GigaVUE Cloud Suite for Azure Configuration Guide

GigaVUE Cloud Suite

Product Version: 5.10

Document Version: 2.0

(See Change Notes for document updates.)

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
5.10.01	2.0	08/28/2020	Fixed formatting and cross-references issues, and streamlined instructions throughout the guide.
5.10.00	1.0	08/14/2020	Original release of this document with 5.10.00 GA.

Contents

GigaVUE Cloud Suite for Azure

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 Microsoft Azure Cloud.

Refer to the following sections for details:

- About GigaVUE Cloud Suite for Azure
- Prepare Virtual Machines to Monitor Traffic
- Get Started with GigaVUE Cloud Suite for Azure Deployment
- Deploy GigaVUE Cloud Suite for Azure
- Configure and Manage Resources for Traffic flow
- Administer GigaVUE Cloud Suite
- Install and Upgrade GigaVUE-FM
- Compatibility Matrix for Azure

Audience

This guide is intended for users who have basic understanding of Microsoft® Azure. This document expects users to be familiar with Azure implementations and identity management.

License Information

The GigaVUE Cloud Suite Cloud suite is available in both the public Azure cloud and in Azure Government, and supports the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG) model that you can avail from the Azure Marketplace.

Bring Your Own License (BYOL)

The licenses for the BYOL option can be purchased based on the number of TAP points and the term of the license. Gigamon offers the following options for purchasing the license:

- Traffic visibility for up to 100 virtual TAP points (NICs)

- Traffic visibility for up to 1000 virtual TAP points (NICs)

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

The minimum term for the license is 3 months.

A free trial is made available in the Azure Marketplace. The trial version provides traffic visibility for up to 10 virtual TAP points for 30 days. When a new license is purchased, the 10 virtual TAP points are replaced with the TAP points the licensing option supports.

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

Pay-As-You-Go (PAYG)

The Pay-As-You-Go (PAYG) option is available in the Azure Marketplace. The PAYG option charges the users for the Azure services availed on an hourly basis. For example, Azure charges the users for the period the GigaVUE-FM VM and the rest of the solution components are running. When the VMs stop, Azure stops charging the users. The PAYG model has no term contract.

It is a perpetual license that supports up to 100 TAP points. To support additional TAP points, licenses must be purchased from Gigamon.

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

Apply Licensing

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

Install and Upgrade GigaVUE-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 simply launch the GigaVUE-FM instance in your VNet. For installing the GigaVUE-FM instance, refer to Get Started with GigaVUE Cloud Suite for Azure Deployment.

> **NOTE:** You cannot upgrade your current version of the GigaVUE-FM instance deployed in Azure environment to GigaVUE-FM 5.8.00. You must perform a fresh installation of GigaVUE-FM 5.8.00.

- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to *GigaVUE-FM Installation and Upgrade Guide* available in the Customer Portal.

Overview of GigaVUE Cloud Suite for Azure

This chapter introduces the components of the GigaVUE Cloud Suite for Azure and the supported architecture. Refer to the following sections for details:

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

About 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:

- GigaVUE-FM
- GigaVUE V Series node
- GigaVUE V Series controller
- GigaVUE Cloud Suite G-vTAP controller

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.

You can choose one of the following two options for configuring the components described above:

Option 1: Standard Configuration	GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in all VNets
Option 2: Shared Controller Configuration	GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in a shared VNet
	NOTE: Peering must be active between VNets within the same monitoring domain if the shared controller and V Series option is chosen for configuring the components.

This guide provides instructions on launching GigaVUE-FM in Azure. For information about installing GigaVUE-FM in your enterprise data center, refer to the "Installation and Upgrade" section in the *GigaVUE-FM and GigaVUE Cloud Suite for VMware Configuration Guide* available in the Customer Portal.

