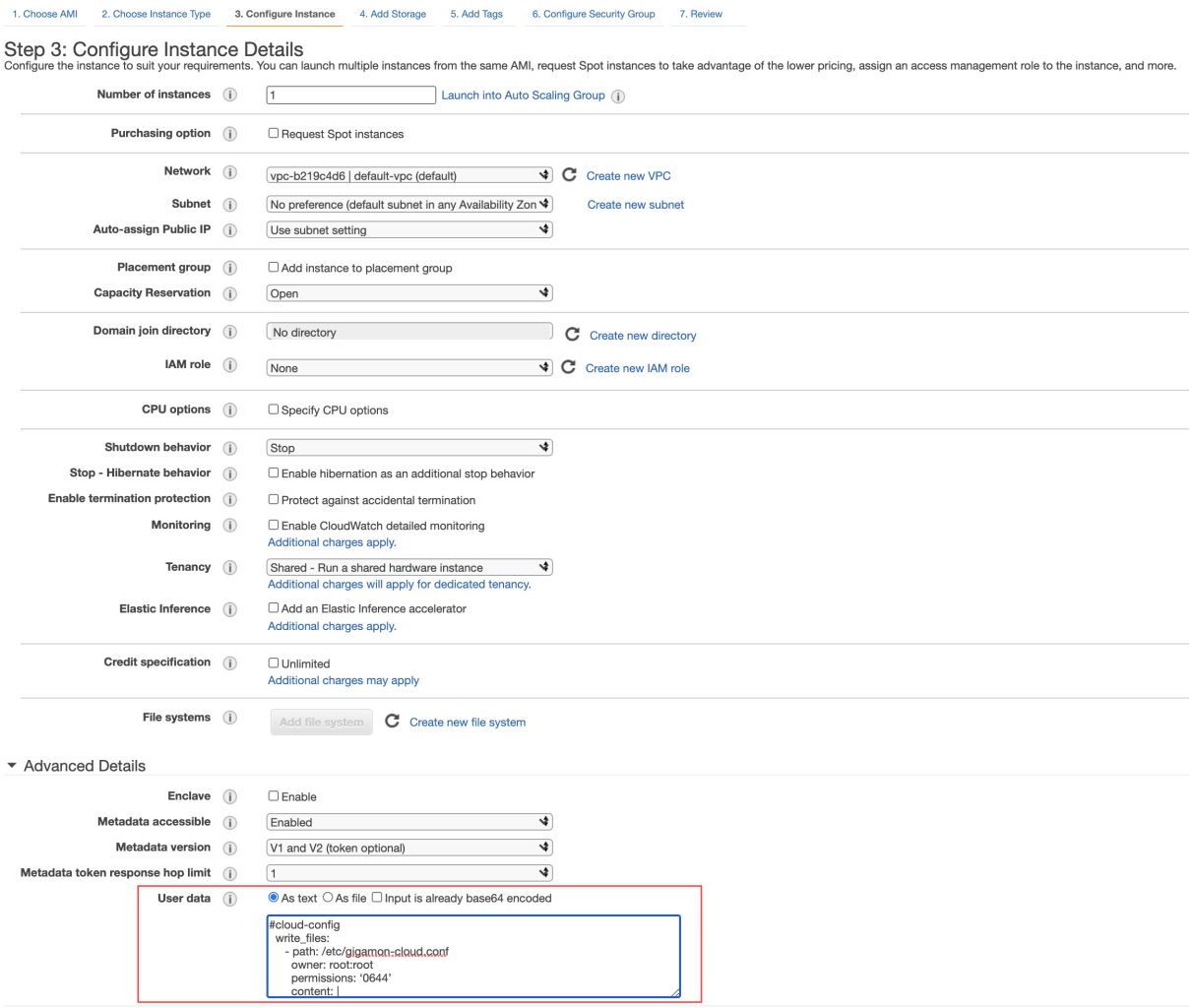


b. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The G-vTAP Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

- Use only the default **user** and **password** details given in the user data.
- If there is no monitoring domain in GigaVUE-FM with the same monitoring domain name and connection name as given in your user data, then GigaVUE-FM automatically creates a monitoring domain under AnyCloud and your V Series nodes or proxys gets deployed under that monitoring domain.
- In the above mentioned case, the Traffic Acquisition Tunnel MTU is set to the default value 1500. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** and click Save.

You can 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					
	pulkraj-vpc				Connected
		G-vTapController	34.219.250.141	1.7-304	Ok
		Gigamon-VSeriesProxy-1	34.211.211.49	2.1.0	Ok
		Gigamon-VSeriesNode-1	172.30.24.188	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: <Connection Name>
        user: orchestration
        password: orchestration123A!
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

c. Restart the G-vTAP Controller service.

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

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

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

Configure G-vTAP Agent in AWS

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

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

To register G-vTAP Agent using a configuration file:

1. Install the G-vTAP Agent in the Linux or Windows platform. For detailed instructions, refer to Linux G-vTAP Agent Installation and Windows G-vTAP Agent Installation.
2. Log in to the G-vTAP Agent.

3. Edit the local configuration file and enter the following user data.

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

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

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

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

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

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

Configure an External Load Balancer

You can use your own load balancer to uniformly distribute the traffic from AWS target VMs to V Series 2 nodes. The load balancer distributes the traffic to the V Series 2 nodes and the GigaVUE-FM auto-scales the 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 V Series 2 nodes and the AWS Auto Scaling group monitors the load of all V Series nodes. AWS Auto Scaling group can add or remove nodes if the traffic load is heavy or low.

You can configure an external load balancer through AWS and GigaVUE-FM, Refer to the following sections for more details:

- Configure an external load balancer in AWS
- Configure an external load balancer in GigaVUE-FM

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 (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 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.
   f. Add required number of Network Interfaces.

   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.

