GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide

GigaVUE Cloud Suite

Product Version: 6.2

Document Version: 1.0

Last Updated: Wednesday, March 8, 2023

(See Change Notes for document updates.)

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.2.00	1.0	02/15/2023	The original release of this document with 6.2.00 GA

Contents

GigaVUE Cloud Suite for Azure–GigaVUE V Series 2

This guide describes how to install, configure and deploy the GigaVUE Cloud solution on the Microsoft® Azure cloud. Use this document for instructions on configuring the GigaVUE Cloud components and setting up the traffic monitoring sessions for the Azure Cloud.

Refer to the following sections for details:

Overview of GigaVUE Cloud Suite for Azure

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. GigaVUE-FM is a key component of the GigaVUE Cloud Suite for Azure.

GigaVUE-FM integrates with the Azure APIs and deploys the components of the GigaVUE Cloud Suite for Azure in an Azure Virtual Network (VNet).

Refer to the following sections for details:

- Components of GigaVUE Cloud Suite for Azure
- Architecture of GigaVUE Cloud Suite for Azure

Components of GigaVUE Cloud Suite for Azure

The GigaVUE Cloud Suite for Azure consists of the following components:

Component	Description

GigaVUE® Fabric Manager (GigaVUE-FM)	A web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud for Azure.
	GigaVUE-FM manages the configuration of the rest of the components in your cloud platform.
	• G-vTAP Controllers (only if you are using G-vTAP Agent as the traffic acquisition method)
	• For V Series 2 Configuration
	  • GigaVUE® V Series Proxy
	  • GigaVUE® V Series 2 nodes

G-vTAP Agents	An agent that is installed in your virtual machines. This agent mirrors the selected traffic from the virtual machines to the GigaVUE V Series node.
G-vTAP Controllers	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.
Next generation G-vTAP Agent	Next generation G-vTAP agent is a lightweight solution that acquires traffic from Virtual Machines and in-turn improves the performance of the G-vTAP agent mirroring capability. The solution has a prefiltering capability at the tap level that reduces the traffic flow from the agent to V Series node and in-turn reduces the V Series load. Next generation G-vTAP gets activated only on Linux systems with a Kernel version above 5.4. Prefiltering allows you to filter the traffic at G-vTAPs before sending it to the V Series nodes. For prefiltering the traffic, GigaVUE-FM allows you to create a prefiltering policy template and the template can be applied to a monitoring session.
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.
GigaVUE V Series nodes	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 Azure uses the standard VXLAN tunnel to deliver traffic to tool endpoints.

This solution is launched by subscribing to the GigaVUE Cloud Suite for Azure in the Azure Marketplace. Once the GigaVUE-FM is launched in Azure, the rest of the solution components are launched from GigaVUE-FM.

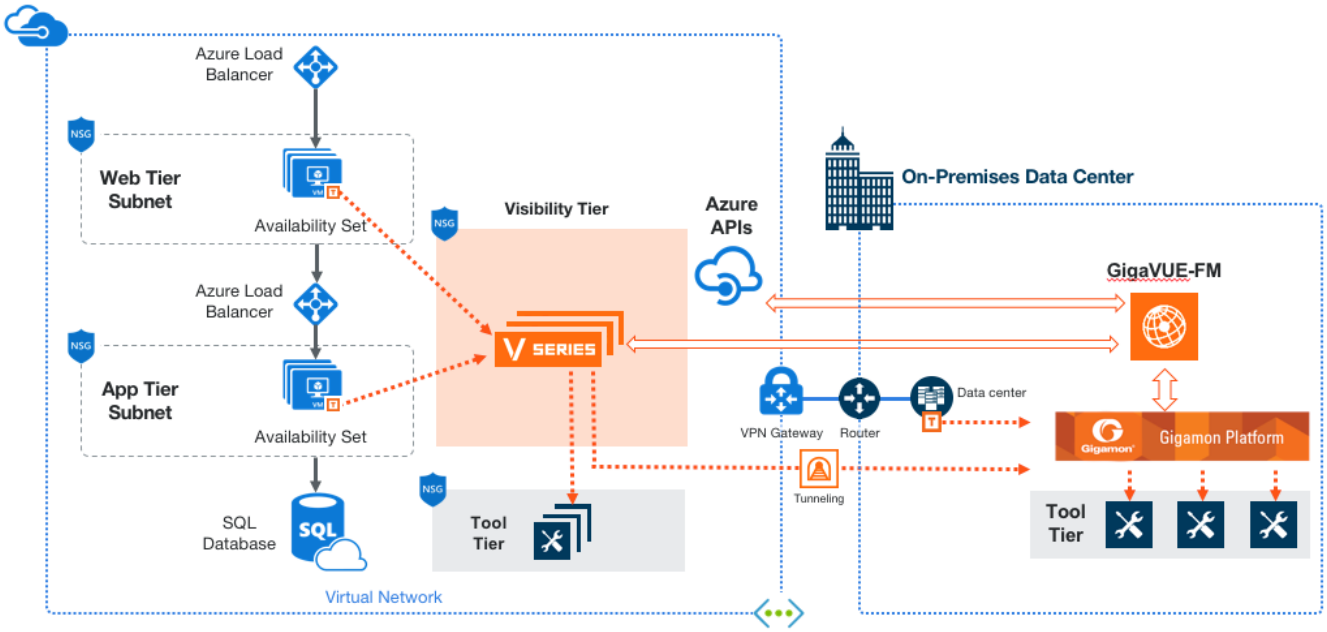
For **V Series 2 configuration**, you can only configure the GigaVUE fabric components in a Centralized VNet only. In case of a shared VNet, you must select a VNet as your Centralized VNet for GigaVUE fabric configuration.

This guide provides instructions on launching GigaVUE-FM in Azure. For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation and Upgrade Guide*.

Architecture of GigaVUE Cloud Suite for Azure

Hybrid Cloud

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



Cloud Overview Page

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms, Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

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

Virtual Dashboard Widgets

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

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

Overview

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

V Series Alarms

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

Connection Status

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

Usage

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

Summary

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

Get Started with GigaVUE Cloud Suite for Azure

This chapter describes how to plan and start the GigaVUE Cloud Suite for Azure deployment on the Microsoft® Azure cloud.

Refer to the following sections for details:

- License Information
- Before You Begin
- Install and Upgrade GigaVUE-FM

License Information

The GigaVUE Cloud Suite Cloud suite is available in both the public Azure cloud and in Azure Government, and supports the Volume Based License (VBL) model that you can avail from the Azure Marketplace.

Refer to the following topics for detailed information:

- Volume Based License (VBL)
- Apply License

Volume Based License (VBL)

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

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

Base Bundles

GigaVUE-FM has the following three base bundles:

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

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

Bundle Replacement Policy

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

Add-on Packages

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

Rules for add-on packages:

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

The list of the available add-on SKUs are:

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

How GigaVUE-FM Tracks Volume-Based License Usage

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

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

Manage Volume-Based License

To manage active Volume-Based License:

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

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

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

Use the following buttons to manage your active VBL.

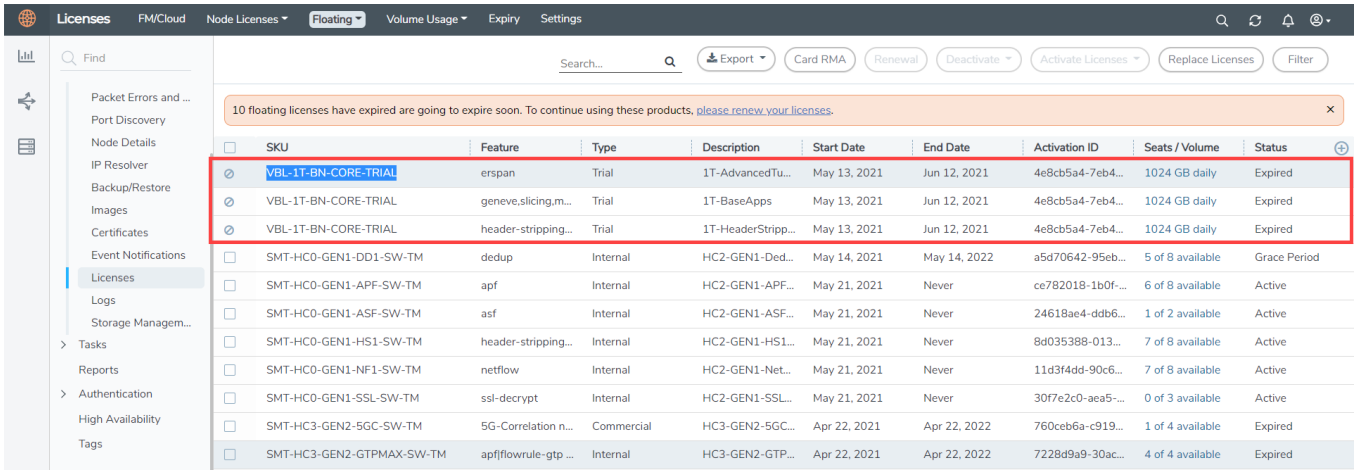
Button	Description
Activate Licenses	Use this button to activate a Volume-Based License. Refer Activate Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this option to narrow down the list of active Volume-Based Licenses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

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

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

Default Trial Licenses

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



This license includes the following applications:

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

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

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

Apply License

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

Before You Begin

You must create an account and configure a VNet as per your requirements. This section describes the requirements for launching the GigaVUE-FM VM.

- Prerequisites
- VPN Connectivity
- Obtain GigaVUE-FM Image

Prerequisites

To enable the flow of traffic between the components and the monitoring tools, you must create the following requirements:

- Resource Group
- Virtual Network
- Subnets for VNet
- Network Interfaces (NICs) for VMs
- Network Security Groups
- Virtual Network Peering
- Access control (IAM)
- Default Login Credentials

Resource Group

The resource group is a container that holds all the resources for a solution.

To create a resource group in Azure, refer to Create a resource group topic in the Azure Documentation.

Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

To create a virtual network in Azure, refer to Create a virtual network topic in the Azure Documentation.

Subnets for VNet

The following table lists the two recommended subnets that your VNet must have to configure the GigaVUE Cloud Suite Cloud components in Azure.

You can add subnets when creating a VNet or add subnets on an existing VNet. Refer to Add a subnet topic in the Azure Documentation for detailed information.

Subnet	Description
Management Subnet	Subnet that the GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data Subnet	A data subnet can accept incoming mirrored traffic from agents to the GigaVUE V Series nodes or be used to egress traffic to a tool from the GigaVUE V Series nodes. There can be multiple data subnets. ▪ Ingress is VXLAN from agents ▪ Egress is either VXLAN tunnel to tools or to GigaVUE HC Series tunnel port, or raw packets through a NAT when using NetFlow. **NOTE:** If you are using a single subnet, then the Management subnet will also be used as a Data Subnet.
Tool Subnet	A tool subnet can accept egress traffic to a tool from the GigaVUE V Series nodes. There can be only one tool subnet. ▪ Egress is either VXLAN tunnel to tools or to GigaVUE HC Series tunnel port, or raw packets through a NAT when using NetFlow.

Network Interfaces (NICs) for VMs

For G-vTAP Agents to mirror the traffic from the VMs, you must configure one or more Network Interfaces (NICs) on the VMs.

- **Single NIC**—If there is only one interface configured on the VM with the G-vTAP Agent, the G-vTAP Agent sends the mirrored traffic out using the same interface.

- **Multiple NICs**—If there are two or more interfaces configured on the VM with the G-vTAP Agent, the G-vTAP Agent monitors any number of interfaces but has an option to send the mirrored traffic out using any one of the interfaces or using a separate, non-monitored interface.

Network Security Groups

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

To create a network security group and add in Azure, refer to Create a network security group topic in the Azure Documentation.

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

In your Azure portal, select a network security group from the list. In the Settings section select the Inbound and Outbound security rules to the following rules.

Network Security Groups for V Series 2 Node

Following are the Network Firewall Requirements for V Series 2 configuration.

Direction	Type	Protocol	Port	Source/Destination	Purpose
GigaVUE-FM					
Inbound	• HTTPS • SSH	TCP	• 443 • 22	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	V Series 2 Node IP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation G-vTAP Agents to send statistics to GigaVUE-FM.
Outbound	• Custom TCP Rule • ICMP (optional)	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

Direction	Type	Protocol	Port	Source/Destination	Purpose
					with V Series Proxy
Outbound (configuration without V Series Proxy)	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate withGigaVUE V Series
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Controller to communicate with G-vTAP Agents
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Agents to communicate with G-vTAP Controller
Outbound	UDP	UDP (VXLAN)	VXLAN (default 4789)	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to VXLAN tunnel traffic to GigaVUE V Series Nodes
GigaVUE 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 withGigaVUE V Series
GigaVUE 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 withGigaVUE V Series
Inbound	UDP	UDP (VXLAN)	VXLAN (default 4789)	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN) tunnel traffic to

Direction	Type	Protocol	Port	Source/Destination	Purpose
					GigaVUE V Series Nodes
Outbound	Custom UDP Rule	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	AllowsGigaVUE V Series to communicate and tunnel traffic to the Tool
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound (optional)	ICMP	ICMP	• echo request • echo reply	Tool IP	AllowsGigaVUE V Series to health check tunnel destination traffic

Virtual Network Peering

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. Virtual Network Peering is only applicable when multiple Virtual Networks are used in a design. Refer to Virtual Network Peering topic in Azure documentation for more details.

Access control (IAM)

You must have full resource access to the control the GigaVUE Cloud Suite cloud components. Refer to Check access for a user topic in the Azure documentation for more details.

To add a role assignment, refer to Steps to assign an Azure role.

Default Login Credentials

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

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.
GigaVUE V Series proxy	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.
G-VTAP Controller	You can login to the GigaVUE V Series Node by using ssh. The default username and password is not configured.

VPN Connectivity

GigaVUE-FM requires Internet access to integrate with the public API endpoints to integrate with the GigaVUE Cloud Suite Cloud platform. If there is no Internet access, refer to Configure Proxy Server.

Obtain GigaVUE-FM Image

The image for the GigaVUE Cloud Suite Cloud is available in both the Azure Public Cloud and in the Azure Government portal.

GigaVUE Cloud Suite Cloud Suite in Azure Public Cloud

GigaVUE Cloud Suite Cloud is available in the Azure Marketplace for the Volume Based License options.

GigaVUE Cloud Suite Cloud Suite in Azure Government

Azure Government is an isolated Azure region that contains specific regulatory and compliance requirements of the US government agencies.

To monitor the VMs that contain all categories of Controlled Unclassified Information (CUI) data and sensitive government data in the Azure Government (US) Region, the Azure Government solution provides the same robust features in Azure Government as in the Azure public cloud.

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 Azure environment, you can launch the GigaVUE-FM instance in your VNet. For installing the GigaVUE-FM instance, refer to Install GigaVUE-FM on Azure.
- 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.

Deploy GigaVUE Cloud Suite for Azure

The image for the GigaVUE Cloud is available in both the Azure Public Cloud and in the Azure Government portal.

- **GigaVUE Cloud in Azure Public Cloud:** GigaVUE Cloud is available in the Azure Marketplace for Bring Your Own License (BYOL), and the Volume Based License (VBL) options.
- **GigaVUE Cloud in Azure Government:** Azure Government is an isolated Azure region that contains specific regulatory and compliance requirements of the US government agencies.

To monitor the VMs that contain all categories of Controlled Unclassified Information (CUI) data and sensitive government data in the Azure Government (US) Region, the Azure Government solution provides the same robust features in Azure Government as in the Azure public cloud.

Refer to the following topics for details:

- Deployment Options for GigaVUE Cloud Suite for Azure
- Install GigaVUE-FM on Azure
- Establish Connection to Azure
- Prepare G-vTAP Agent to Monitor Traffic
- Create Azure Credentials
- Create Monitoring Domain
- Configure GigaVUE Fabric Components in GigaVUE-FM
- Configure Role-Based Access for Third Party Orchestration
- Configure GigaVUE Fabric Components in Azure
- Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure

Refer Deploying GigaVUE Cloud Suite for Azure using V Series with Hybrid architecture for more detailed information.

Deployment Options for GigaVUE Cloud Suite for Azure

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

- Deploy GigaVUE Fabric Components using Azure
- Deploy GigaVUE Fabric Components using GigaVUE-FM
  - Traffic Acquisition Method as G-vTAP
  - Traffic Acquisition Method as Tunnel

Deploy GigaVUE Fabric Components using Azure

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

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure
3	Establish connection between GigaVUE-FM and Azure	Establish Connection to Azure
4	Install G-vTAP Agents **NOTE:** When using Azure as your orchestration system you can only use G-TAP Agents.	For Linux: Linux G-vTAP Agent Installation For Windows: Windows G-vTAP Agent Installation
5	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials
6	Create a Monitoring Domain **NOTE:** Ensure that the Use FM to Launch Fabric toggle button is disabled.	Create Monitoring Domain
7	Configure GigaVUE Fabric Components **NOTE:** Select G-vTAP as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in Azure

Step No	Task	Refer the following topics
8	Create Monitoring session	Configure Monitoring Session
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
10	Deploy Monitoring Session	Deploy Monitoring Session
11	View Monitoring Session Statistics	View Monitoring Session Statistics

Deploy GigaVUE Fabric Components using GigaVUE-FM

If you wish to deploy your fabric components using GigaVUE-FM, it can done is two ways based on the traffic acquisition method you choose.

Traffic Acquisition Method as G-vTAP

Follow instruction in the below table if you wish to use G-vTAP as your traffic acquisition method. In this case the traffic from the Virtual Machines are acquired using the G-vTAP Agents and it is sent to the GigaVUE V Series Nodes.

Step No	Task	Refer the following topics
1	Obtain GigaVUE-FM Image	Obtain GigaVUE-FM Image
2	Install GigaVUE-FM on Azure	Install GigaVUE-FM on Azure
3	Establish connection between GigaVUE-FM and Azure	Establish Connection to Azure
4	Install G-vTAP Agents	For Linux: Linux G-vTAP Agent Installation For Windows: Windows G-vTAP Agent Installation
5	Create Azure Credentials to monitor workloads across multiple Azure subscriptions	Create Azure Credentials
6	Create a Monitoring Domain **NOTE:** Ensure that the Use FM to Launch Fabric toggle button is enabled.	Create Monitoring Domain
7	Configure GigaVUE Fabric Components **NOTE:** Select G-vTAP as the Traffic Acquisition Method.	Configure GigaVUE Fabric Components in Azure
8	Create Monitoring session	Configure Monitoring Session
9	Add Applications to the Monitoring Session	Add Applications to Monitoring Session
10	Deploy Monitoring Session	Deploy Monitoring Session
11	View Monitoring Session Statistics	View Monitoring Session Statistics

Traffic Acquisition Method as Tunnel

Follow instruction in the below table if you wish to use Tunnel as your traffic acquisition method. In this case you can use tunnels as a source where the traffic is directly tunneled to V Series nodes without deploying G-vTAP Agents or G-vTAP controllers.