Architecture of GigaVUE Cloud Suite for Azure

The GigaVUE Cloud Suite for Azure supports many deployment modes. The following cloud deployment models are the most common:

- Hybrid Cloud
- Multi-VNet Cloud
- Shared Controller/GigaVUE V Series Node Configuration

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.
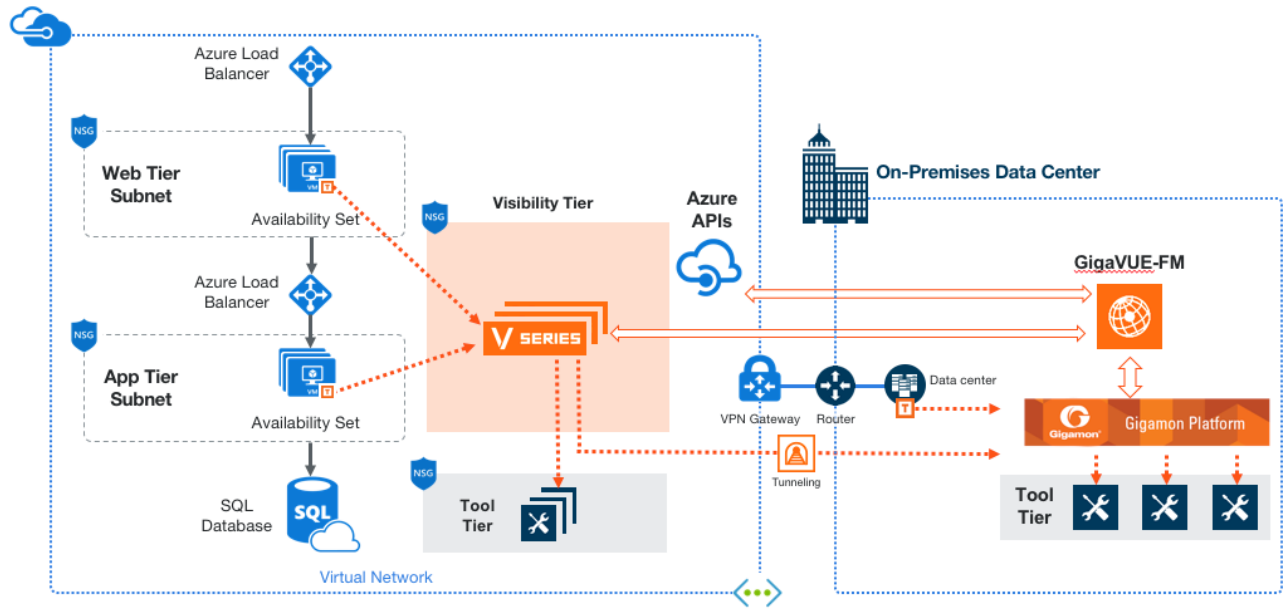
Multi-VNet Cloud

In the public cloud deployment model, you can send the customized traffic from a single VNet to the tools residing in the same VNet or from multiple VNets to the tools residing in a different, shared VNet.
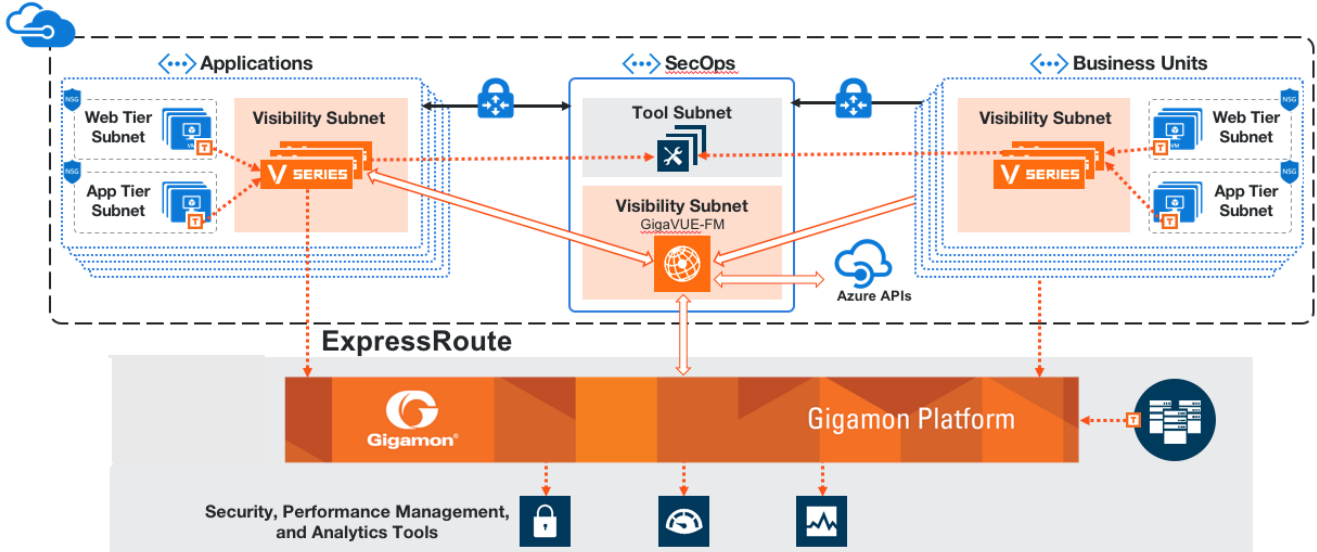
Shared Controller/GigaVUE V Series Node Configuration