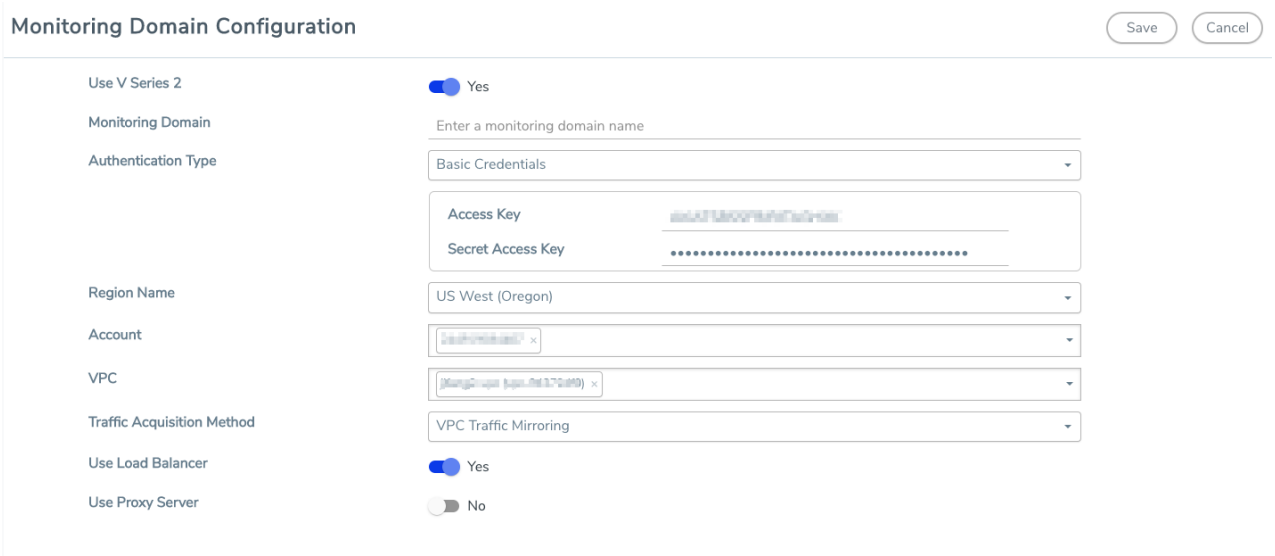
> **NOTE:** For detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in the AWS EC2 Auto Scaling document.

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

Configure an external load balancer in GigaVUE-FM

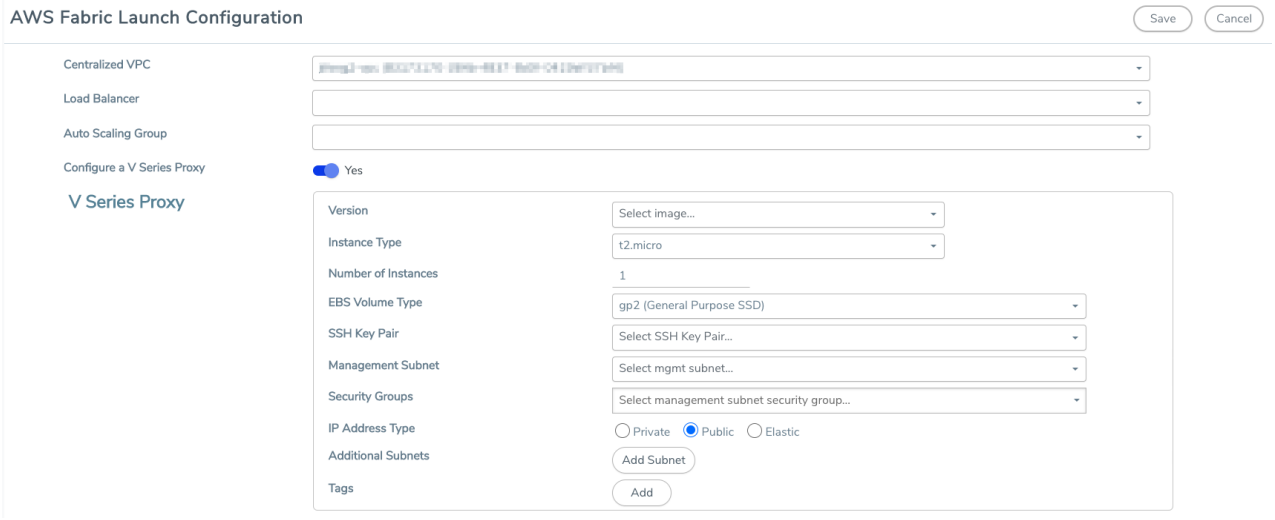
To configure an external load balancer in GigaVUE-FM:

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.

Refer Deploying Load Balancer on AWS to Scale-in and Scale-out the Gigamon Visibility Fabric for more detailed information.

Upgrade GigaVUE fabrics in GigaVUE-FM

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes. For more detailed information about 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

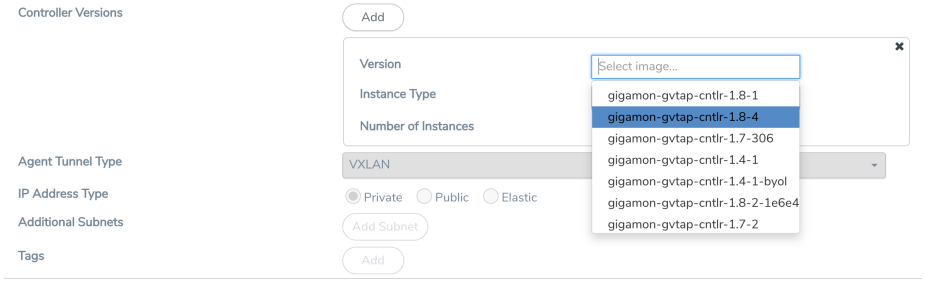
NOTE: G-vTAP Controllers cannot be upgraded. Only a new version that is compatible with the G-vTAP Agent's version can be added or removed in the **AWS Fabric Launch Configuration** page.

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.

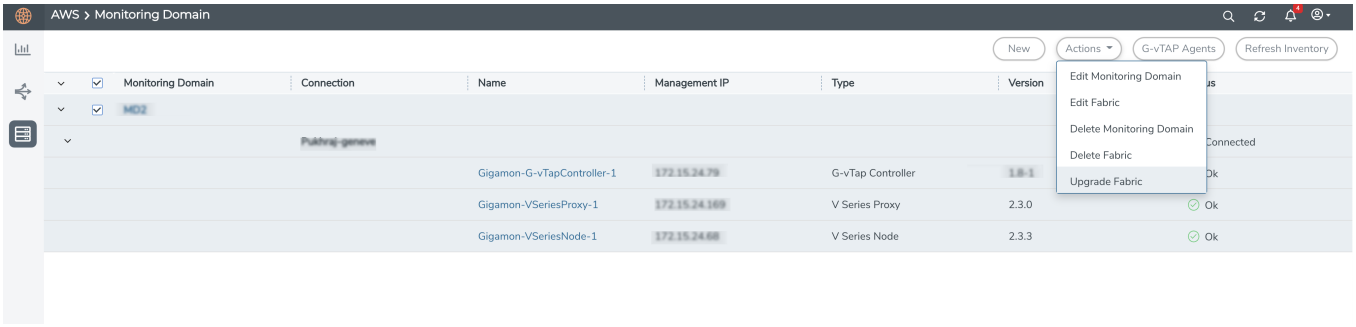
  For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes are launched. Then, the old version of V Series Proxy and Nodes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