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

Install GigaVUE-FM on Azure

The GigaVUE-FM can be launched from the Azure VM dashboard or Azure Marketplace. The following instructions describes how to launch GigaVUE-FM in your VNet from the Azure VM Dashboard. Refer to Create a Linux virtual machine in the Azure topics in Azure Documentation for more information.

In the **Virtual Machines** page, click **Create** to create an Azure Virtual Machine. The following table describes the important fields.

Parameter	Description
Basics	
Subscription	Select your subscription.
Resource Group	Select an existing resource group or create a new resource group. For more information, refer to Create a resource group topic in the Azure Documentation.

Parameter	Description
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Image	Select the latest GigaVUE-FM images. **NOTE:** You cannot select multiple images for a VM. Refer to Configure GigaVUE Fabric Components in Azure for more details on configuring GigaVUE V Series Node, GigaVUE V Series Proxy, and G-vTAP Controller in Azure.
Size	For V Series 2 configuration, the recommended instance types are as follows: • GigaVUE-FM - **Standard_D4s_v3** • G-vTAP Controller - **Standard_B1ms** • V Series Node - **Standard_D4s_v4** • V Series Proxy - **Standard_B1ms**
	For the V Series 1 configuration, the recommended instance types are as follows: • GigaVUE-FM - **Standard_DS2_v2** • G-vTAP Controller - **Standard_B1s** • V Series Node - **Standard_DS2_v2** • V Series Controller - **Standard_B1s**
Authentication Type	Select an authentication type. • SSH public key o Enter the administrator username for the VM. o Enter the SSH public key pair name. • Password o Enter the administrator username for the VM. o Enter the administrator password.
Disks	
Disk Size	The required disk size for GigaVUE-FM is **2 x 40GB**.
Networking	
Virtual Network	Select an existing VNet or create a new VNet. For more information, refer to Create a virtual network topic in the Azure Documentation. On selecting an existing VNet, the **Subnet** and the **Public IP** values are auto-populated.
Configure network security group	Select an existing network security group or create a new network security group. For more information, refer to Network Security Groups. Configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components.

> **NOTE:** Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the VM deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in Azure, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

Establish Connection to Azure

When you first connect GigaVUE-FM to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for GigaVUE-FM to integrate with Azure APIs and to automate the fabric deployment and management. GigaVUE-FM supports two types of authentications with Azure.

Refer to the following topics.

- Managed Identity (recommended)
- Application ID with client secret
- Accept EULA and Enable Programmatic Deployment in Azure

Managed Identity (recommended)

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.Enable MSI for the GigaVUE-FM VM by using the Azure CLI command:

az vm assign-identity -g <Resource group where FM is deployed> -n <GigaVUE-FM name>

The above command enables MSI for the GigaVUE-FM for the entire subscription. If more restrictions are needed, use "**-scope <resource group id>**" as an extension to the command to restrict the MSI permissions for GigaVUE-FM to a resource group.

> **NOTE:** It may take up to 10 minutes or more for Azure to propagate the permissions. GigaVUE-FM will fail during this time to connect to Azure.

Managed Identity (MSI) is only available when GigaVUE-FM is launched inside Azure. If GigaVUE-FM is launched in one VNet and the GigaVUE V Series Nodes are deployed in a different VNet, then Virtual Network Peering must be configured. Refer thePrerequisites for more details on how to configure Virtual Network Peering. You can run these commands in the Azure Portal in an cloud shell (icon in upper right of portal as seen here): 

There are 2 steps to have MSI work:

1. Enable MSI on the VM running in GigaVUE-FM.
2. Assign permissions to this VM on all the resources where you need GigaVUE-FM to manage.

Enable MSI on the VM running GigaVUE-FM

NOTE: If you are using an older CLI version, the command "az vm assign-identity" is replaced with the new command: "az vm identity assign"

1. Launch the GigaVUE-FM Virtual Machine in Azure.
2. Enable MSI and Assign roles to the VM. You can use the CLI or portal to enable MSI and assign roles to VMS.

Enable MSI using the CLI

1. Assign a custom role at resource group level where you will deploy the fabric:

   ```
   az vm identity assign -g xxx-fm-feb15 -n xxx-fm-feb15 --role "FM Custom Role RG Level" --scope /subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/xxxz-rg
   ```

2. If you need the private images, then you have to assign permissions to the resource group of the fabrics. Therefore run this:

   ```
   az vm identity assign -g xxx-fm-feb15 -n xxx-fm-feb15 --role "FM Custom Role RG Level"--scope /subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/vseries-rg
   ```

   ```
   az vm identity assign -g xxx-fm-feb15 -n xxx-fm-feb15 --role "FM Custom Role RG Level"--scope /subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/gvtap-rg
   ```

3. Assign a custom role at the subscription level to view the complete account details:

   ```
   az vm identity assign -g xxx-feb8-fm -n xxx-feb8-fm --role "FM Custom Role Subscription Level" --scope /subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111
   ```

For more information, refer to Configure managed identities for Azure resources using Azure CLI topic in the Azure Documentation.

Enable MSI Using the Portal

You can enable MSI at the time of launch or after the launch of GigaVUE-FM through the portal.

For more information, refer to the following topics in the Azure Documentation:

- Create, list, delete, or assign a role to a user-assigned managed identity
- Assign Azure roles

Application ID with client secret

GigaVUE-FM supports application id with client secret authentication. When using GigaVUE-FM to connect to Azure, it uses a service principal. A service principal is an account for a non-human such as an application to connect to Azure. The key fields required for GigaVUE-FM to connect to Azure are Subscription ID, Tenant ID, Application ID, and Application Secret. When GigaVUE-FM is launched out Azure, Application ID with client secret is prefered.

- When creating the service principal using the Azure CLI, the output of that command will display the "appId" and "password" fields. These two are the Application ID and Application Secret fields that are required for GigaVUE-FM to connect to Azure. Copy them.
- Now, using the Azure CLI again, do an 'account show' command and copy the Subscription ID and the Tenant ID of your subscription.

The GigaVUE-FM to Azure connection supports application id with client secret authentication. When using GigaVUE-FM to connect to Azure, it uses a service principal. A service principal is an account for a non-human such as an application to connect to Azure.

GigaVUE-FM must be able to access the URLs listed in the Allow the Azure portal URLs on your firewall or proxy server in order to connect to Azure.
Following are the required endpoints for Azure GovCloud:

- authentication_endpoint = https://login.microsoftonline.us/
- azure_endpoint = https://management.usgovcloudapi.net/

To create a service principal in Azure, refer to the following topics in the Azure Documentation:

- Create an Azure service principal with the Azure CLI
- Create an Azure service principal with Azure PowerShell
- Create an Azure service principal with Azure Portal

Custom Roles

The 'built-in' roles provided by Microsoft are open to all resources. You can create a custom role if required.

You can create a custom role in Azure as described in the following examples. The "assignableScopes" are the objects which this role is allowed to be assigned. In the example below, for the RG level role, you can assign permissions for GigaVUE-FM to access your resource group and also two other resource groups where the GigaVUE V Series proxy/controller and G-vTAP controllers are placed. Without the GigaVUE V Series proxy/controller and G-vTAP controllers you would only see images in the marketplace.

For more information, refer to Azure custom roles topic in the Azure Documentation.

Using CLI:

```
az role definition create --role-definition FM-custom-role-azure-RG-level.json
```

This section provides examples of the JSON file above.The assignable scopes can be at the Resource Group level, or at the entire Subscription level. This is defined in that JSON file.

Example: Custom Role at Resource Group Level

The following is an example of what you need at RG level:

```
{
"Name": "FM Custom Role RG Level",
"IsCustom": true,
"Description": "Minimum permissions for FM to operate",
"Actions": [
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/powerOff/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/instanceView/read",
"Microsoft.Compute/locations/vmSizes/read",
"Microsoft.Compute/images/read",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/publicIPAddresses/read",
```

```
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/publicIPAddresses/read ",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
],
"NotActions": [

],
"AssignableScopes": [
"/subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/xxxz-rg",
"/subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/vseries-
rg",
"/subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/gvtap-rg"
]
}
```

Example: Custom Role for Subscription Level

The following is an example of what you need at the Subscription level:

```
"Name": "FM Custom Role Subscription Level",
"IsCustom": true,
"Description": "Minimum permissions for FM to operate at a subscription level",
"Actions": [
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/powerOff/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/instanceView/read",
"Microsoft.Compute/locations/vmSizes/read",
```

```
"Microsoft.Compute/images/read",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/publicIPAddresses/read ",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
 "Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
],
"NotActions": [

],
"AssignableScopes": [
 "/subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111"
]
}
```

Add Custom Role to Subscription or Resource Group

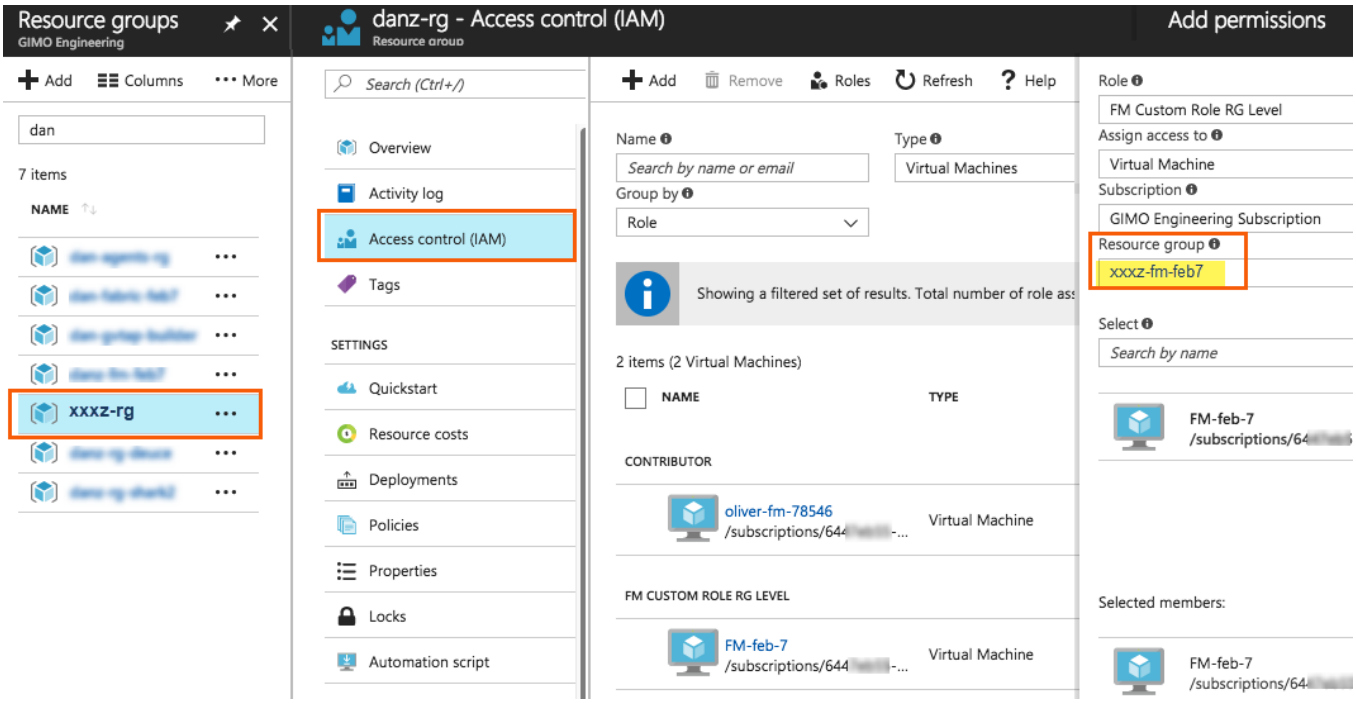
After creating the custom role, you can add the role to either the Resource Group, or at the Subscription level in the Azure console. In this example, the role is added to my Resource Group. As the GigaVUE-FM connection gets connected to the VNET in the resource Group

"xxxz-rg", the following permissions/roles are added to the Resource Group. If you want to have GigaVUE-FM create a resource group to launch fabric into, you must add these permissions to the subscription level instead.

For more information, refer to Create or update Azure custom roles in the Azure Documentation.

> **NOTE:** You are adding permissions for the GigaVUE-FM running in Azure (Virtual Machine).

In this example, GigaVUE-FM is running in another resource group "xxxz-fm-feb7". Select the VM and give the required permissions to access the other resource group "xxxz-rg":



You can also use the CLI to perform the same process. This adds the GigaVUE-FM instance in RG "xxx-feb8-fm" to have access to another RG called "xxxz-rg":

CLI to add role to Resource Group

```
az vm assign-identity -g xxx-feb8-fm -n xxx-feb8-fm --role "FM Custom Role RG
Level" --scope /subscriptions/6447xxx11-1x11-111x-11xx-
11x11xx11111/resourceGroups/xxxz-rg
```

CLI for Subscription Level

```
az vm assign-identity -g xxx-feb8-fm -n xxx-feb8-fm --role "FM Custom Role
Subscriptions Level" --scope /subscriptions/6447xxx11-1x11-111x-11xx-
11x11xx11111
```

If you want to update the Role, you can edit the JSON file, and then update the Role in Azure using the following CLI command:

update role

```
az role definition update --role-definition FM-custom-role-azure-RG-level.json
```

Pre-defined Roles

Resource groups pre-created (which the GigaVUE-FM monitors):

- Assign Reader
- Virtual Machine Contributor
- Network Contributor
- Storage Account Contributor

Resource groups created by GigaVUE-FM: Contributor on subscription level

Accept EULA and Enable Programmatic Deployment in Azure

For GigaVUE-FM to be able to launch the fabric images, you must accept the terms of the end user license agreements (EULAs) and enable programmatic access. This can be done in the Azure portal or through PowerShell.

1. **Accept the Gigamon EULAs for each SKU.** These examples show accepting the EULAs from a PowerShell terminal in the Azure Portal:
   a. HOURLY FM:

```
Azure:/
PS Azure:\> Get-AzMarketplaceTerms -Publisher "gigamon-inc" -Product
"gigamon-fm-6_XX_XX_hourly" -Name "GigaVUE Cloud Suite 6.XX.XX Hourly
(100 pack)" | Set-AzMarketplaceTerms -Accept
```

   b. BYOL FM:

```
Azure:/
PS Azure:\> Get-AzMarketplaceTerms -Publisher "gigamon-inc" -Product
"gigamon-fm-6_XX_XX" -Name "GigaVUE Cloud Suite 6.XX.XX" | Set-
AzMarketplaceTerms -Accept
```

   c. Fabric Images (need to accept on all 3):

```
Azure:/
PS Azure:\> Get-AzMarketplaceTerms -Publisher "gigamon-inc" -Product
"gigamon-fm-6_XX_XX" -Name "gvtap-cntlr" | Set-AzMarketplaceTerms -
Accept


Azure:/
PS Azure:\> Get-AzMarketplaceTerms -Publisher "gigamon-inc" -Product
"gigamon-fm-6_XX_XX" -Name "vseries-cntlr" | Set-AzMarketplaceTerms -
Accept


Azure:/
PS Azure:\> Get-AzMarketplaceTerms -Publisher "gigamon-inc" -Product
"gigamon-fm-6_XX_XX" -Name "vseries-node" | Set-AzMarketplaceTerms -
Accept
```

2. Configure programmatic deployment through the Azure portal so that GigaVUE-FM can launch these images:
   a. Find the images in the Azure Marketplace.
   b. Click the "**Want to deploy programmatically? Get started**" link.
   c. Review the terms of service and the subscription name and then click **Enable**.

DISCLAIMER: These are general guidelines for enabling a deployment in Azure. Since the Azure interface is subject to change and is outside Gigamon's purview, please see Azure documentation for instructions on using Azure.

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). This agent mirrors the selected traffic from the VMs, encapsulates it using VXLAN tunneling, and forwards it 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 VXLAN tunnel interface to the GigaVUE V Series node.

A source interface can be configured with one or more Network Interface Cards (NICs). While configuring a source interface, you can specify the direction of the traffic to be monitored in the VM. The direction of the traffic can be egress, ingress, or both.

Refer to the following sections for more information:

- Linux G-vTAP Agent Installation
- Windows Agent Installation
- Create Images with the Agent Installed

Linux G-vTAP Agent Installation

Refer to the following sections for the Linux agent installation:

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

Single NIC Configuration

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

For example, assume that there is only one interface eth0 in the monitoring VM. 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.

NOTE: Using a single NIC/vNIC as the source and the destination interface may cause increased latency in sending the traffic out from the VM.

Example of the G-vTAP config file for a single NIC/vNIC configuration:

Grant permission to monitor ingress and egress traffic at iface

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

Dual NIC Configuration

A G-vTAP Agent lets you configure two NICs/vNICs. One NIC/vNIC can be configured as the source interface and another NIC/vNIC can be configured as the destination interface.

For example, assume that there is eth0 and eth1 in the monitoring VM. 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.

Example of the G-vTAP config file for a dual NIC/vNIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# 'eth0' to monitor and 'eth1' to transmit the mirrored packets.
# eth0  mirror-src-ingress mirror-src-egress
# eth1  mirror-dst
```

Install G-vTAP Agents

You must have sudo/root access to edit the G-vTAP Agent configuration file.

For dual or multiple NIC/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).

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

Refer to the following topics for details:

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

Install G-vTAP from Ubuntu/Debian Package

To install from a Debian package:

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

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

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

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

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

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

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

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

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

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

4. Save the file.

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

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

6. Reboot the instance.

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

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

Install G-vTAP from RPM package

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

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

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

3. Modify the file /etc/gvtap-agent/gvtap-agent.conf 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: <Username>
           password: <Password>
           remoteIP: <IP address of the G-vTAP Controller 1>,
                     <IP address of the G-vTAP Controller 2>
           remotePort: 8891
   ```

6. Reboot the instance.

Check the status with the following command:

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

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

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

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

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

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent **6.2.00** MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**and the G-vTAP Agent service starts automatically.

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

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

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

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

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

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

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

4. Save the file.

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

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

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

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

Windows G-vTAP Agent Installation Using ZIP Package

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

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

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

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

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

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

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

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

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

5. Save the file.

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

   ```
   Registration:
           groupName: <Monitoring Domain Name>
           subGroupName: <Connection Name>
           remoteIP: <controller list IP addresses separated by comma>
   ```

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

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

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

Create Images with the Agent Installed

If you want to avoid downloading and installing the G-vTAP Agents every time there is a new VM to be monitored, you can save the G-vTAP Agent running on a VM as a private image. When a new VM is launched that contains the G-vTAP Agent, GigaVUE-FM automatically detects the new VM and updates the number of monitoring VMs in the monitoring session.

To save the G-vTAP Agent as an image, refer to Capture VM to managed image topic in the Microsoft Azure Documentation.