In the shared controller and V Series node deployment model, the following Gigamon components are deployed in a shared VNet:

- G-vTAP Controllers
- GigaVUE V Series Controllers
- GigaVUE V Series nodes

With this deployment model it is easy to manage the controllers and nodes as they are launched from a shared VPC (thereby, reducing the cost involved in the configuration and management of the controllers and nodes in each VPCs).
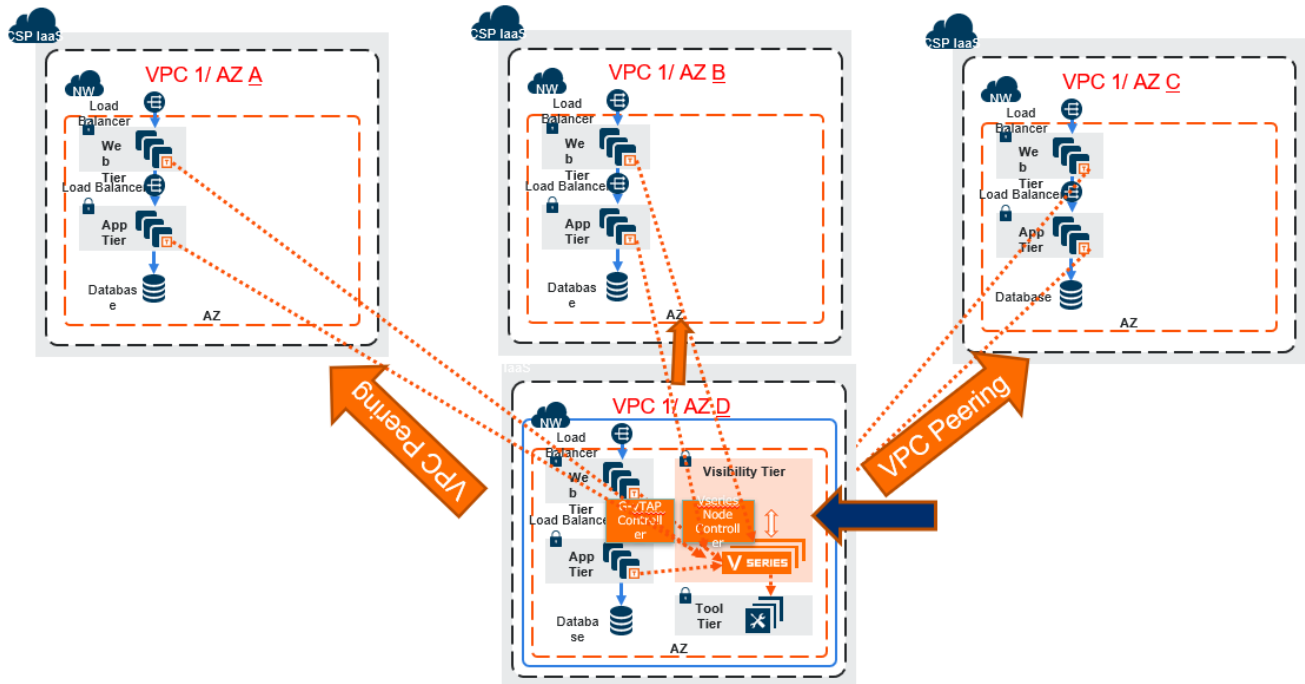
Role Based Access Control

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 for Azure 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 for Azure 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 Components in Azure • Create Monitoring Domain and Launch Visibility Fabric • Configure Proxy Server
Traffic Control Management: This includes the following traffic control resources: • Monitoring session • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• Create, Clone, and Deploy Monitoring Session • Add Applications to Monitoring Session • Create Maps • View Statistics • Create Tunnel End Points

NOTE: Cloud APIs are also RBAC enabled.