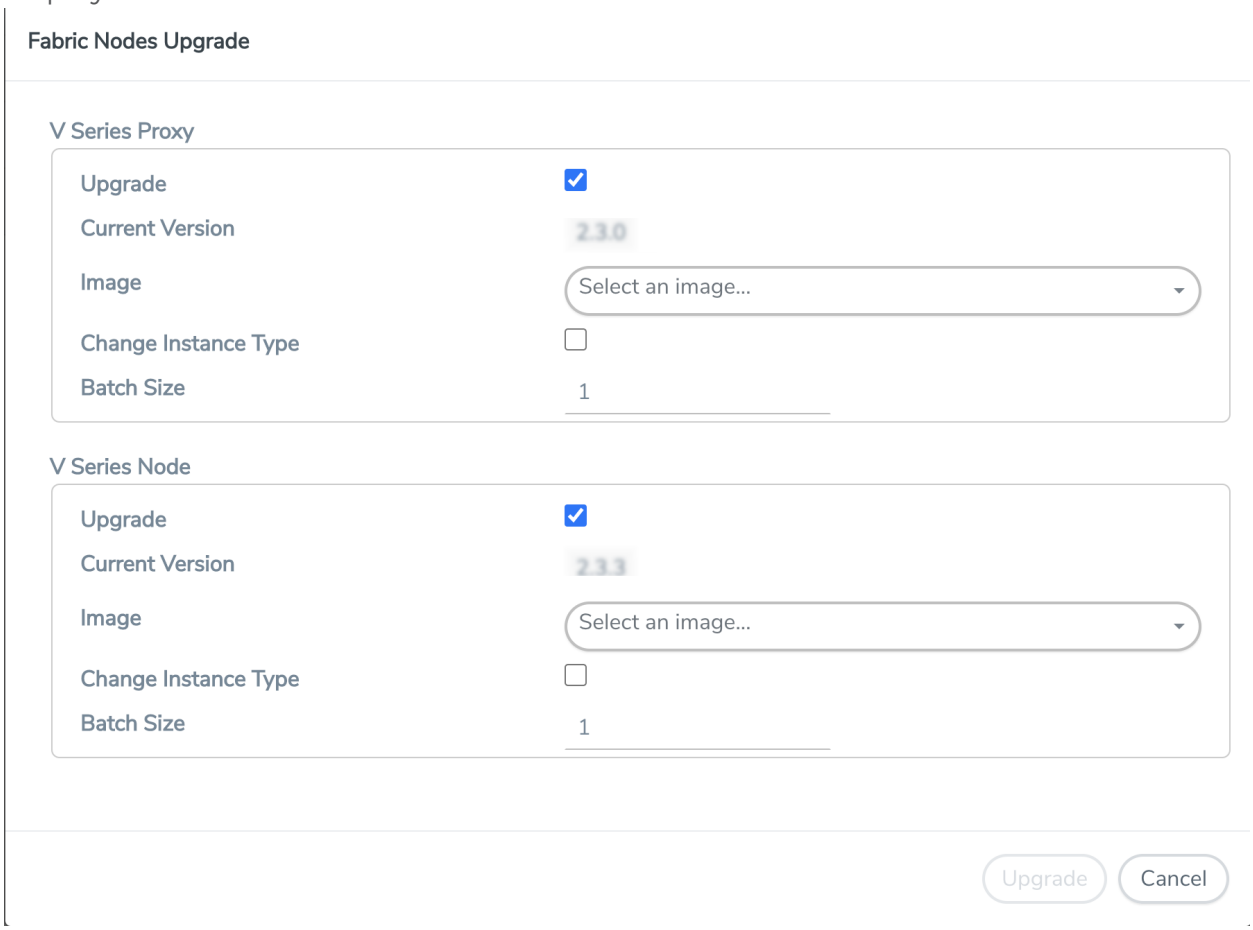
  For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

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

1. From the left navigation pane, select **Inventory > VIRTUAL > AWS > 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

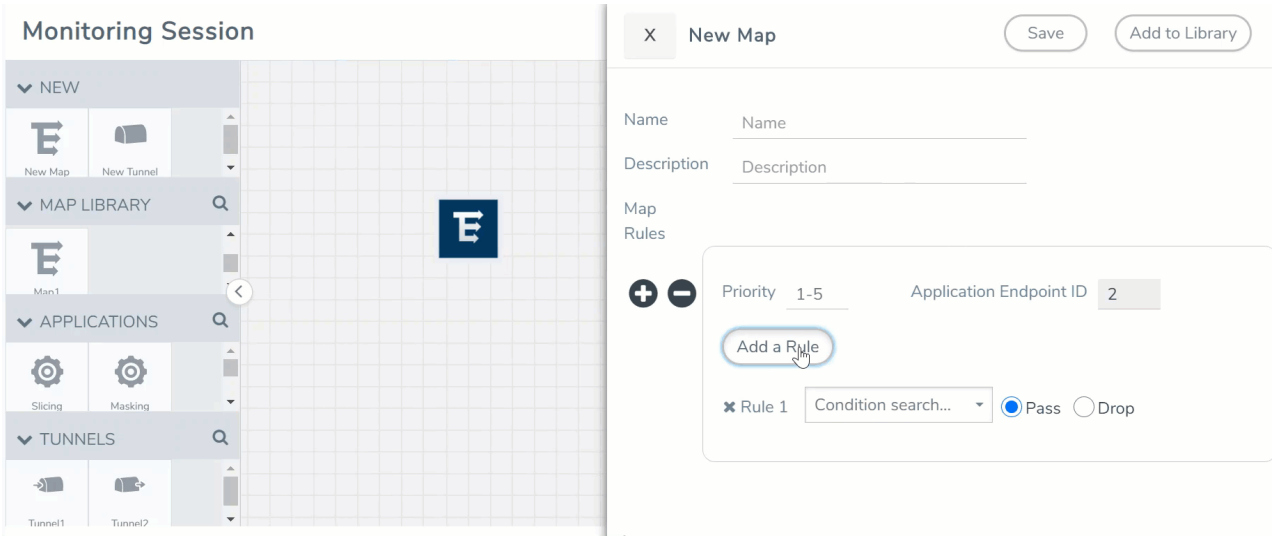
Create a New Map

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

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

To create a new map:

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



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

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

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

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

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

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

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

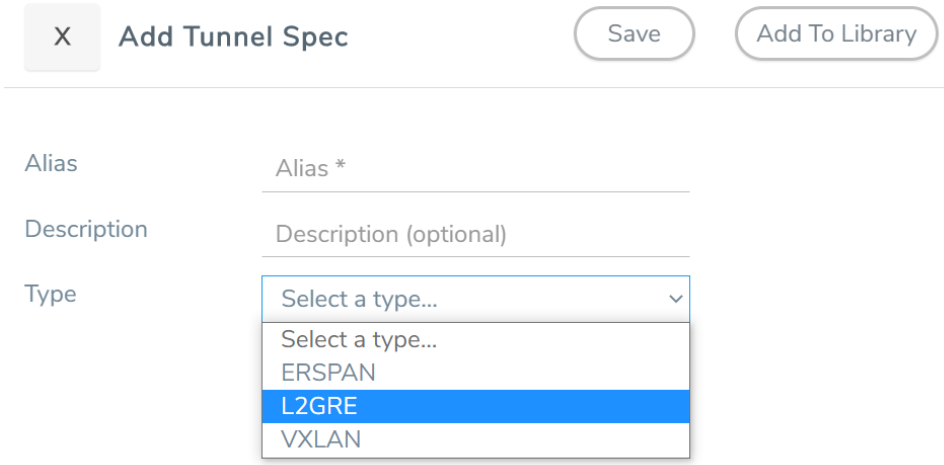
Create Ingress and Egress Tunnels

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

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

To create a new tunnel endpoint:

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



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

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

4. Click **Save**.

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

Add Applications to Monitoring Session

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

- Slicing
- Masking
- Dedup
- Load Balancing
- PCAPng
- GENEVE De-encapsulation

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

- Application Metadata Intelligence
- Application Filtering Intelligence

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

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

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

To add a GigaSMART application:

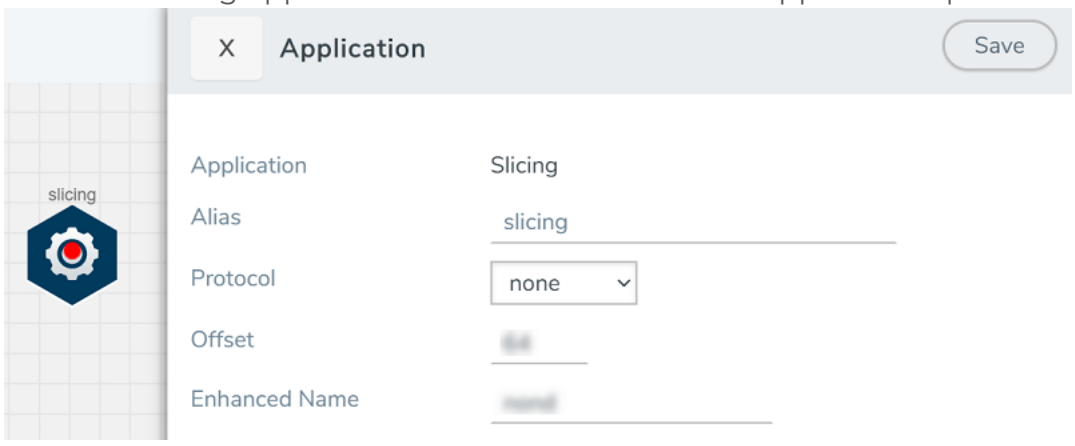
1. Drag and drop an application from **APPLICATIONS** to the canvas.
2. In the canvas, click the application and select **Details**.
3. Enter or select the required values for the selected application and click **Save**.

Slicing

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

To add a slicing application:

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



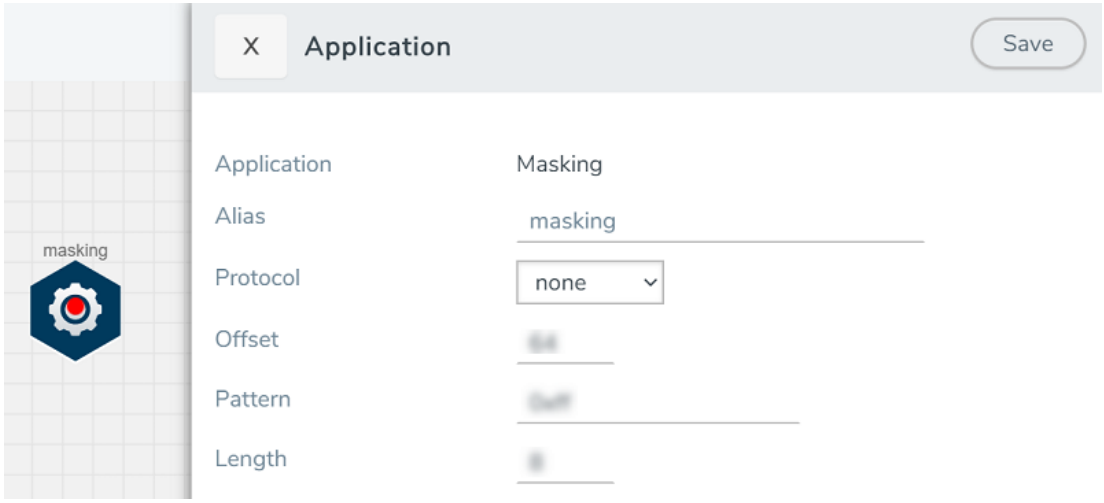
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the slicing.
   - From the **Protocol** drop-down list, specify an optional parameter for slicing the specified length of the protocol.
   - In the **Offset** field, specify the length of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

Masking

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

To add a masking application:

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



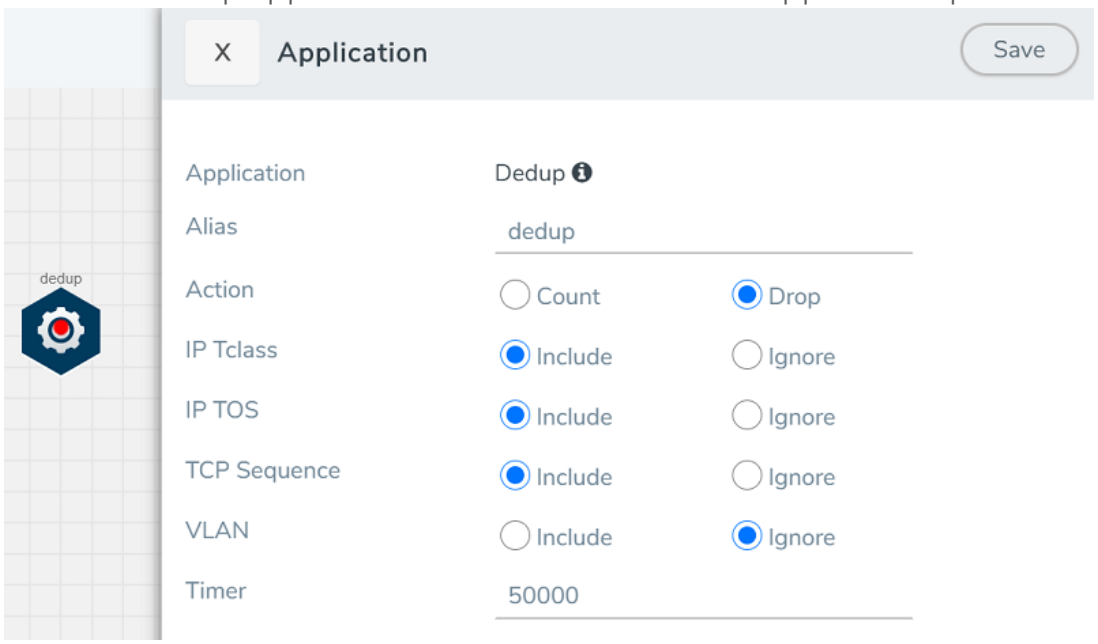
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the masking.
   - From the **Protocol** drop-down list, specify an optional parameter for masking the specified length of the protocol.
   - In the **Offset** field, specify the length of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