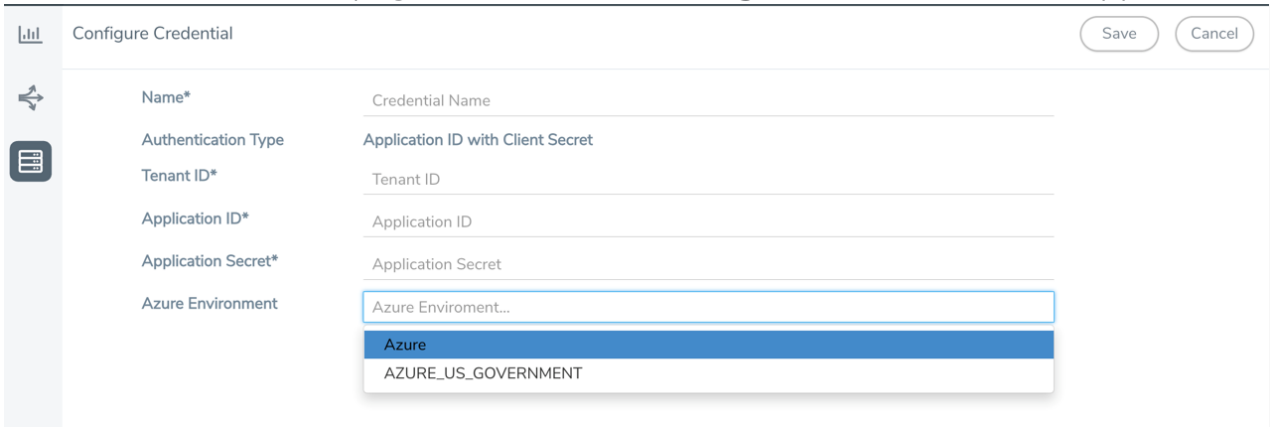
Create Azure Credentials

You can monitor workloads across multiple Azure subscriptions within one monitoring domain. All the deployed GigaVUE fabric nodes are shared among many Azure subscriptions to reduce the cost since each Azure subscription used to have a set of GigaVUE fabric nodes.

- After launching GigaVUE-FM in Azure, the **Managed Identity** authentication credential is automatically added to the Azure Credential page as the default credential.
- You can only add the **Application ID with Client Secret** authentication credentials to the Azure Credential page.

To create Azure credentials:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Settings > Credential**. The Azure Credential page appears.
2. In the Azure Credential page, click **Add**. The **Configure Credential**wizard appears.



3. Enter or select the appropriate information for the Azure credential as described in the following table.

Field	Description
Name	An alias used to identify the Azure credential.
Authentication Type	**Application ID with Client Secret**: Connection with Azure with a service principal. Enter the values for the following fields. o **Tenant ID**—a unique identifier of the Azure Active Directory instance. o **Application ID**—a unique identifier of an application in Azure platform. o **Application Secret**—a password or key to request tokens. Refer to Application ID with client secret for detailed information.
Azure Environment	Select an Azure environment where your workloads are located. For example, Azure_US_Government.

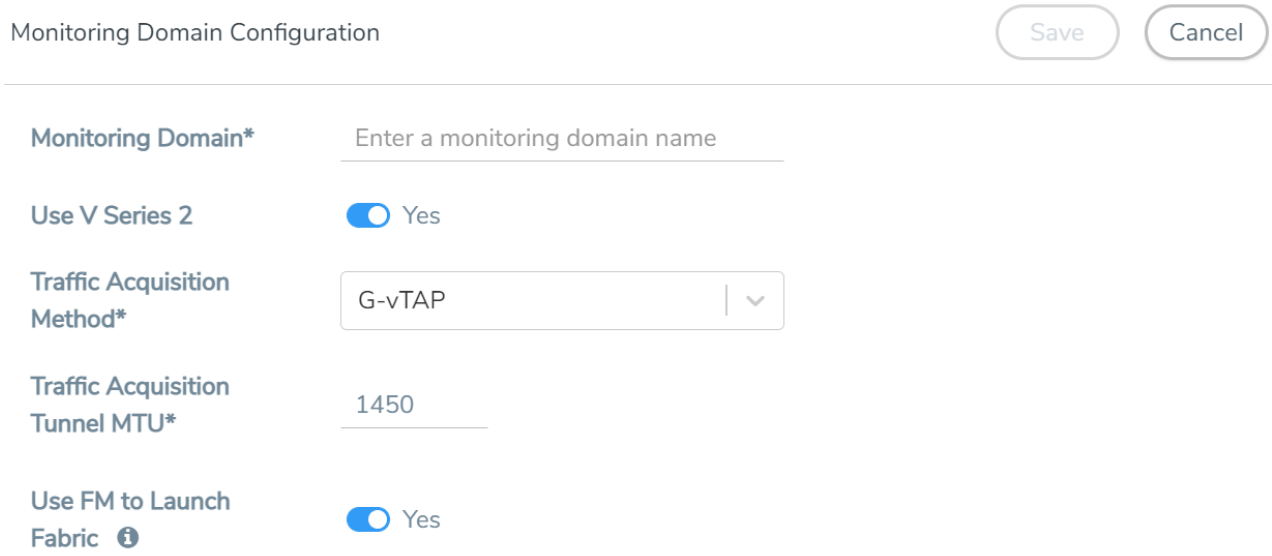
4. Click **Save**. You can view the list of available credentials in the Azure Credential page.

Create Monitoring Domain

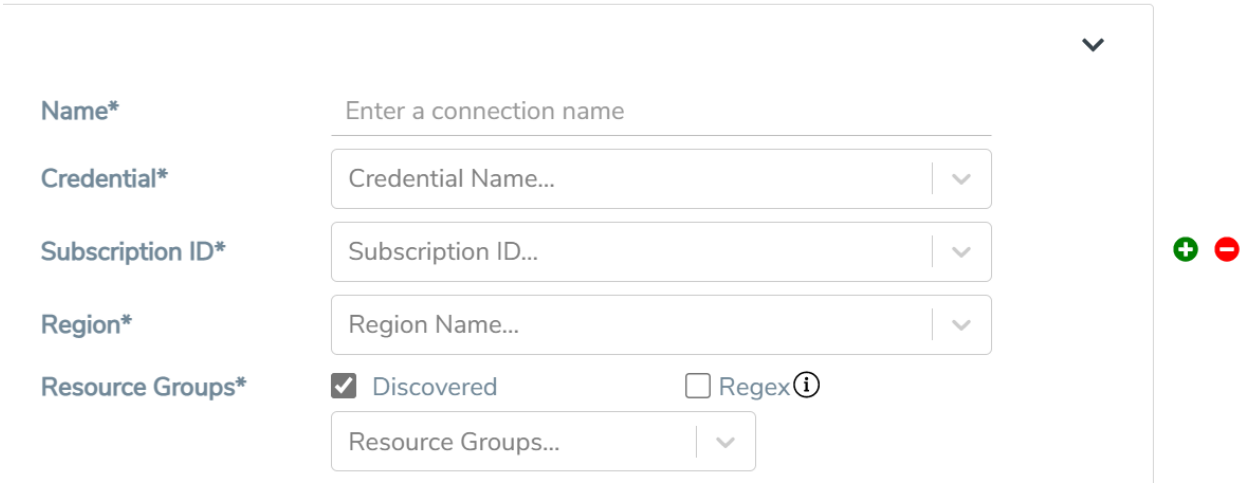
You must establish a connection between GigaVUE-FM and your Azure environment before you can perform the configuration steps. Creating a monitoring domain in GigaVUE-FM allows you to establish a connection between your Azure environment and GigaVUE-FM. After establishing a connection, you will be able to use GigaVUE-FM to specify a launch configuration for the G-vTAP Controllers, GigaVUE V Series Proxy, and GigaVUE V Series Nodes in the specified VNet and Resource Groups. GigaVUE-FM connects to Azure using either an Application ID with the client secret or the MSI method of authentication. After the connection establishment, GigaVUE-FM launches the G-vTAP Controller, GigaVUE V Series Proxy, and GigaVUE V Series 2 Node.

To create an Azure monitoring domain in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, click New. The **Azure Monitoring Domain Configuration** wizard appears.



3. Enter or select the appropriate information for the monitoring domain as described in the following table.

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain.
Use V Series 2	Select **Yes** for V Series 2 configuration.
Traffic Acquisition Method	Select a Tapping method. The available options are: ▪ **G-vTAP**: If you select G-vTAP as the tapping method, the traffic is acquired from the G-vTAP Agents installed on your standard VMs in the Resource Group or in the Scale Sets. Then the acquired traffic is forwarded to the GigaVUE V Series nodes. You must configure the G-vTAP Controller to monitor the G-vTAP Agents. ▪ **Customer Orchestrated Source**: If you use select **Customer Orchestrated Source** as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series nodes without deploying G-vTAP Agents or G-vTAP controllers. **NOTE:** Select the Traffic Acquisition Method as **Customer Orchestrated Source** if you wish to use Observability Gateway (AMX) application.
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. For VXLAN, the default value is 1450. 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 Azure.
Connections Connections	 **NOTE:** You can add multiple connections in a monitoring domain. Refer to Create Azure Credentials for more information on adding multiple **Application ID with Client Secret** authentication

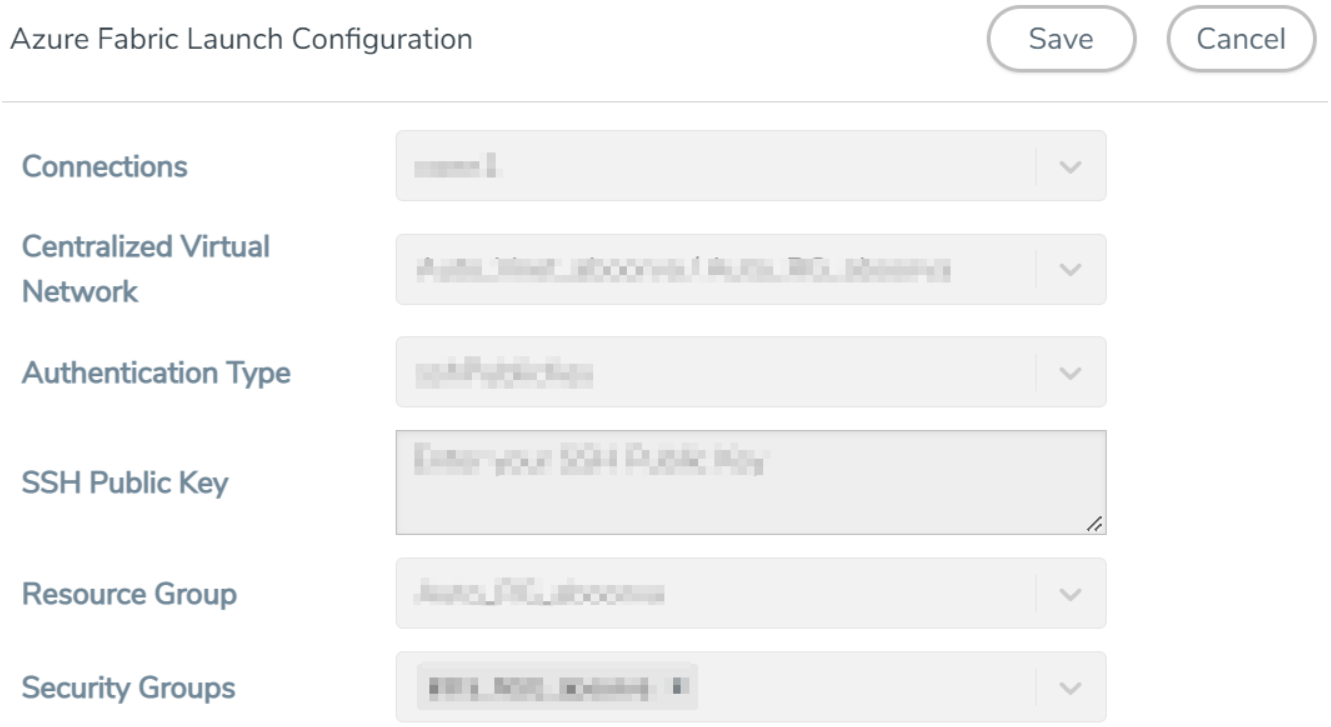
Field	Description
credentials.	
Name	An alias used to identify the connection.
Credential	Select an Azure credential. For detailed information, refer to Create Azure Credentials.
Subscription ID	A unique alphanumeric string that identifies your Azure subscription.
Region	Azure region for the monitoring domain. For example, West India.
Resource Groups	Select the Resource Groups of the corresponding VMs to monitor. **NOTE:** This field is only available if you select **G-vTAP** as the **Traffic Acquisition Method.**

4. Click **Save** and the **Azure Fabric Launch Configuration** wizard appears.

Configure GigaVUE Fabric Components in GigaVUE-FM

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

In the same **Azure Fabric Launch Configuration** page, you can configure all the GigaVUE fabric components.



Enter or select the required information as described in the following table.

Fields	Description
Connections	A connection that you created in the monitoring domain page. Refer to Create Monitoring Domain for more information.
Centralized Virtual Network	Alias of the centralized VNet in which the G-vTAP Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.
Authentication Type	Select Password or SSH Public Key as the Authentication Type to connect with the Centralized VNet. **NOTE:** SSH Public Key is the only supported authentication type for V Series 2 solution.

Fields	Description
SSH Public Key	The SSH public key for the GigaVUE fabric nodes.
Resource Group	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM.
Security Groups	The security group created for the GigaVUE fabric nodes.
Click **Yes** to configure V Series Proxy for the monitoring domain. Refer to Configure GigaVUE V Series Proxy	

To deploy GigaVUE fabric images (V Series nodes, GvTAP Controllers, and V Series Proxies) in GigaVUE-FM, you must accept the terms of the GigaVUE fabric images from the Azure marketplace using the Azure CLI or PowerShell.
Example:

```
az vm image list --all --publisher gigamon-inc --offer gigamon-fm-<version>
az vm image terms accept --urn gigamon-inc:gigamon-fm-<version>:vseries-node:<version>
az vm image terms accept --urn gigamon-inc:gigamon-fm-<version>:vseries-proxy:<version>
az vm image terms accept --urn gigamon-inc:gigamon-fm-<version>:gvtap-cntlr:<version>
```

Refer to the following topics for details:

- Configure G-vTAP Controllers
- Configure GigaVUE V Series Proxy
- Configure GigaVUE V Series Node

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.

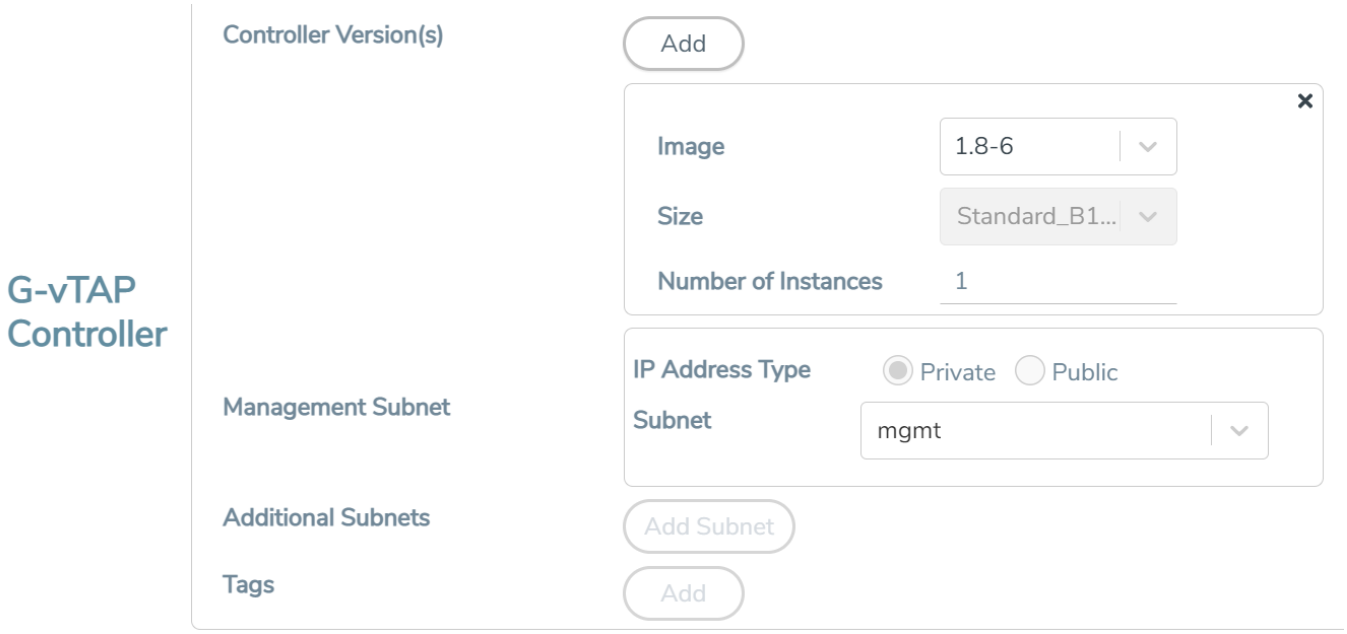
NOTE: A single G-vTAP Controller can manage up to 1000 G-vTAP Agents. The recommended minimum instance type is Standard_B1s for G-vTAP Controller.

A G-vTAP Controller can only manage G-vTAP Agents that has the same version.

To configure the G-vTAP Controllers:

NOTE: You cannot configure G-vTAP Controller for Tunnel as the traffic acquisition method.

In the **Azure Fabric Launch Configuration** page, Enter or select the appropriate values for the G-vTAP Controller as described in the following table.



Fields	Description
Controller Version(s)	The G-vTAP Controller version you configure must always be the same as the G-vTAP Agents' version number deployed in the VM machines. If there are multiple versions of G-vTAP Agents deployed in the VM machines, then you must configure multiple versions of G-vTAP Controllers that matches the version numbers of the G-vTAP Agents. **NOTE:** If there is a version mismatch between G-vTAP controllers and G-vTAP Agents, GigaVUE-FM cannot detect the agents in the instances. To add G-vTAP Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP Agents installed in the instances. **c.** From the **Size** drop-down list, select a size for the G-vTAP Controller. The default size is Standard_B1s. **d.** In **Number of Instances**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.
Management Subnet	**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 G-vTAP Controller instances and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Azure's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. On selecting Public IP address type, you must select all the required Public IPs. **Subnet**: Select a Subnet for G-vTAP Controller. The subnet that is used for communication between the G-vTAP Controllers and the G-vTAP Agents, as well as to communicate with GigaVUE-FM. Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management plane/subnet. **NOTE:** Some instance types are supported in Azure platform. Refer to Microsoft Azure documentation to learn on supported instance types.
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 data 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 Azure environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name that is easy to identify such as us-west-2-gvtap-controllers. To add a tag: **a.** Click **Add**. **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

GigaVUE V Series Proxy can manage 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.