Dedup

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

To add a de-duplication application:

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



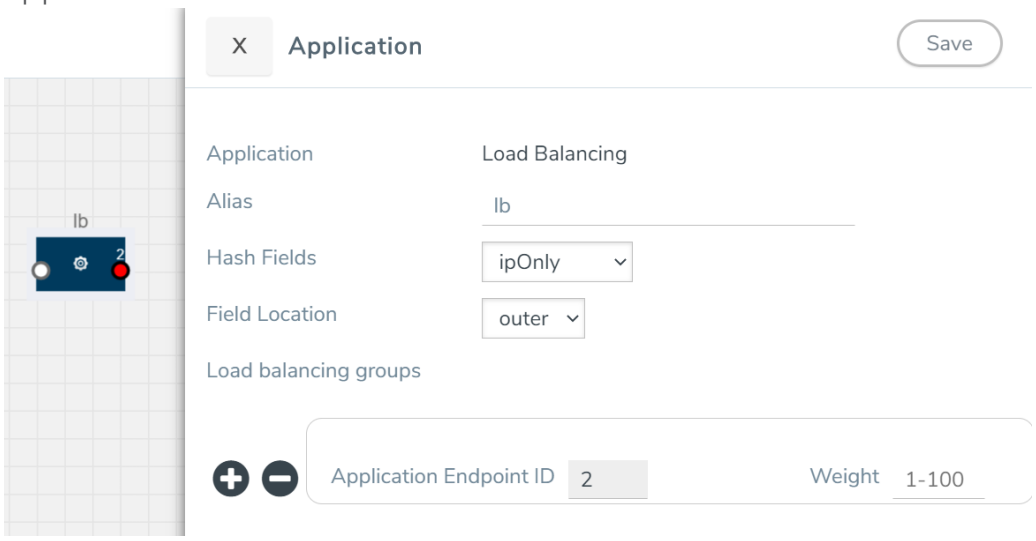
3. In the Application quick view, enter the information as follows:
   - In the **Alias** field, enter a name for the de-duplication.
   - In the Action field, select **Count** or **Drop** the detected duplicate packets.
   - For **IP Tclass**, **IP TOS**, **TCP Sequence**, and **VLAN** fields, select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

Load Balancing

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

To add a load balancing application:

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



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

     NOTE: Field location is not supported for **gtpuTeid**.
   - In the **load balancing groups**, add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.
4. Click **Save**.

PCAPng

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

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

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

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

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

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

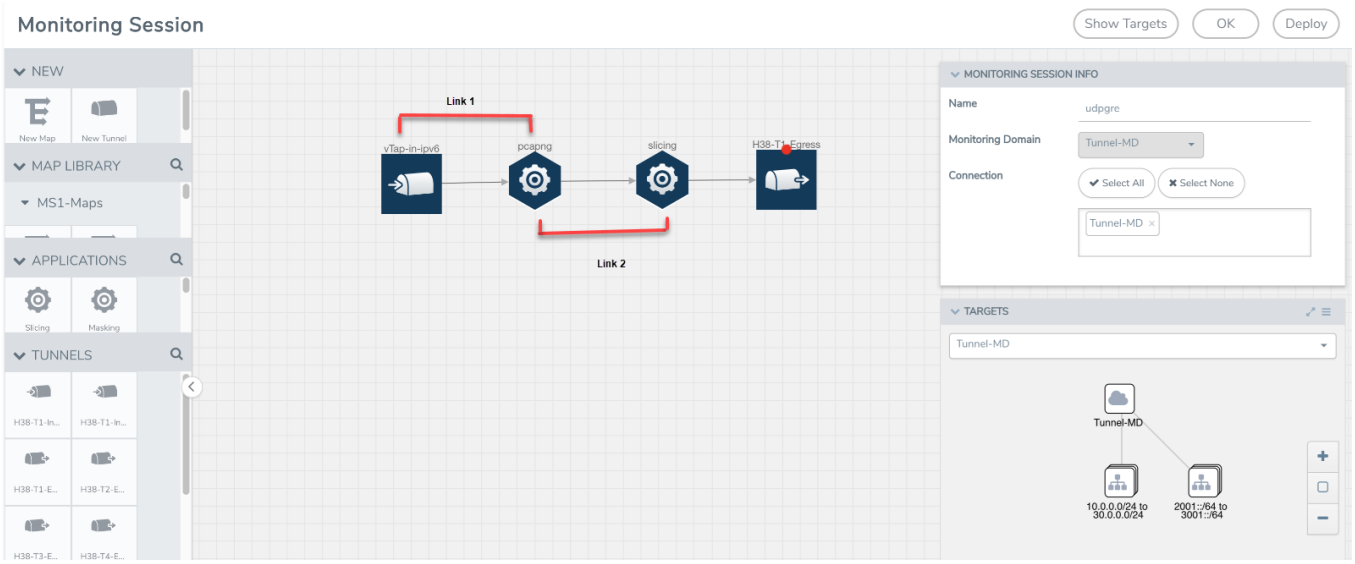
3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

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

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

Refer to the following image for a sample configuration.