NOTE: A single GigaVUE V Series Proxy can manage up to 100 GigaVUE V Series nodes. The recommended minimum instance type is Standard_B1s for V Series Proxy.

To configure the GigaVUE V Series Proxy:

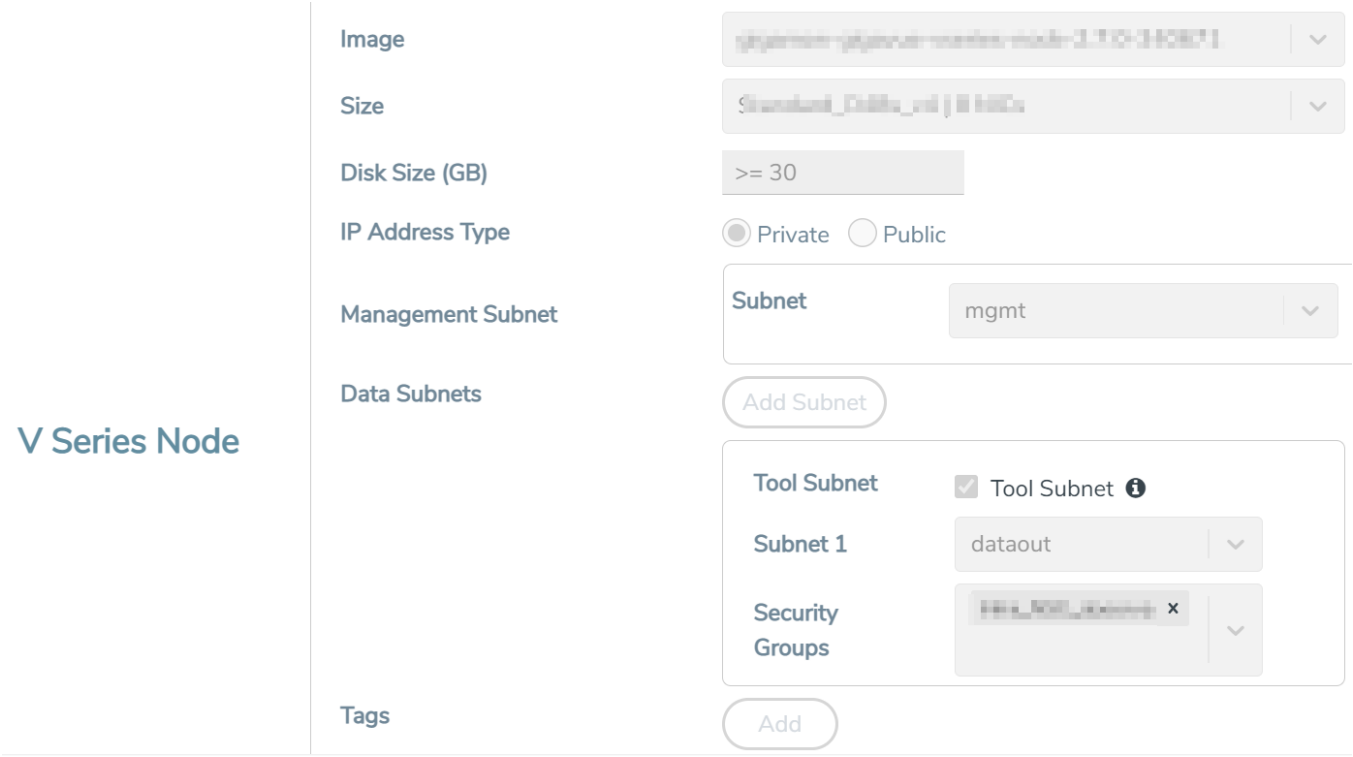
1. In the **Azure Fabric Launch Configuration** page, Select **Yes** to **Configure a V Series Proxy** and the V Series Proxy fields appears.
2. Enter or select the appropriate values for the V Series Proxy. Refer to the G-vTAP Controller field descriptions for detailed information.

Configure GigaVUE V Series Node

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

To launch a GigaVUE V Series node:

In the **Azure Fabric Launch Configuration** page, enter or select the appropriate values for the GigaVUE V Series Node.



Fields	Description
Image	From the **Image** drop-down list, select aGigaVUE V Series image.
Size	From the **Size** down-down list, select a size for theGigaVUE V Series. The default size for V Series 2 configuration is **Standard_D4s_v4**.
Disk Size (GB)	The size of the storage disk. The default disk size is 30GB. **NOTE:** When using Application Metadata Exporter, the minimum recommended Disk Size is 80GB.
IP Address Type	Select one of the following IP address types:

Fields	Description
	▪ 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 theGigaVUE V Series instances and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Azure's pool of public IP address. On selecting Public IP address type, you must select the number of Public IPs defined in the Maximum Instance.
Management Subnet	**Subnet**: Select a management subnet forGigaVUE V Series. The subnet that is used for communication between the G-vTAP Agents and the GigaVUE V Series Nodes, as well as to communicate with GigaVUE-FM. Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management plane/subnet.
Data Subnet(s)	The subnet that receives the mirrored VXLAN tunnel traffic from the G-vTAP Agents. Select a **Subnet** and the respective **Security Groups**. Click **Add** to add additional data subnets. **NOTE:** Using the **Tool Subnet** checkbox you can indicate the subnets to be used by theGigaVUE V Series to egress the aggregated/manipulated traffic to the tools.
Tag(s)	(Optional) The key name and value that helps to identify theGigaVUE V Series instances in your Azure environment. For example, you might haveGigaVUE V Series deployed in many regions. To distinguish theseGigaVUE V Series based on the regions, you can provide a name that is easy to identify. To add a tag: **a.** Click **Add**. **b.** In the **Key** field, enter the key. For example, enter Name. **c.** In the **Value** field, enter the key value.
Min Instances	The minimum number of GigaVUE V Series nodes to be launched in the Azure connection. The minimum number of instances that can be entered is 1. **NOTE:** Nodes will be launched when a monitoring session is deployed if GigaVUE-FM discovers some targets to monitor. The minimum amount will be launched at that time. The GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances	The maximum number of GigaVUE V Series nodes that can be launched in the Azure connection. When the number of instances per V Series node exceeds the max instances specified in this field, increase the number in the Max Instances to Launch. When additional V Series nodes are launched, GigaVUE-FM rebalances the instances assigned to the nodes. This can result in a brief interruption of traffic.

Click **Save** to complete the Azure Fabric Launch Configuration.

A monitoring domain is created, and you can view the monitoring domain and fabric component details by clicking on a monitoring domain name in the**Monitoring Domain** page.

Configure Role-Based Access for Third Party Orchestration

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

Users

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

Add Users

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

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

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

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

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

To add users perform the following steps:

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

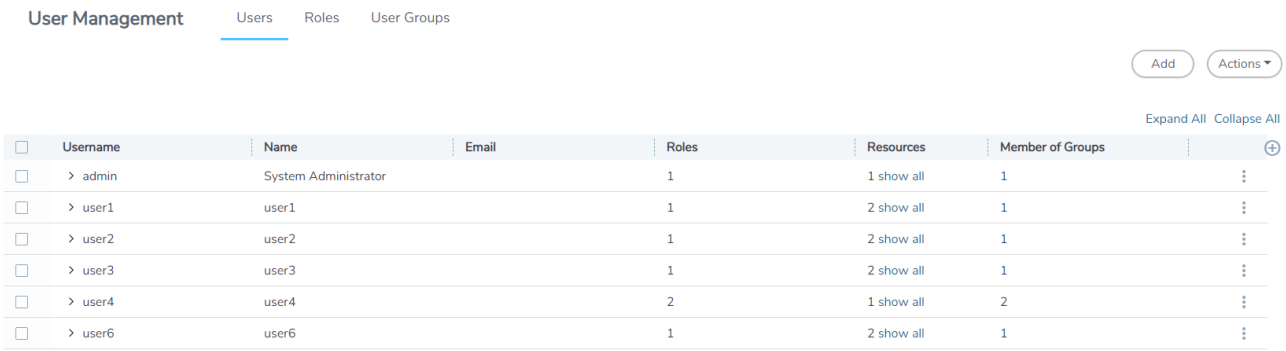


Figure 1 *FM Users Page*

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

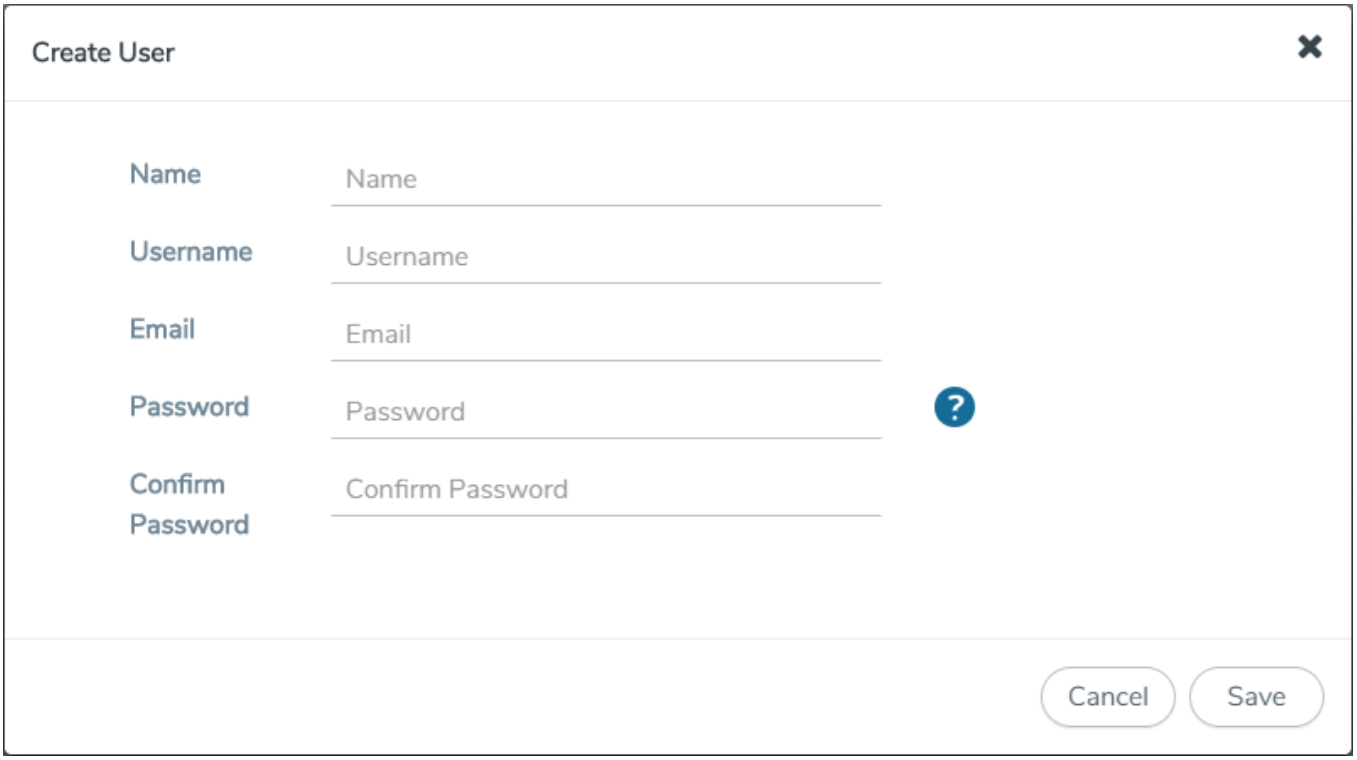


Figure 2 *Create User*

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

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

NOTE: GigaVUE-FM will prompt for your password.

b. Click **Save**.

The new user is added to the summary list view.

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

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

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

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

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

Create Roles

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

Create Roles

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

GigaVUE-FM has the following default roles:

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

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

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

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

Category	Associated Resources
All	Manages all resources ▪ A user with fm_super_admin role has both read and write access to all the resource categories. ▪ A user with fm_user role has only read access to all the resource categories.
Infrastructure Management	Manages resources such as devices, cards, ports and cloud resources. You can add or delete a device in GigaVUE-FM, enable or disable cards, modify port parameters, set leaf-spine topology. The following resources belong to this category:

Category	Associated Resources
	▪ **Physical resources:** Chassis, slots, cards ports, port groups, port pairs, cluster config, nodes and so on ▪ **GigaVUE-FM inventory resources:** Nodes, node credentials ▪ **Device backup/restore:** Device and cluster configuration ▪ **Device license configuration:** Device/cluster licensing ▪ **Statistics:** Device, port ▪ **Tags**: Events, historical trending ▪ **Device security**: SystemTime, System EventNotification, SystemLocalUser, System Security Policy Settings, AAA Authentication Settings,Device User Roles, LDAP Servers, RADIUS Servers, TACACS+ Servers ▪ **Device maintenance**: Sys Dump, Syslog ▪ **Cloud Infrastructure resources**: Cloud Connections, Cloud Proxy Server, Cloud Fabric Deployment, Cloud Configurations, Sys Dump, Syslog, Cloud licenses, Cloud Inventory. **NOTE:** Cloud APIs are also RBAC enabled.
Traffic Control Management	Manages inline resources, flow maps, GigaSMART applications, second level maps, map chains, map groups. The following resources belong to this category: ▪ **Infrastructure resources**: IP interfaces, circuit tunnels, tunnel endpoints, tunnel load balancing endpoints, ARP entries ▪ Intent Based Orchestration resources: Policies, rules ▪ **GigaSMART resources:** GigaSMART, GSgroups, vPorts, Netflow exporters ▪ **Map resources**: Fabric, fabric resources, flow maps, maps, map chains, map groups, map templates ▪ **Application intelligence resources**: Application visibility, Metadata, application filter resources ▪ **Tag**: Flow manipulation - Netflow operations, Statistics - device port ▪ Active visibility

Category	Associated Resources
	▪ **Inline resources**: Inline networks, Inline network groups, Inline tools, Inline tool groups, Inline serial tools, Inline heartbeat profile ▪ **Cloud operation resources**: Monitoring session, stats, map library, tunnel library, tools library, inclusion/exclusion maps. **NOTE:** Cloud APIs are also RBAC enabled.
FM Security Management	Ensures secure GigaVUE-FM environment. Users in this category can manage user and roles, AAA services and other security operations.
System Management	Controls system administration activities of GigaVUE-FM. User in this category are allowed to perform operations such as backup/restore of GigaVUE-FM and devices, and upgrade of GigaVUE-FM. The following GigaVUE-FM resources belong to this category: ▪ Backup/restore ▪ Archive server ▪ License ▪ Storage management ▪ Image repo config ▪ Notification target/email
Forward list/CUPS Management	Manages the forward list configuration. The following resources belong to this category: ▪ GTP forward list ▪ SIP forward list ▪ Diameter forward list
Third Party Orchestration	Used to deploy fabric components using external orchestrator.
Device Certificate Management	Manages device certificates.
Other Resource Management	Manages virtual and cloud resources

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

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

To create a role:

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

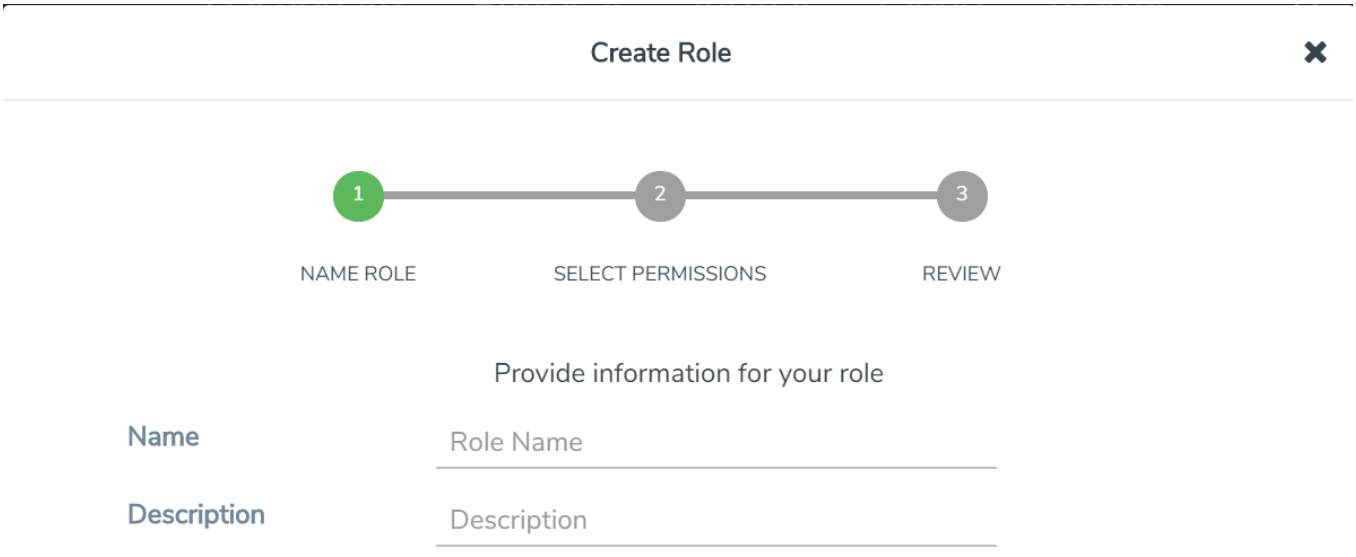


Figure 3 *Create Roles*

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

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

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

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

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

The new role is added to the summary list view.

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

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

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

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

Refer to the following notes:

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

Create User Groups

You can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups.

Create User Groups

Starting in software version 5.8.00, you can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups.