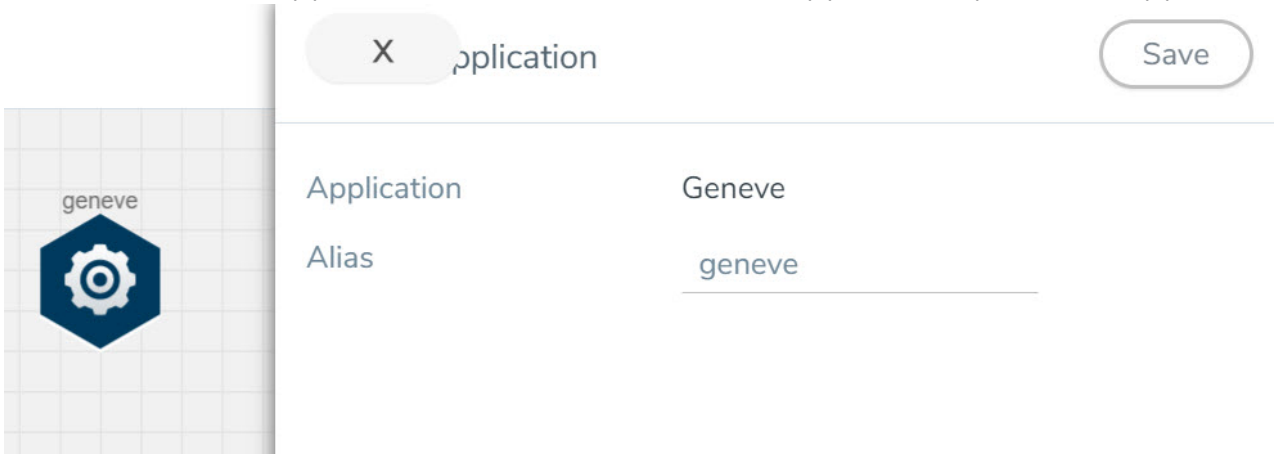


GENEVE De-encapsulation

The GENEVE De-encapsulation application is used to acquire and strip GENEVE headers. To route the traffic through the third-party network appliances seamlessly, the AWS gateway load balancer with a VPC adds GENEVE header to packets as they are forwarded to a third-party network appliance. Each appliance is expected to terminate the GENEVE tunnel and process the GENEVE encapsulated traffic traffic. When the GigaVUE-FM directs the acquisition of the customer traffic, the packets are encapsulated and forwarded as GENEVE tunnels that are terminated in GigaVUE V Series nodes.

To add a GENEVE application:

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



3. Enter an alias for the GENEVE application.
4. Click **Save**.

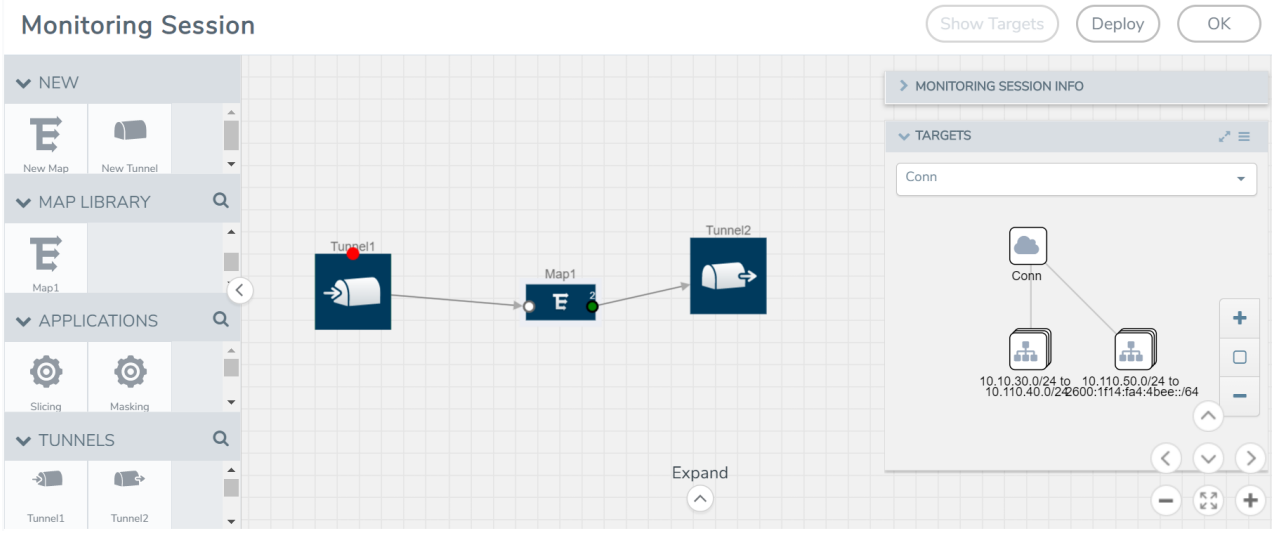
Deploy Monitoring Session

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 buttons:

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

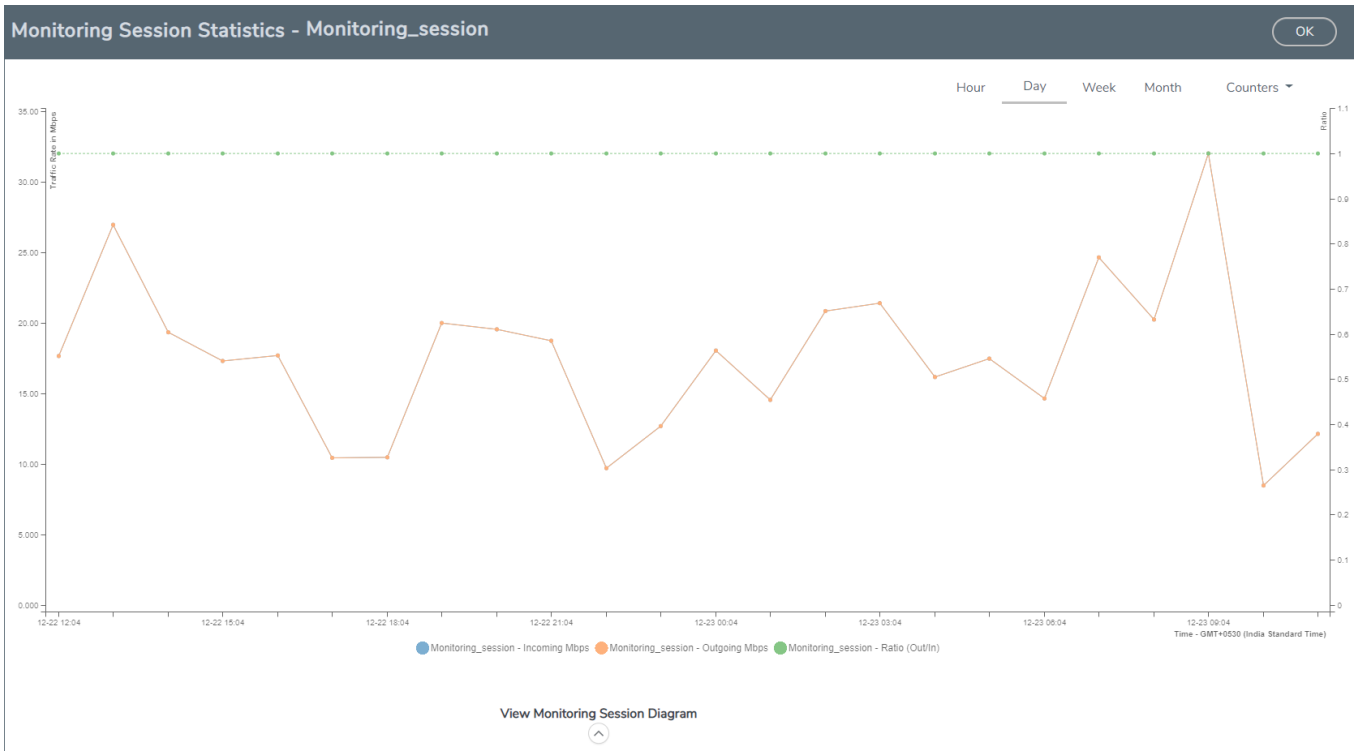
Button	Description
	again..
Delete	Deletes the selected monitoring session.