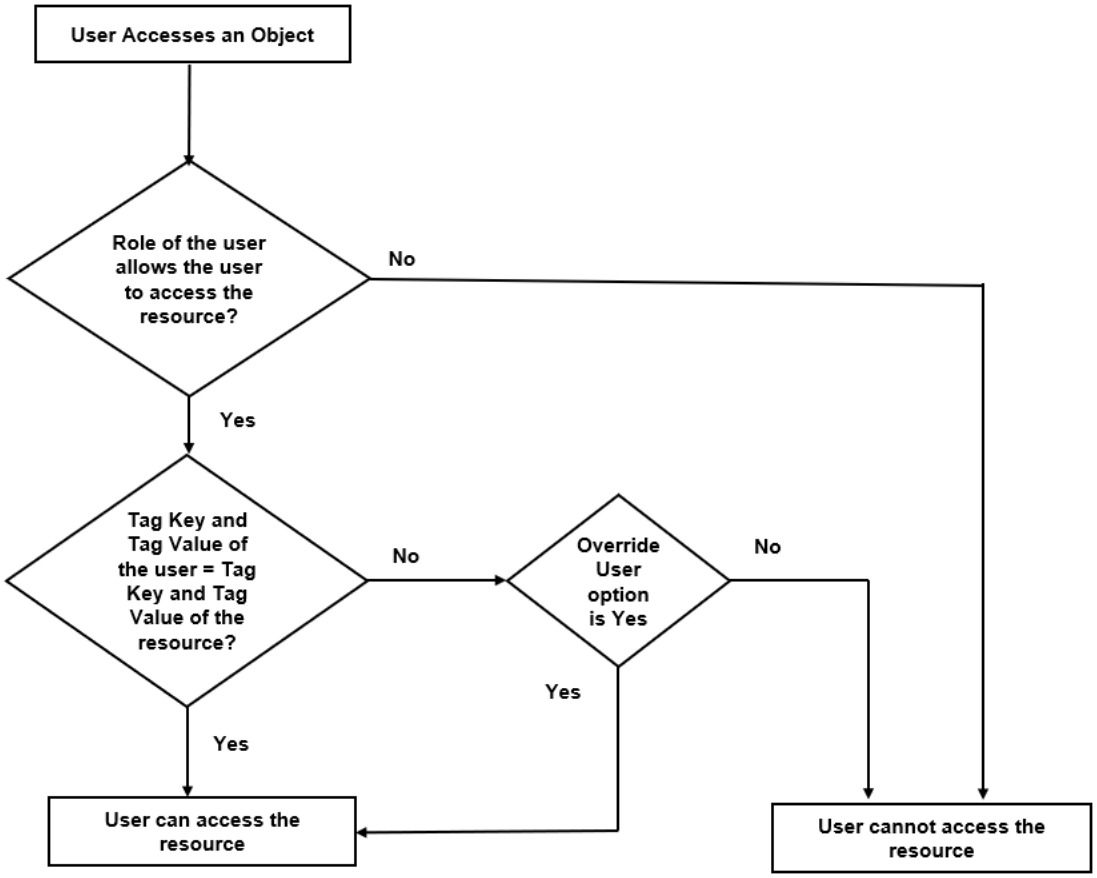
The following user groups are available by default in GigaVUE-FM. You will not be able to edit or change these groups in the system.

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

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

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

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



To create a group:

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

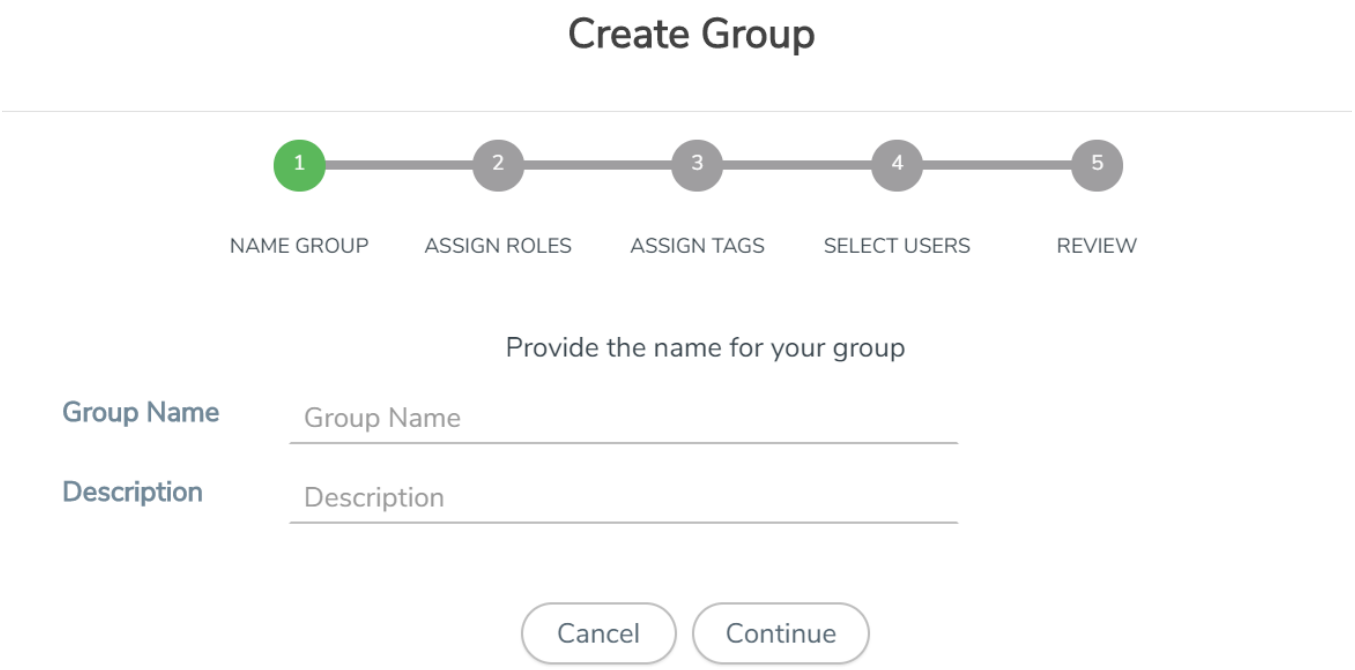


Figure 4 *Create Group*

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

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

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

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

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

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

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

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

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

Configure GigaVUE Fabric Components in Azure

This section provides step-by-step information on how to register GigaVUE fabric components using Azure Portal or a configuration file.

Overview of Third-Party Orchestration

You can use your own Azure Orchestrator to deploy the GigaVUE fabric nodes instead of using GigaVUE-FM to deploy your fabric components.

The third-party orchestration feature allows you to deploy GigaVUE fabric components using your own Azure orchestration system. These fabric components register themselves with GigaVUE-FM using the information provided by the user. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

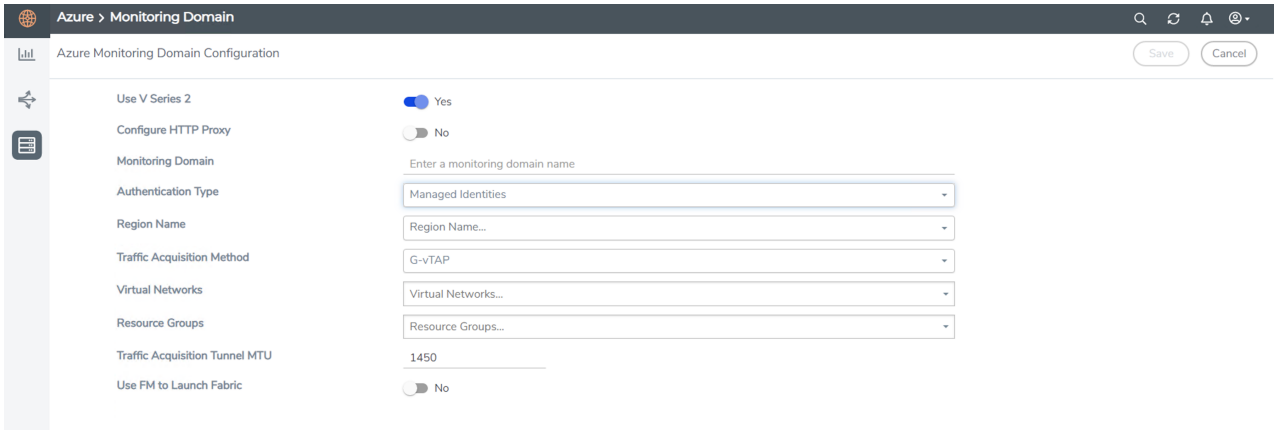
You can either manually deploy the fabric nodes using a configuration file or you can use the Azure portal to launch the instances and deploy the fabric nodes using Custom data. Using the Custom data provided by you, the fabric nodes register itself with the GigaVUE-FM. Based on the group name and the sub group name details provided in the Custom data, GigaVUE-FM groups these fabric nodes under their respective monitoring domain and connection name. Health status of the registered nodes is determined by the heartbeat messages sent from the respective nodes.

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

- When configuring G-vTAP Controller, select **G-vTAP** as the Traffic Acquisition Method.
- When you select **Customer Orchestrated Source** as your Traffic Acquisition Method, G-vTAP Agent and G-vTAP Controller registration are not applicable.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the GigaVUE V Series Nodes or G-vTAP Controllers.
- Deployment of G-vTAP Controller, GigaVUE V Series Node, and GigaVUE V Series Proxy through a third-party orchestrator is supported only on Linux platform.
- Deployment of G-vTAP Agent through a third-party orchestrator is supported on Linux and Windows platforms. Refer to Linux Agent Installation and Windows G-vTAP Agent Installation for detailed information.

To register fabric nodes under Azure monitoring domain:

1. Create a monitoring domain in GigaVUE-FM. Refer to Create a Monitoring Domain for detailed instructions.
2. In the **Monitoring Domain Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you are going to configure the fabric components in Azure Orchestrator.



3. After creating your monitoring domain, you can deploy your fabric components through Azure Portal.

In your Azure Portal, you can configure the following GigaVUE fabric components:

- Configure G-vTAP Controller in Azure
- Configure G-vTAP Agent in Azure
- Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure

Configure G-vTAP Controller in Azure

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

To register G-vTAP Controller in Azure Portal, use any one of the following methods.

- Register G-vTAP Controller during Virtual Machine Launch
- Register G-vTAP Controller after Virtual Machine Launch

Register G-vTAP Controller during Virtual Machine Launch

In your Azure portal, to launch the G-vTAP Controller init virtual machine and register G-vTAP Controller using custom data, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.

2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The G-vTAP Controller uses this custom 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: <Username>
        password: <Password>
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
```

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

The G-vTAP Controller deployed in your Azure portal appears on the Monitoring Domain page of GigaVUE-FM.

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

Register G-vTAP Controller after Virtual Machine Launch

To register G-vTAP Controller after launching a Virtual Machine using a configuration file, follow the steps given below:

1. Log in to the G-vTAP Controller.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom data.

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

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

3. Restart the G-vTAP Controller service.

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

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

Configure G-vTAP Agent in Azure

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

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

To register G-vTAP Agent in Azure Portal, use any one of the following methods.

- Register G-vTAP Agent during Virtual Machine Launch
- Register G-vTAP Agent after Virtual Machine Launch

Register G-vTAP Agent during Virtual Machine Launch

> **NOTE:** Registering G-vTAP Agent during Virtual Machine Launch is not applicable for Windows Agents. You can register your Windows Agents after launching the Virtual machine, using a configuration file.

In your Azure portal, to launch the G-vTAP Agent init virtual machine and register the G-vTAP Agent using custom data, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The G-vTAP Agent uses this custom 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: <Username>
        password: <Password>
        remoteIP: <IP address of the G-vTAP Controller 1>, <IP address of the G-vTAP
Controller 2>
        remotePort: 8891
```

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

Register G-vTAP Agent after Virtual Machine Launch

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.

To register G-vTAP Agent after launching a Virtual Machine using a configuration file, follow the steps given below:

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 custom 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: <Username>
    password: <Password>
    remoteIP: <IP address of the G-vTAP Controller 1>,
           <IP address of the G-vTAP Controller 2>
    remotePort: 8891
```

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

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

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 GigaVUE V Series Node and GigaVUE V Series Proxy in Azure

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if the user does not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in Azure Portal, use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch
- Register GigaVUE V Series Proxy after Virtual Machine Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Virtual Machine Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy using the custom data in Azure Portal, follow the steps given below:

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The GigaVUE V Series Node and GigaVUE V Series Proxy uses this custom 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: <Username>
        password: <Password>
        remoteIP: <IP address of the GigaVUE-FM> or <IP address of the Proxy>
        remotePort: 443
```

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

Register GigaVUE V Series Proxy after Virtual Machine Launch

To register GigaVUE V SeriesProxy after launching the virtual machine using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Proxy.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom data.

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

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

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

The deployed GigaVUE V Series proxy registers with the GigaVUE-FM. After successful registration, the GigaVUE V Series 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 theGigaVUE V Series proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series proxy and it will be removed from GigaVUE-FM.

Refer Deploying GigaVUE Cloud Suite for Azure using Customer Orchestration for more detailed information.

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

When upgrading GigaVUE-FM to any version higher than 6.0.00 and if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM are lower than or equal to 6.0.00, then for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission. The username would be **orchestration** and the password would be **orchestration123A!** for the user created in GigaVUE-FM. Ensure that there is no existing user in GigaVUE-FM, with the username **orchestration**.

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

Upgrade GigaVUE Fabric Components in GigaVUE-FM for Azure

This chapter describes how to upgrade GigaVUE V Series Proxy and GigaVUE V Series Node. 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 Node and GigaVUE V Series Proxy

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Node, you must upgrade GigaVUE-FM to software version 5.13.01 or above.

Upgrade G-vTAP Controller

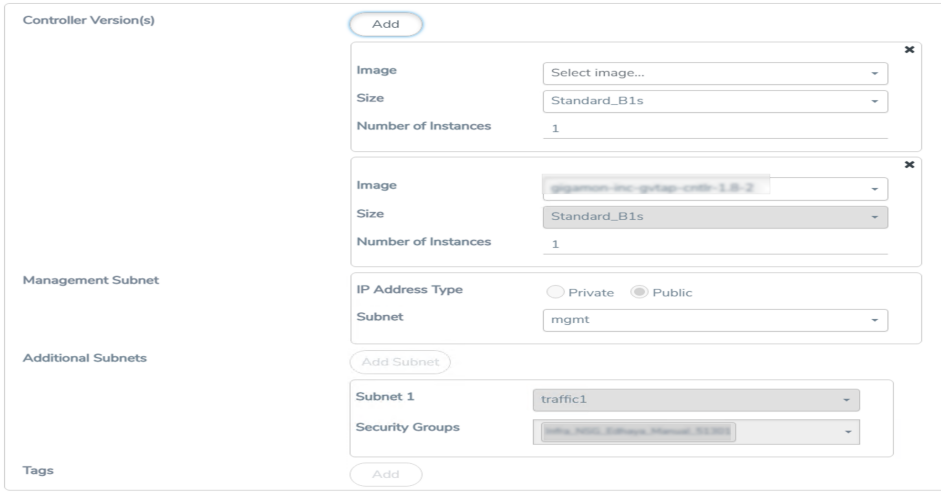
NOTE: G-vTAP Controllers cannot be upgraded. Only a new version that is compatible with the G-vTAP Agent's version can be added or removed in the **Azure Fabric Launch Configuration** page.

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. In the **Azure Fabric Launch Configuration** page, under **Controller Versions**, click **Add**.
b. From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP Agents installed in the instances.
c. From the **Size** drop-down list, select a size for the G-vTAP Controller. The default size is Standard_B1s.
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:

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

a. From the **Image** 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 Node and GigaVUE V Series Proxy

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

There are multiple ways to upgrade the GigaVUE V Series Proxy and Node. You can:

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

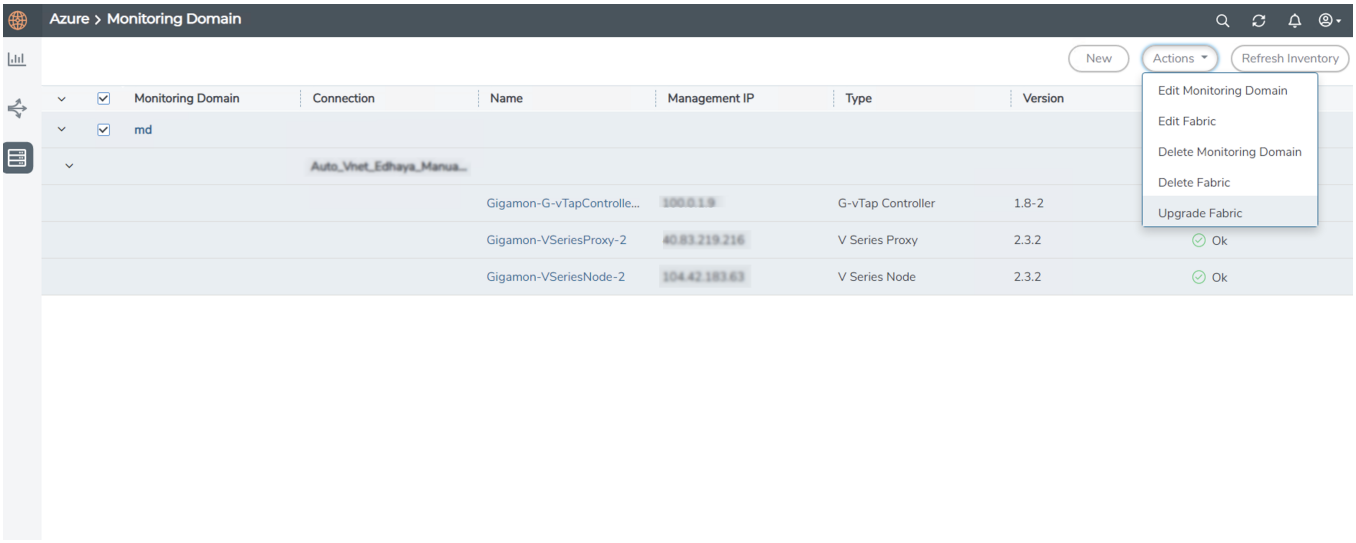
  For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VNet, you can upgrade all of them at once. First, the new version of GigaVUE V Series controller is launched. Next, the new version of GigaVUE V Series nodes are launched. Then, the old version of V Series controller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

  NOTES:
  - When the new version of node and proxy is launched, the old version still exists in the VNet until they are deleted. Make sure the instance type determined during the configuration can accommodate the total number of new and old instances present in the VNet. If the instance type cannot support so many instances, you can choose to upgrade in multiple batches.
  - If there is an error while upgrading the complete set of proxys and nodes present in the VNet, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.
  - If you have deployed your nodes using Public IP address while creating the monitoring domain, then select the same number of Public IP addressess defined in your Max Instances when upgrading your nodes. Refer to Create Monitoring Domain for more detailed information.
- Launch and replace the nodes and proxy in multiple batches.

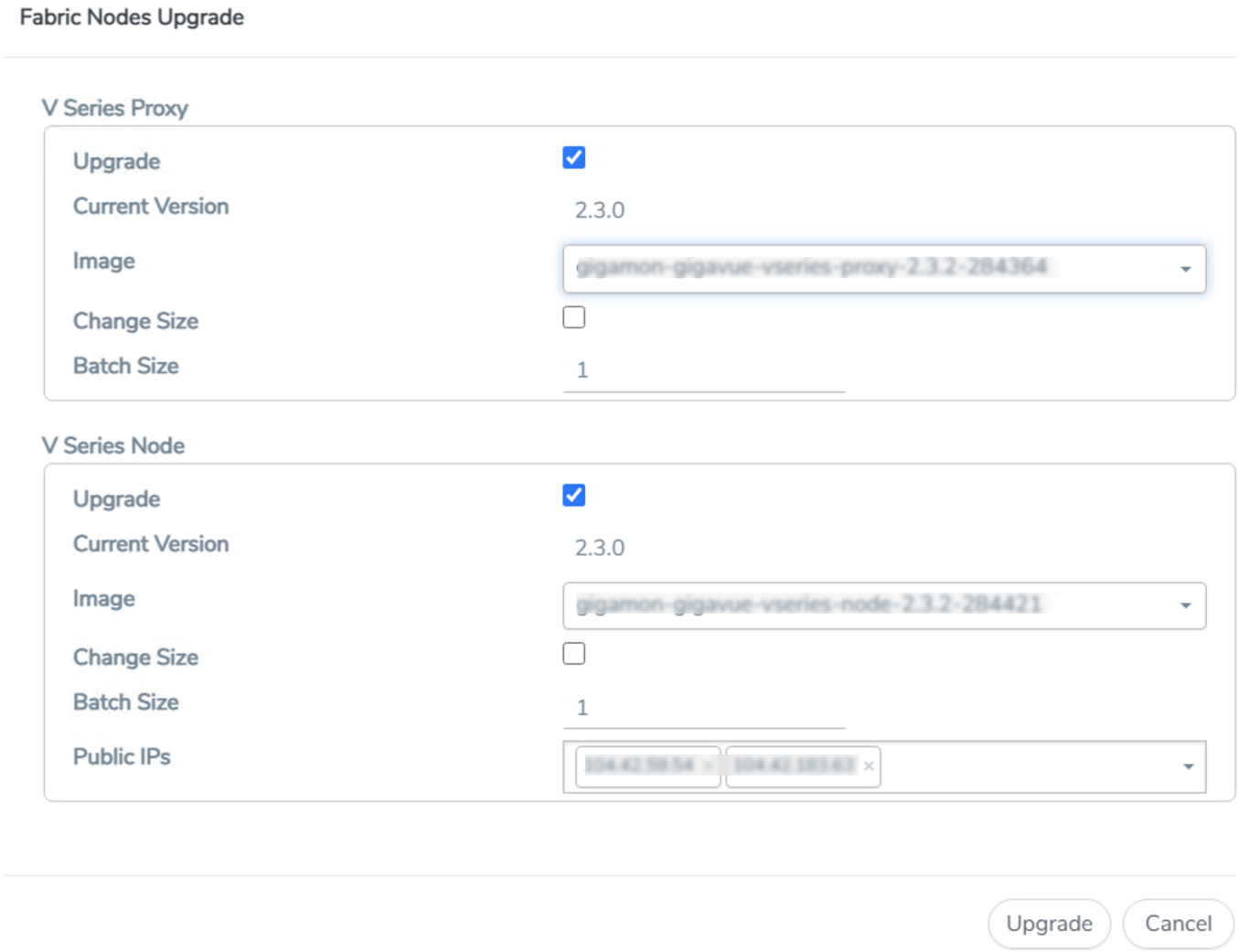
  For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

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

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



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



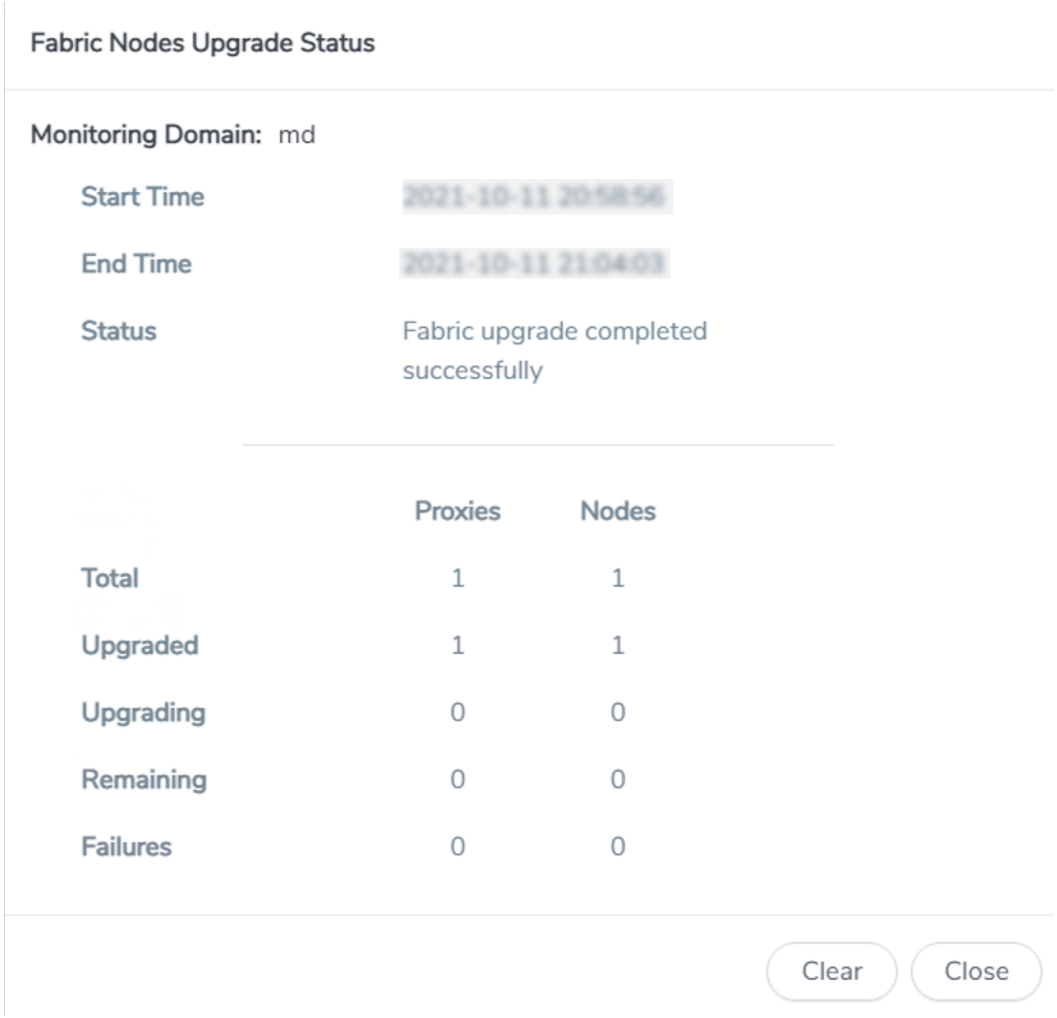
4. To upgrade the GigaVUE V Series Node/Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V SeriesProxy/Nodes.
6. Select the **Change Size** checkbox to change the flavor of the node/proxy, only if required.
7. To upgrade the GigaVUE V Series Node/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. From the Public IPs drop-down list, select the IP addressess equal to the Max Instances defined when creating a monitoring domain.

   NOTE: This is only applicable for nodes deployed using Public IP, when creating a monitoring domain.
9. Click **Upgrade**.

   The upgrade process takes a while depending on the number of GigaVUE V Series Proxys and Nodes upgrading in your Azure 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. The monitoring session is deployed automatically.

To view the detailed upgrade status click **Upgrade in progress** or **Upgrade successful**, the **V Series Node Upgrade Status** dialog box appears.



- Click **Clear** to delete the monitoring domain upgrade status history of successfully upgraded nodes.

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 Ingress and Egress Tunnels
- Create a New Map
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics
- Visualize the Network Topology

Create a Monitoring Session

You must create a monitoring domain before creating a monitoring session. Refer to Create Monitoring Domain for more detailed information on how to create a monitoring domain.

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

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

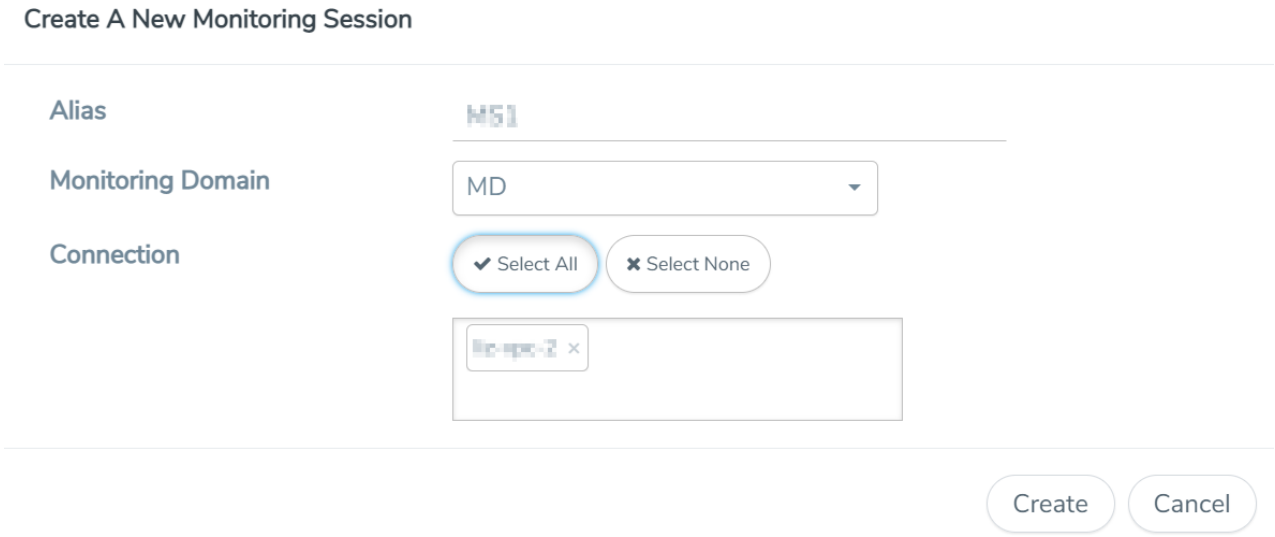
For the connections without G-vTAPs there is no targets that are automatically selected. You can use Customer Orchestrated Source in the monitoring session to accept a tunnel from anywhere.

You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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



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

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

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

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

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

Applying Prefiltering policy template to Monitoring Session

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

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

Prefiltering

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

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

Each monitoring session can have a maximum of 16 rules.

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

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

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

Creating Prefiltering policy template

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

To create a prefiltering policy template do the following steps:

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

2. Click **New**.

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

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

5. Click any one of the following options:
   - Pass — Passes the traffic.
   - Drop — Drops the traffic.

6. Click any one of the following options as per the requirement:
   - Bi-Directional —- Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
   - Ingress — Filters the traffic that flows in.
   - Egress — Filters the traffic that flows out.

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

8. Select the **Filter Type** from anyone of the following options:
   - L3
   - L4

9. Select the **Filter Name** from any one of the following options:
   - ip4Src
   - ip4Dst
   - ip6Src
   - ip6Dst
   - Proto - It is common for both ipv4, ipv6.

10. Select the **Filter Relation** from any one of the following options:
    - Not Equal to
    - Equal to

11. Enter the value for the given filter.

12. Click **Save**.

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

Create Ingress and Egress Tunnels

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

To create a new tunnel endpoint:

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

Field	Description
Alias	The name of the tunnel endpoint. **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Type	VXLAN is the only supported tunnel type for Azure.
Traffic Direction	The direction of the traffic flowing through the V Series node. • Choose **In** (Decapsulation) for creating an Ingress tunnel, 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.
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
Remote Tunnel IP	• For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. • For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint.

4. Click **Save**.

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

After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a

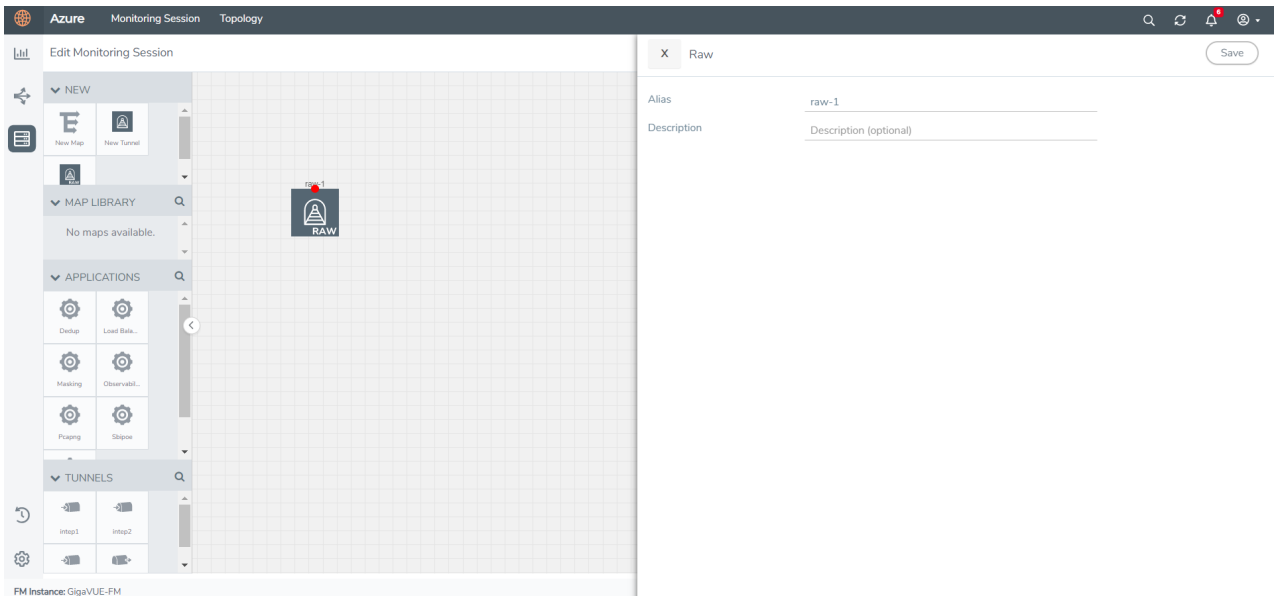
monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

Create Raw Endpoint

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

To add Raw Endpoint to the monitoring session:

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



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

Create a New Map

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

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

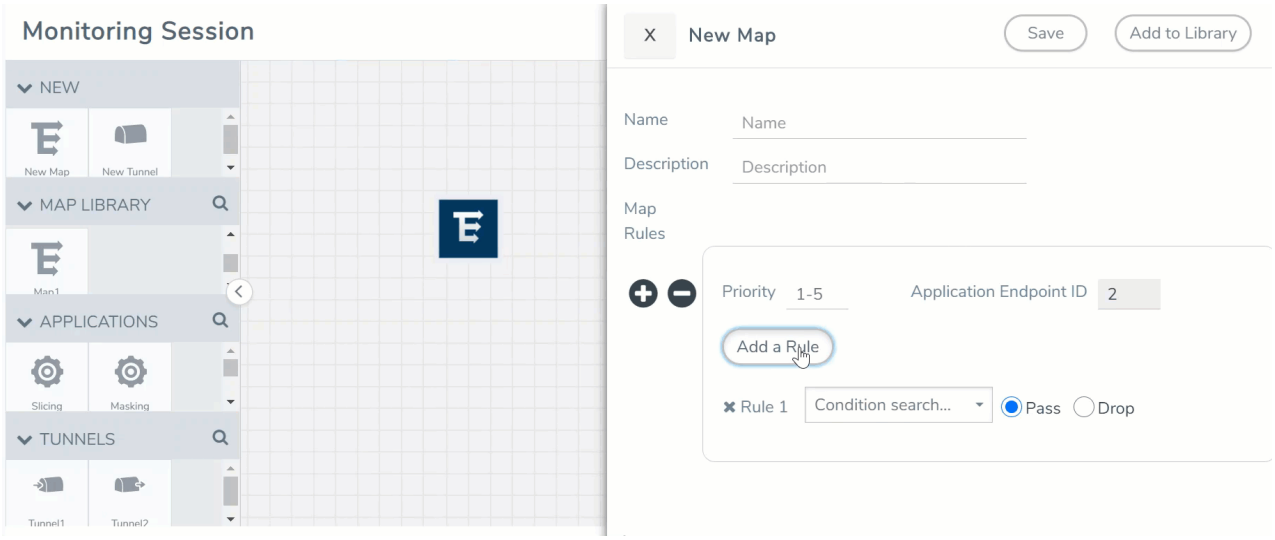
A map is used to filter the traffic flowing through the GigaVUE V Series Nodes. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.

Keep in mind the following when creating a map:

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

To create a new map:

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



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

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

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

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

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

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

Rules and Notes:

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

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

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

Example- Create a New Map using Inclusion and Exclusion Maps

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

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

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

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

Add Applications to Monitoring Session

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

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

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

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

- Application Metadata Intelligence
- Application Filtering Intelligence

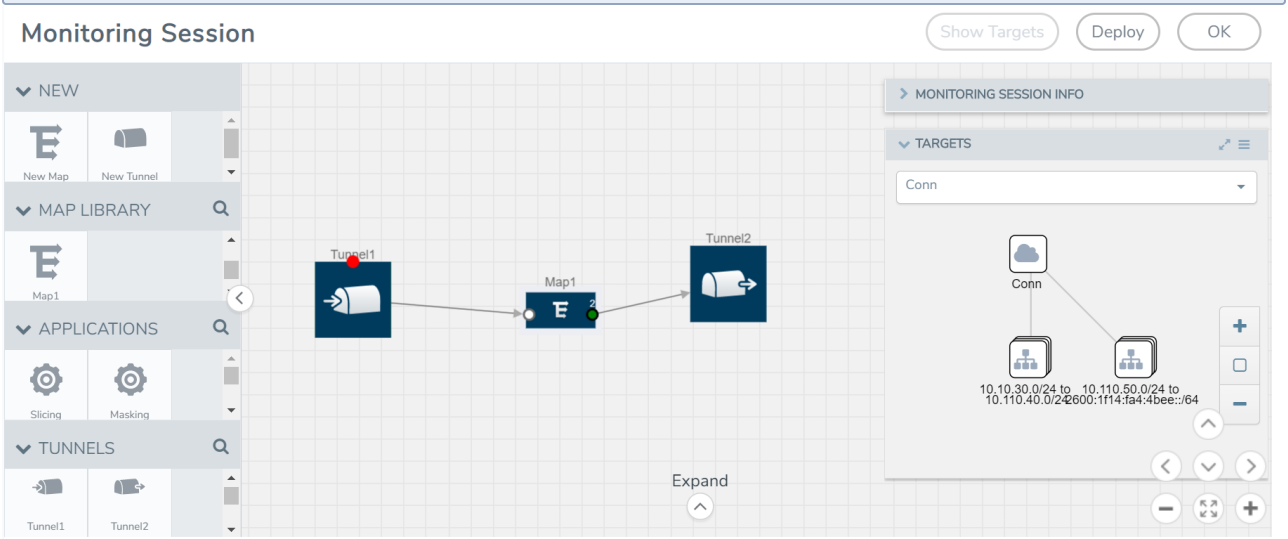
For more information, refer to these GigaSMART Operations in the *GigaVUE Fabric Management Guide*.