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:

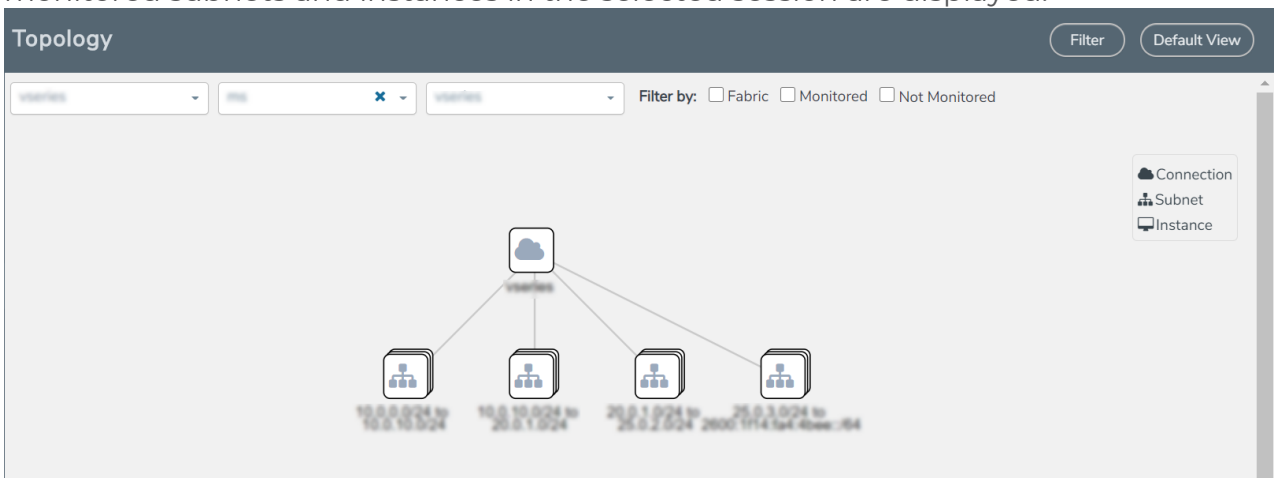
- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view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

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.

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

Administer GigaVUE Cloud Suite for AWS

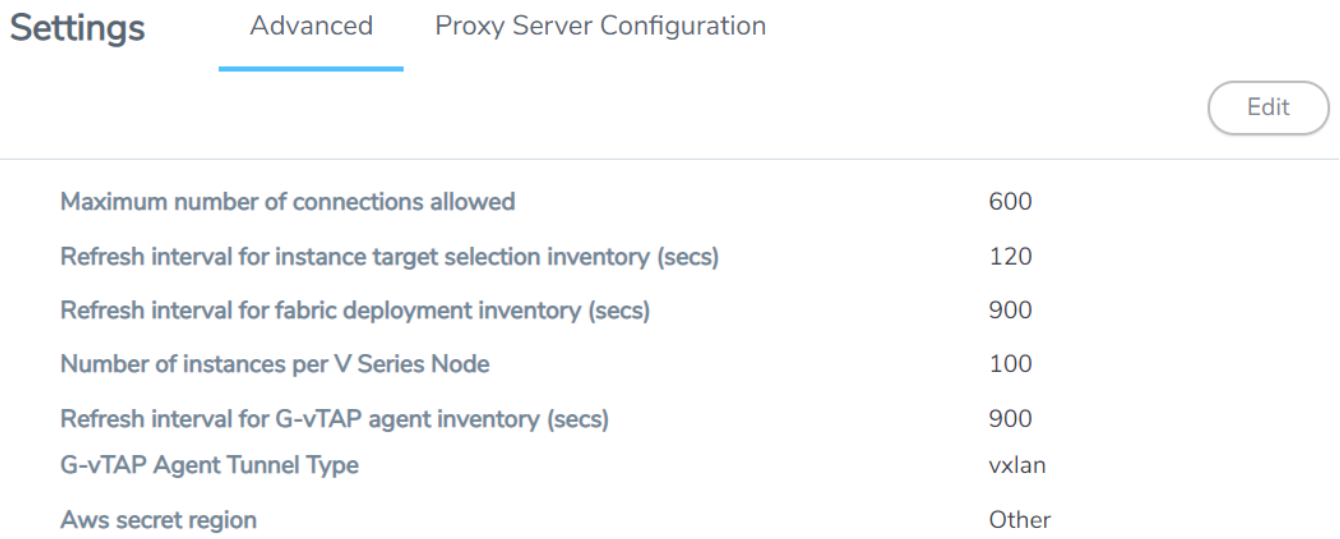
You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

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

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.

Navigate to **Inventory > VIRTUAL > AWS > Settings**.



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

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of VPC connections you can establish in GigaVUE-FM.
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of EC2 instances in AWS.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric nodes
Number of instances per V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node. You can modify the number of instances for the nitro-based instance types
Refresh interval for G-vTAP Agent inventory (secs)	Specifies the frequency for discovering the G-vTAP Agents available in the VPC.
G-vTAP Agent Tunnel Type	Specifies the G-vTAP Agent Tunnel Type
AWS secret region	Specifies the AWS secret region. The following are the available AWS secret regions: • **C2S**—Commercial Cloud Services. Refer to *GigaVUE Cloud Suite for AWS Secret Regions Guide* for more information. • **SC2S**—Secret Commercial Cloud Services. Refer to *GigaVUE Cloud Suite for AWS Secret Regions Guide* for more information. • **Other**—Regular AWS Cloud Services

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

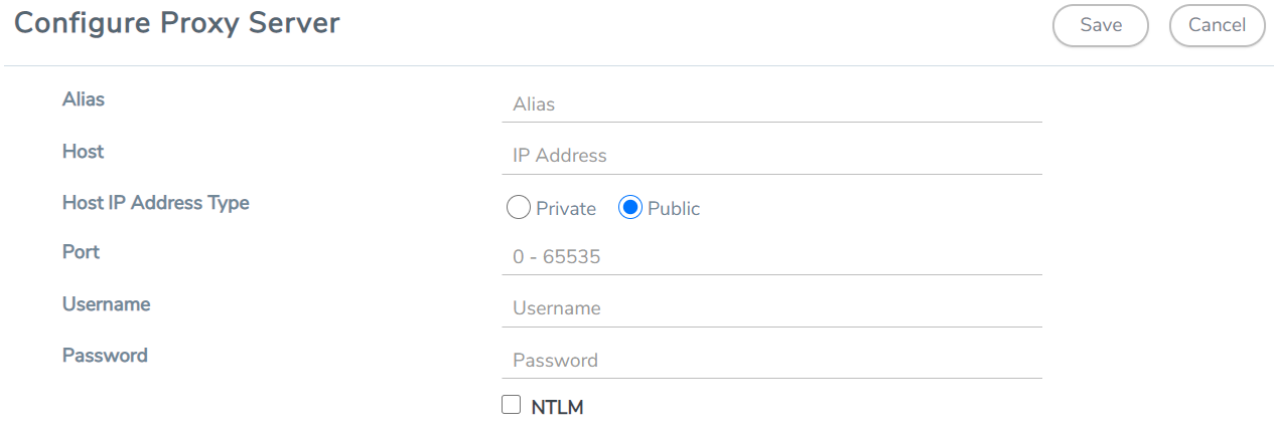
Configure Proxy Server

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. Navigate to **Inventory > VIRTUAL > AWS > 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.
Host IP Address Type	The type of the Host IP address that indicate whether the proxy server IP address is private or public to the VPC.
Port	The port number used by the proxy server for connecting to the Internet.
Username	(Optional) The username of the proxy server.
Password	The password of the proxy server.
NTLM	(Optional) The type of the proxy server used to connect to the VPC. 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 • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

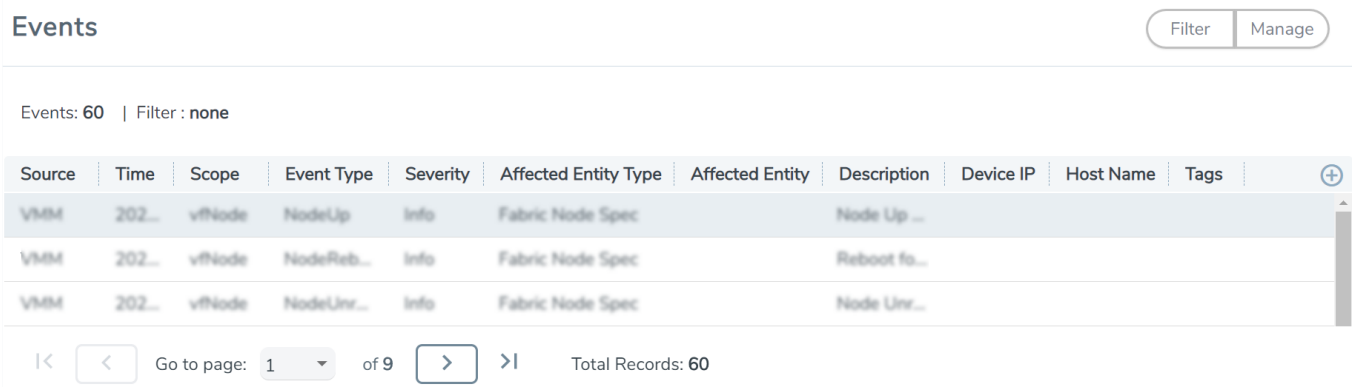
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

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

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

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

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



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

Controls/ Parameters	Description
Source	The source from where the alarms and events are generated.
Time	The timestamp when the event occurred. IMPORTANT: Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured timezone.
Scope	The category to which the alarms or events belong. Alarms and events can belong to the following category: Virtual Fabric Node, VM Domain, VM Manager.

Controls/ Parameters	Description
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.

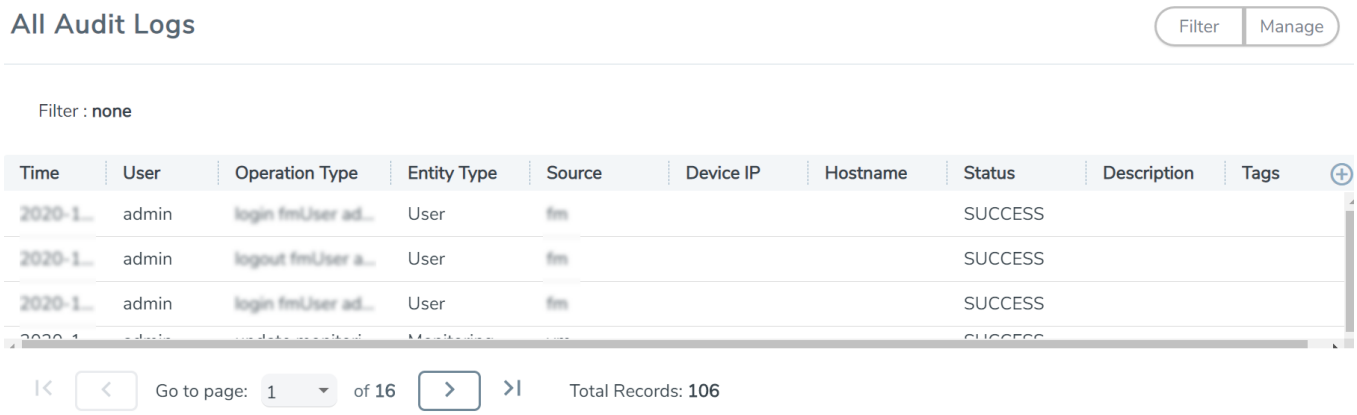
To filter the alarms and event:

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.

Parameters	Description
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.

GigaVUE-FM Version Compatibility for V Series 2 Configuration

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series 2 Nodes
5.16.00	v1.8-5	v1.8-5	v2.6.0	v2.6.0
5.15.00	v1.8-5	v1.8-5	v2.5.0	v2.5.0
5.14.00	v1.8-4	v1.8-4	v2.4.0	v2.4.0
5.13.01	v1.8-3	v1.8-3	v2.3.3	v2.3.3
5.13.00	v1.8-2	v1.8-2	v2.3.0	v2.3.0
5.12.01	v1.8-1	v1.8-1	v2.2.0	v2.2.0
5.12.00	v1.7-1	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 Gigamon Community

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

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

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

GigaVUE Cloud Suite 5.16 Hardware and Software Guides
library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release NOTE: Release Notes are not included in the online documentation. NOTE: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)