Deploy Monitoring Session

To deploy the monitoring session:

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

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



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

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

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

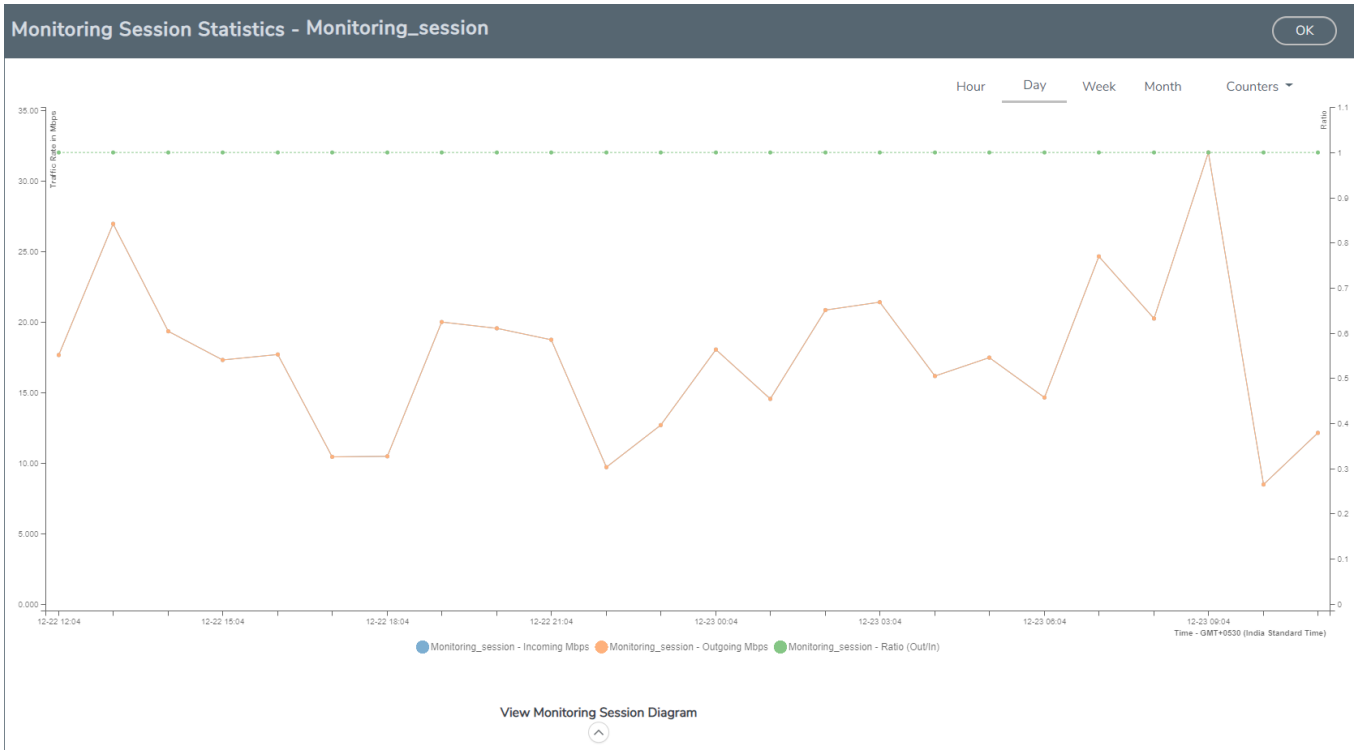
Button	Description
Undeploy	Undeploys the selected monitoring session.
Clone	Duplicates the selected monitoring session.
Edit	Opens the Edit page for the selected monitoring session. **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again..
Delete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

View Monitoring Session Statistics

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

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

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



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

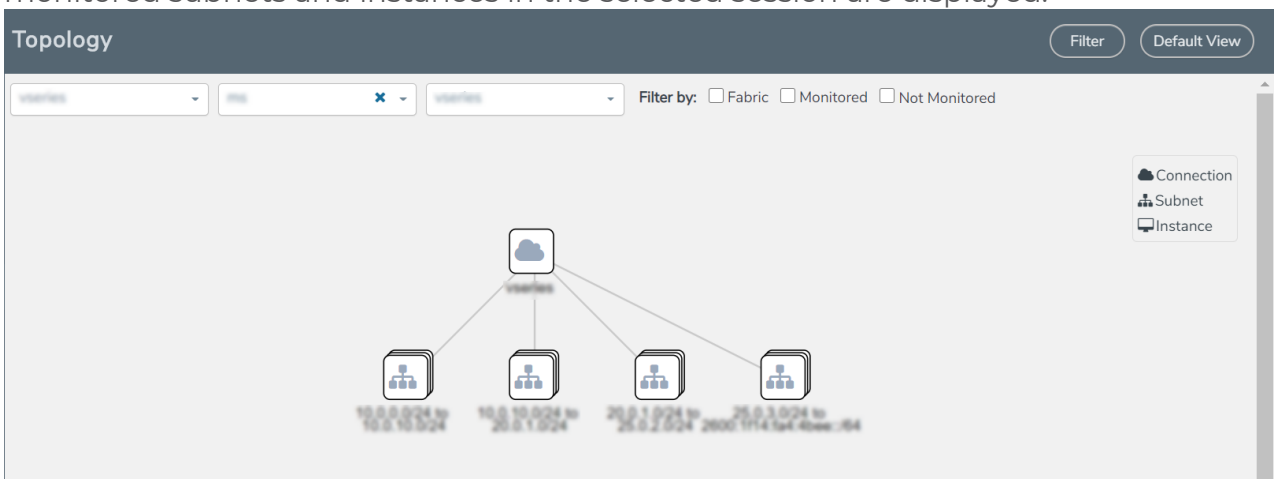
- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view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

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

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

Configure Application Intelligence Solutions on GigaVUE V Series Nodes for Azure

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

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

Important Notes:

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

Configure Environment

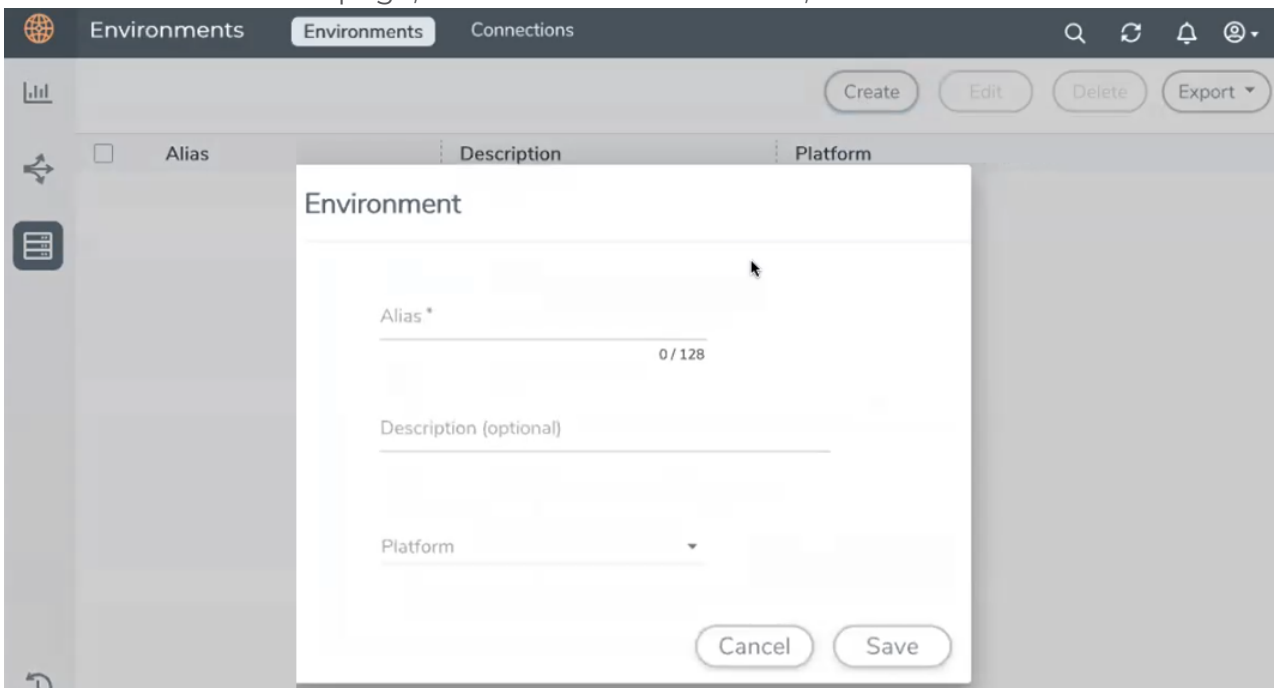
The Environments page allows you to create the following:

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

Create Environment

To configure the Environment:

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



3. Select or enter the following details:

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

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

Use the following buttons to manage your environment:

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

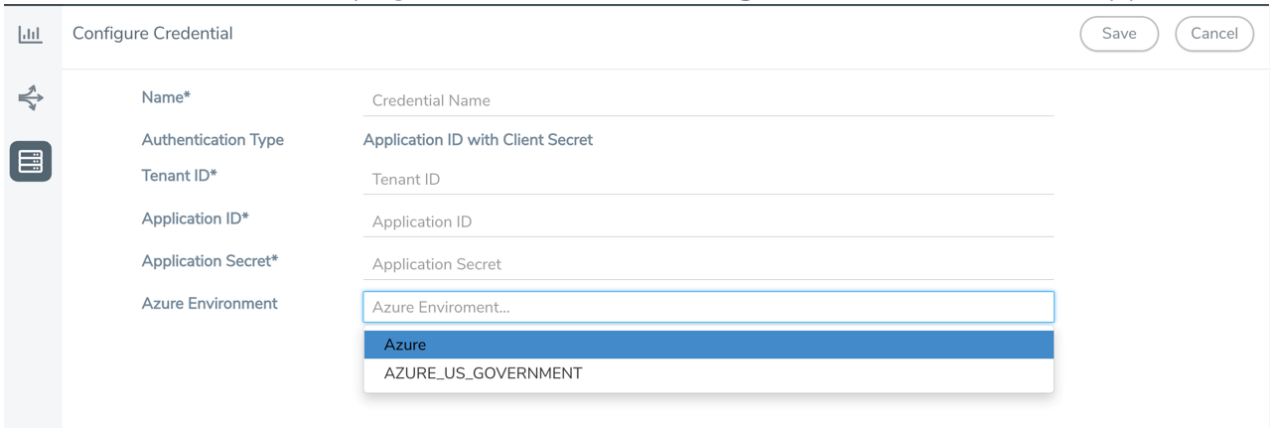
Create Credentials

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

Create Azure Credentials

To create Azure credentials:

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



4. Enter or select the appropriate information for the Azure credential as described in the following table.

Field	Description
Name	An alias used to identify the Azure credential.
Authentication Type	**Application ID with Client Secret**: Connection with Azure with a service principal. Enter the values for the following fields. o **Tenant ID**—a unique identifier of the Azure Active Directory instance. o **Application ID**—a unique identifier of an application in Azure platform. o **Application Secret**—a password or key to request tokens. Refer to Application ID with client secret for detailed information.
Azure Environment	Select an Azure environment where your workloads are located. For example, Azure_US_Government.

5. Click **Save**.

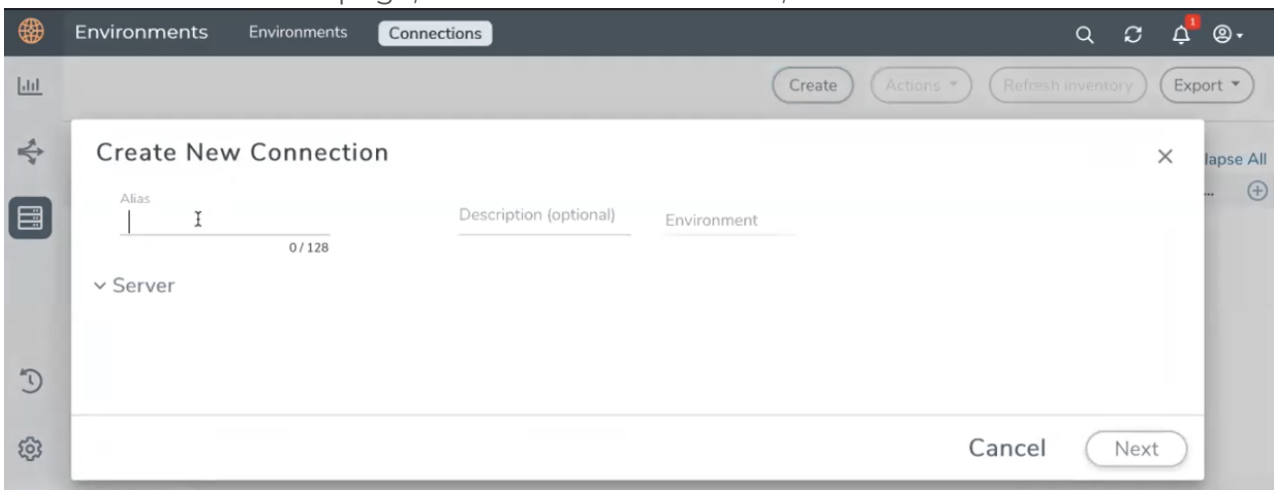
Connect to Azure

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

Create Connection

To create a new Connection:

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



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

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

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

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials for detailed information on how to create credentials.
Subscription ID	Select the subscription ID.
Region Name	The Azure region for the connection. For example, East Asia.
Resource Groups	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM. A Resource Group must contain the VMs that needs to be monitored.
Traffic Acquisition Method	Select a Tapping method. The available options are: • **G-vTAP**: If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP Agents. • **Tunnel**: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to V Series nodes without deploying G-vTAP Agents or G-vTAP controllers.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. **NOTE:** The default MTU is 1450. You can edit the MTU value according to your requirements. The valid range is between 1450 to 9000.

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

Field	Description
Centralized Virtual Network	Alias of the centralized VNet in which the G-vTAP Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.
Authentication Type	SSH Public Key is the only supported authentication type for V Series 2 solution.
SSH Public Key	The SSH public key for the GigaVUE fabric nodes.
Security Groups	The security group created for the GigaVUE fabric nodes.
Configure a V Series Proxy (optional)	Enable the **Configure a V Series Proxy** toggle button if you wish to deploy V Series nodes using a proxy.

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

Field	Description
Controller Version(s)	The G-vTAP Controller version you configure must always be the same as the G-vTAP Agents' version number deployed in the VM machines. If there are multiple versions of G-vTAP Agents deployed in the VM machines, then you must configure multiple versions of G-vTAP Controllers that matches the version numbers of the G-vTAP Agents. **NOTE:** If there is a version mismatch between G-vTAP controllers and G-vTAP Agents, GigaVUE-FM cannot detect the agents in the instances. To add G-vTAP Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP Agents installed in the instances. **c.** From the **Size** drop-down list, select a size for the G-vTAP Controller. The default size is **Standard_B1s**. **d.** In **Number of Instances**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.
Management Subnet	**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 G-vTAP Controller instances and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Azure's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. On selecting Public IP address type, you must select all the required Public IPs. **Subnet**: Select a management subnet for G-vTAP Controller. The subnet that is used for communication between the G-vTAP Controllers and the G-vTAP Agents, as well as to communicate with GigaVUE-FM. Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So, they should share at least one management subnet. **NOTE:** Some instance types are supported in Azure platform. Refer to Microsoft Azure documentation to learn on supported instance types.

Field	Description
Additional Subnets	(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 data 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 G-vTAP Controller instances in your Azure environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name that is easy to identify such as us-west-2-gvtap-controllers. To add a tag: **a.** Click **Add**. **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.

NOTE: In a connection, you can configure multiple versions of a G-vTAP Controller and you can only configure one version of a V Series Proxy.

In the V Series Proxy section, select or enter the values for the fields as described in the previous G-vTAP Controller configuration table. The fields of the V Series Proxy configuration are similar to G-vTAP Controller configuration.

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

Fields	Description
Image	From the **Image** drop-down list, select a V Series node image.
Size	From the **Size** down-down list, select a size for the V Series node. The default size for V Series configuration is **Standard_D4s_v4**.
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 V Series node instances and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Azure's pool of public IP address. On selecting Public IP address type, you must select the number of Public IPs defined in the Maximum Instance.

Fields	Description
Management Subnet	**Subnet**: Select a management subnet for V Series node. The subnet that is used for communication between the G-vTAP Agents and the V Series nodes, as well as to communicate with GigaVUE-FM. Every fabric node (both controllers and the nodes) needs a way to talk to each other and GigaVUE-FM. So, they should share at least one management subnet.
Data Subnets	The subnet that receives the mirrored VXLAN tunnel traffic from the G-vTAP Agents. Select a **Subnet** and the respective **Security Groups**. Click **Add** to add additional data subnets. **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.
Tag(s)	(Optional) The key name and value that helps to identify the V Series node instances in your Azure environment. For example, you might have V Series node deployed in many regions. To distinguish these V Series node based on the regions, you can provide a name that is easy to identify. To add a tag: **a.** Click **Add**. **b.** In the **Key** field, enter the key. For example, enter Name. **c.** In the **Value** field, enter the key value.

Use the following buttons to manage your Azure connections :

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

To create Application Intelligence sessions, refer to Create an Application Intelligence Session in Virtual Environment.

Refer the following Gigamon Validated Design for more detailed information on how to achieve deep observability in Azure

- Supplementing the Existing Tools to Gain Deep Observability in Azure (5.15)

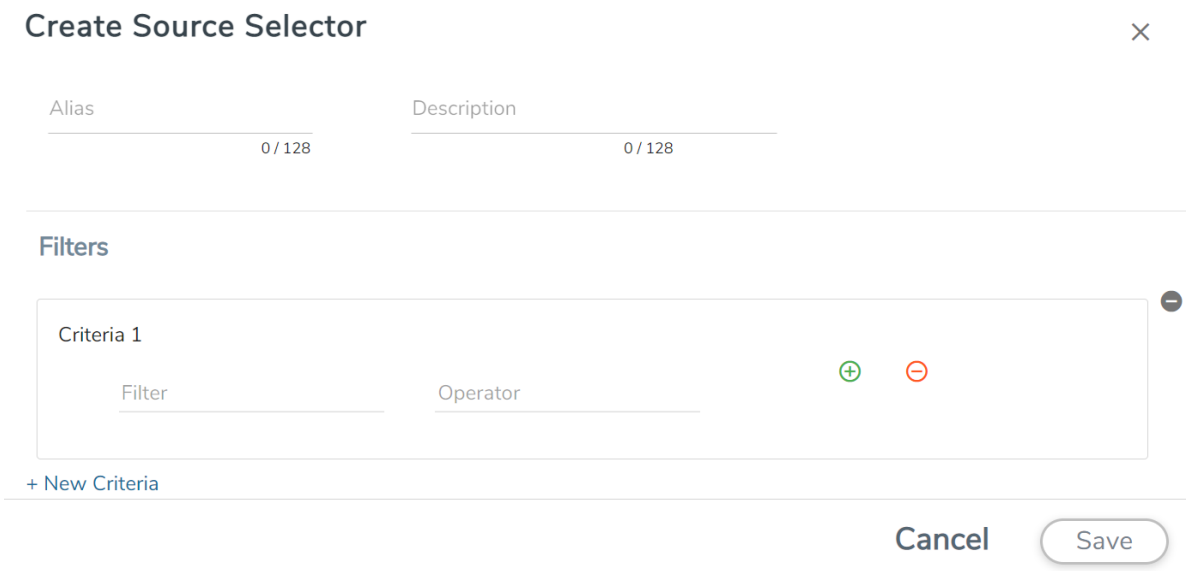
Create Source Selectors

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

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

To configure the Source Selectors:

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



3. Enter or select the required information:

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

4. Click Save to save the source selector.

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

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

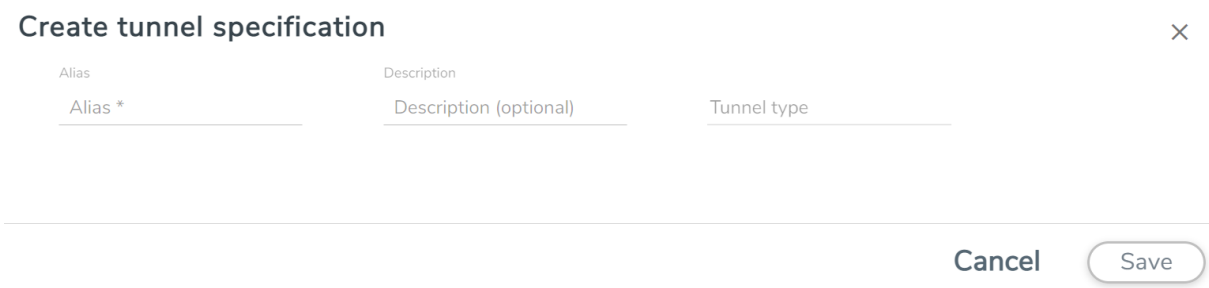
Create Tunnel Specifications

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

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

To configure the tunnels:

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



3. Enter or select the following information:

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

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

User Defined Application

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

To configure User Defined Application signatures :

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

Create Rules under User Defined Application

1. Click **Inventory**.

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

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

4. Enter **Application Name**.

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

Note: The least value will have the highest priority.

6. In the created rule:

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

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

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

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

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

9. Click the **Rule** tab.

10. Select a rule to view its protocol details.

Supported Protocols and Attributes

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

For supported Regex patterns, refer Supported RegExp Syntax

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

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

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

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

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

Mindata

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

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

Supported RegExp Syntax

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

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

Limitations

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

Configure Application Intelligence Session

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

Prerequisites

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

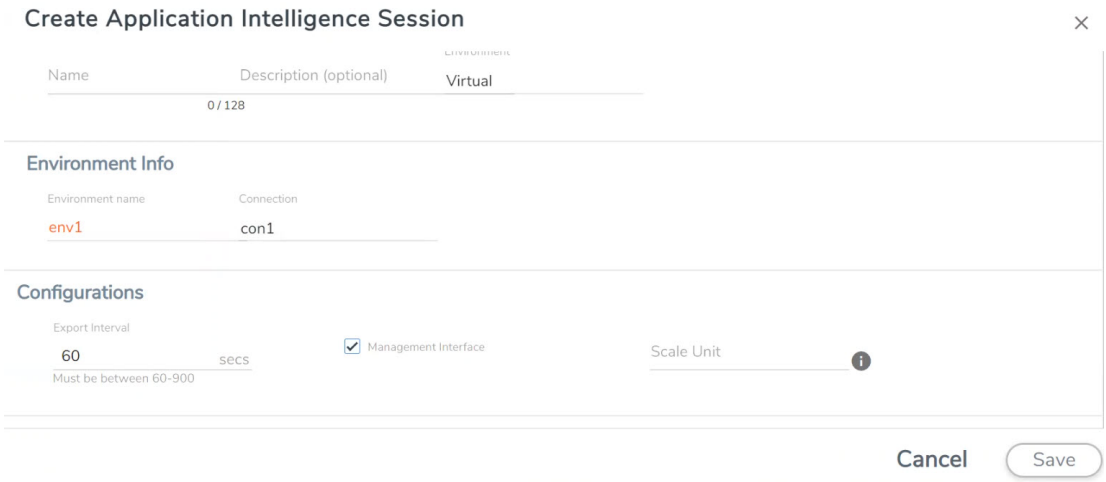
> **NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

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

To create an Application Intelligence Session:

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cloud Health Monitoring

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

Configuration Health Monitoring

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

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

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

For G-vTAP Agents:

- AWS
- Azure
- OpenStack

For VPC Mirroring:

- AWS

For OVS Mirroring and VLAN Trunk Port:

- OpenStack

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

Traffic Health Monitoring

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

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

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware

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

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

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

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

Create Threshold Template

To create threshold templates:

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

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

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

Apply Threshold Template

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

Apply Threshold Template to Monitoring Session

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

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

Apply Threshold Template to Applications

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

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

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

Edit Threshold Template

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

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

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

Clear Thresholds

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

Clear Thresholds for Applications

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

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

Clear Thresholds across the Monitoring Session

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

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds page appears**. Click **Clear**.

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

Supported Resources and Metrics

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

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

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

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

View Health Status

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

View Health Status of the Entire Monitoring Session

To view the health status of a monitoring session:

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

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

View Health Status of an Application

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

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

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

View Health Status for Individual V Series Nodes

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

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

View Application Health Status for Individual V Series Nodes

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

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

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

View Health Status on the Monitoring Session Page

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

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

Health

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

V Series Node Health

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

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

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

Target Source Health

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

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

Fabric Health Analytics for Virtual Resources (BETA)

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

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

Rules and Notes:

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

Virtual Inventory Statistics and Cloud Applications Dashboard

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

To access the dashboards:

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

The following table lists the various virtual dashboards:

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

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

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

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

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

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

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

Administer GigaVUE Cloud Suite for Azure

You can perform the following administrative tasks:

- Set Up Email Notifications
- Configure Proxy Server
- Configure Azure Settings
- Role Based Access Control
- About Events
- About Audit Logs

Set Up Email Notifications

Notifications are triggered by a range of events such as Azure license expiry, VM instance terminated, and so on. You can setup the email notification for a particular event or a number of events and the recipient or recipients to whom the email should be sent.

Gigamon strongly recommends you enable email notifications so there is immediate visibility of the events affecting node health. The following are the events for which you can setup the email notifications:

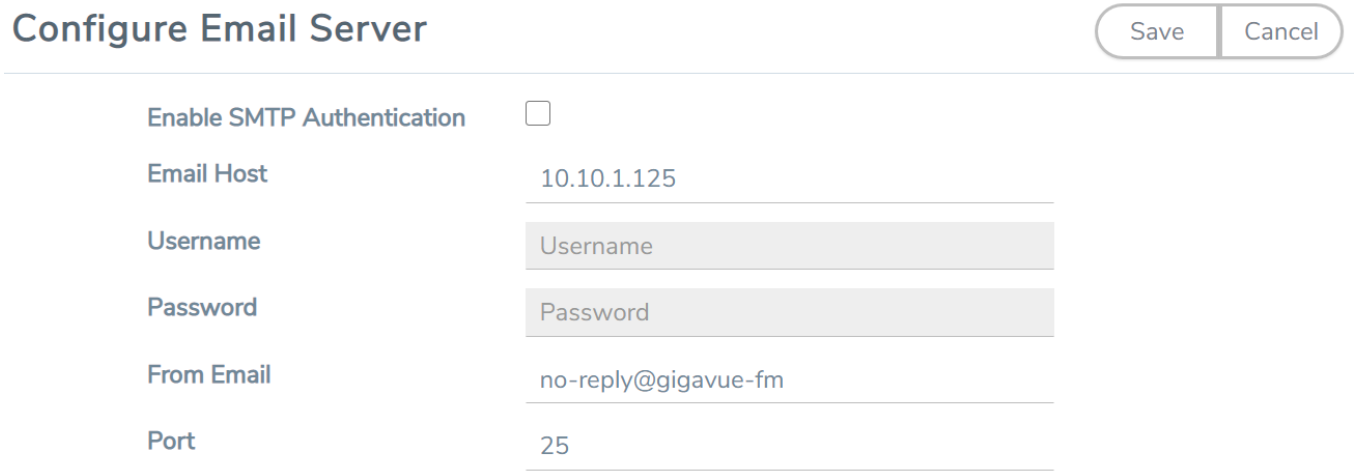
- Azure License Expire
- Fabric Node Down
- Fabric Node Reboot Failed
- Fabric Node Rebooted
- Fabric Node Replacement Launch Failed
- Fabric Node Replacement Launched
- Fabric Node Restart Failed
- Fabric Node Restarted
- Fabric Node Unreachable
- Fabric Node Up

Configure Email Notifications

To configure the automatic email notifications:

1. On left navigation pane, select **Settings > System > Email Servers**. The **Email Servers** page appears.

2. In the Email Servers page, click **Configure**. The **Configure Email Server** wizard appears. For field information, refer to"Email Servers" section in the *GigaVUE Administration Guide*.



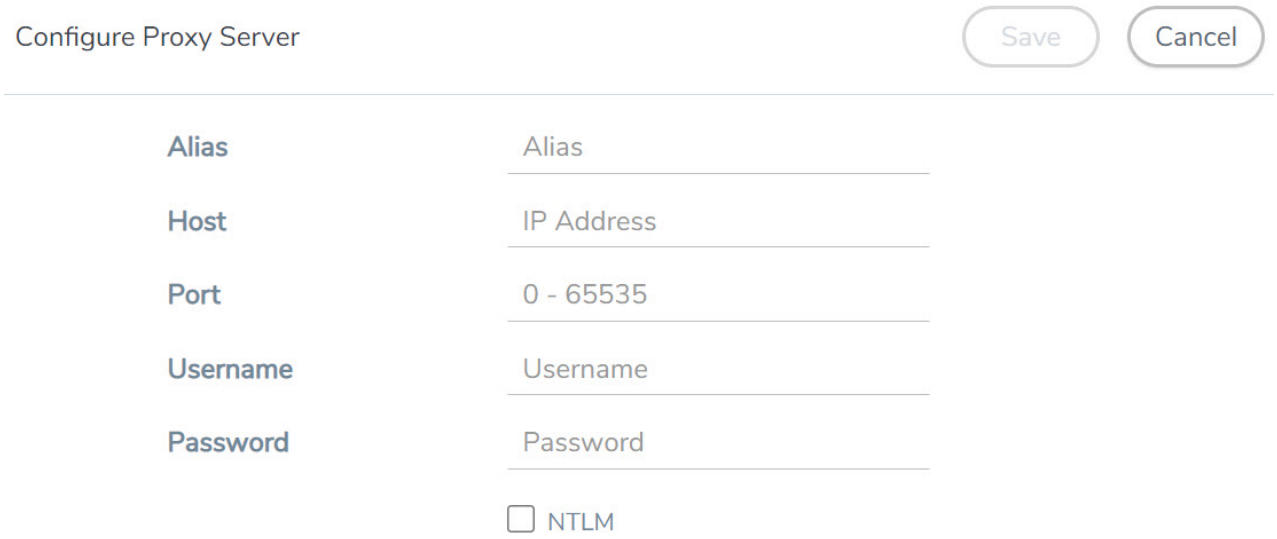
3. Click **Save**.

Configure Proxy Server

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

To create a proxy server:

1. Go to **Inventory > VIRTUAL > Azure**, and then click **Settings > Proxy Server Configuration**. The Proxy Server Configuration page appears.
2. In the **Proxy Server Configuration** page, click **Add**. The **Configure Proxy Server** page appears.



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

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

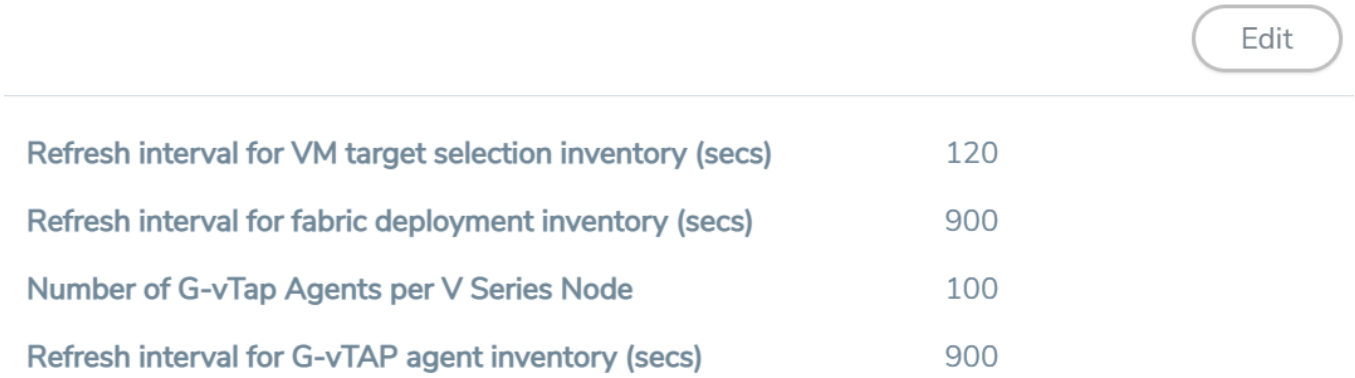
4. Click **Save**. The new proxy server configuration is added to the Proxy Server Configuration page. The proxy server is also listed in the Azure Connection page in GigaVUE-FM.

NOTE: If you change any of the fields in the Proxy Server Configuration page after the initial connection is established between the GigaVUE-FM and Azure, then you must also edit the connection and select the proxy server again and save (in the Azure Connection Page). Otherwise, GigaVUE-FM will not use the new configuration that was saved and may be disconnected from the Azure platform.

Configure Azure Settings

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

Go to **Inventory > VIRTUAL > Azure**, and then click **Settings > Advanced Settings** to edit the Azure settings.



Refer to the following table for more information about the settings:

Settings	Description
Refresh interval for VM target selection inventory(secs)	Specifies the frequency for updating the state of Virtual Machines target selection in Azure.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the state of fabric deployment information such as subnets, security groups, images, and VNets.
Number of G-vTAP Agents per GigaVUE V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node.
Refresh interval for G-vTAP Agent inventory (secs)	Specifies the frequency for discovering the G-vTAP Agents available in the VNet.

Role Based Access Control

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

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

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

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

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

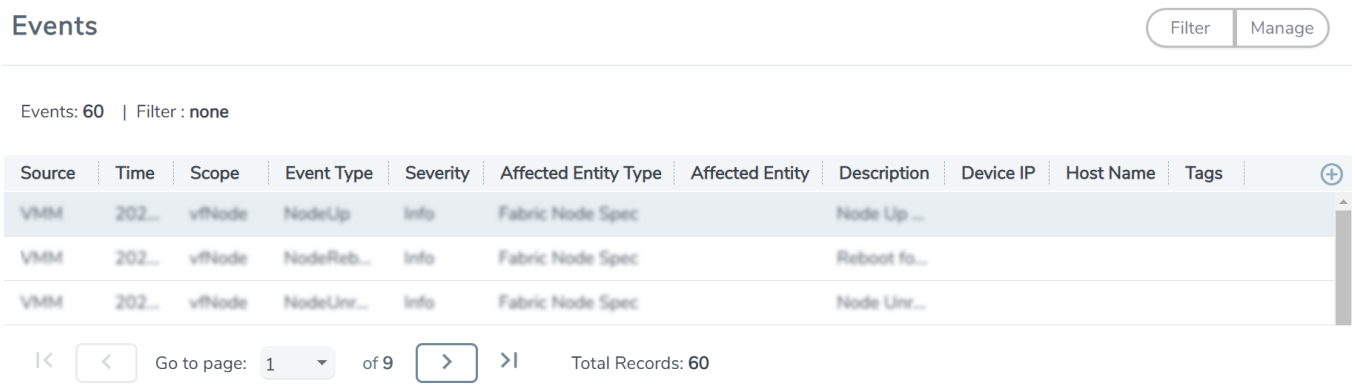
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

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

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

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

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



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

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

Controls/ Parameters	Description
Affected Entity	The resource ID of the affected entity type.
Description	The description of the event, which includes any of the possible notifications with additional identifying information where appropriate.
Device IP	The IP address of the device.
Host Name	The host name of the device.

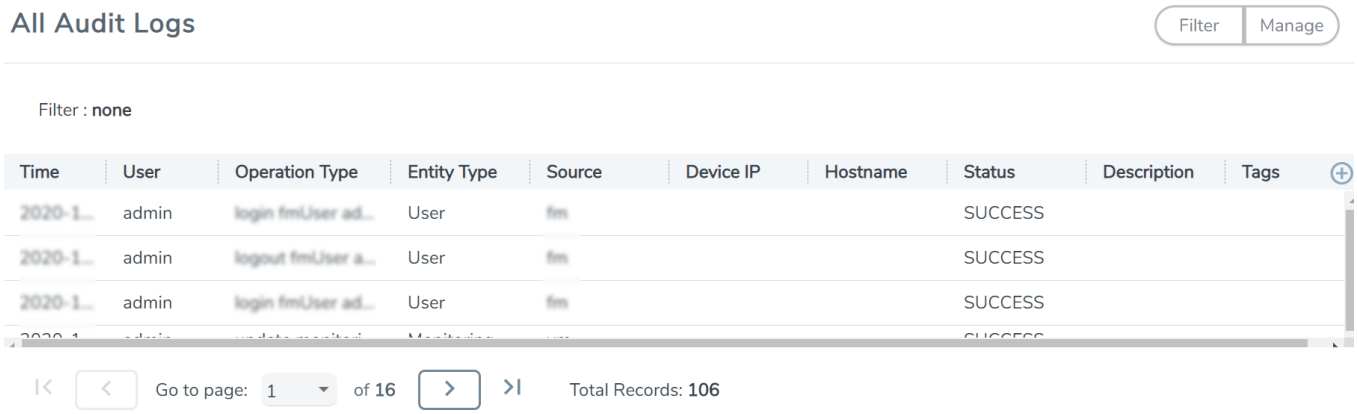
To filter the alarms and event:

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

About Audit Logs

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

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



The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.

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

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

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

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

To filter the audit logs, do the following:

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

GigaVUE-FM Version Compatibility Matrix

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

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

GigaVUE-FM Version Compatibility for V Series 2 Configuration

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

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

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

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA10 Hardware Installation Guide
GigaVUE-TA40 Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA100-CXP Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
***GigaVUE V Series Applications Guide**
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide
***GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide**
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
***GigaVUE Cloud Suite for Third Party Orchestration**
GigaVUE Cloud Suite for AnyCloud Guide
Universal Container Tap Guide
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
GigaVUE Cloud Suite for AWS Secret Regions Guide
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes

GigaVUE Cloud Suite 6.2 Hardware and Software Guides
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	
For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	**Document Title**	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	**Describe the issue**	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? **Be as specific as possible.**	
	Any other comments?	

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The VÜE Community

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

Visit the VÜE site to:

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

- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)