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

Get Started with GigaVUE Cloud Suite for Azure Deployment

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
- Deploy GigaVUE Cloud Suite for Azure

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.

- Network Requirements
- Network Security Groups

Network Requirements

To enable the flow of traffic between the components and the monitoring tools, your VNets and VMs should meet the following requirements:

- Subnets for VNet
- Network Interfaces (NICs) for VMs

Subnets for VNet

Table 1: Types of Subnets lists the two recommended subnets that your VNet must have to configure the GigaVUE Cloud Suite Cloud components in Azure.

Table 1: Types of Subnets

Subnet	Description
Management Subnet	Subnet that the GigaVUE-FM uses to communicate with the GigaVUE Cloud Suite 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.

Subnet	Description
	• Ingress is VXLAN from agents
	• Egress is either VXLAN tunnel to tools or to GigaVUE H 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.

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 Cloud Suite V Series Controllers, GigaVUE Cloud Suite 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.

It is recommended to create a separate security group for each component using the rules and port numbers listed in Table 2: Security Group Rules .

Table 2: Security Group Rules

Direction		Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
GigaVUE-FM Inside Azure					
Inbound	HTTPS	TCP(6)	443	Anywhere Any IP	Allows G-vTAP Controllers, GigaVUE Cloud Suite V Series Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM

Direction		Protocol	Port Range	Source and CIDR, IP, or Security Group	Purpose
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP agents
GigaVUE Cloud Suite V Series Controller					
Inbound	Custom TCP Rule	TCP	9902	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite V Series Controllers
GigaVUE Cloud Suite V Series node					
Inbound	Custom TCP Rule	TCP	9903	Custom GigaVUE V Series Controller IP	Allows GigaVUE Cloud Suite V Series Controllers to communicate with GigaVUE Cloud Suite V Series nodes
VXLAN Traffic					
Inbound	Custom UDP Rule	VXLAN	4789		Allows mirrored traffic from G-vTAP agents to be sent to GigaVUE Cloud Suite V Series nodes using VXLAN tunnel Allows monitored traffic to be sent from GigaVUE Cloud Suite V Series nodes to the tools using VXLAN tunnel

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 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 in Azure Public Cloud

GigaVUE Cloud Suite Cloud is available in the Azure Marketplace for both the Bring Your Own License (BYOL) and the Pay-As-You-Go (PAYG) options.

GigaVUE Cloud Suite 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.

Deploy GigaVUE Cloud Suite for Azure

Launch GigaVUE-FM VM from Azure

The GigaVUE-FM can be launched from the Azure VM dashboard or Azure Marketplace. The following instructions describe launching the GigaVUE-FM from the Azure VM Dashboard. This section describes how to launch the GigaVUE-FM in your VNet.

To launch the GigaVUE-FM:

1. Login to the Azure portal and select **Virtual Machines**.
2. Click **Add** and in the Compute tile, search for Gigamon.
3. Locate the latest version of the GigaVUE-FM, click **Create**.
4. Enter the Basic settings.
   a. Choose either the **SSH public key** or **password authentication type for SSH access**.
   b. Select the appropriate **Subscription** and **Location**.
5. Choose the Virtual Machine size.
   a. The recommended VM type is **D4S_V3 Standard**.
   b. Click **Select**.

6. Select the appropriate **Virtual Network** (VNet), **Subnet**, and **Public IP Address**.Select the **Network Security Group** created to allow GigaVUE-FM to communicate with the rest of the components. Click **Ok**.

7. Verify the summary and click **Create**.

8. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface as follows:

    a. Find your VM and expand the page in the **Descriptions** tab to view the VM information.

    b. Copy the Public DNS value and paste it into a new browser window or tab.

    c. If GigaVUE-FM is deployed in Azure, use admin123A!! as the password for the admin user to login to GigaVUE-FM. It is highly recommended to change the password after logging in to GigaVUE-FM.

> **NOTE:** For security reasons, it is **highly recommended** to change the password after logging in to GigaVUE-FM.

Prepare Virtual Machines to Monitor Traffic

A **G-vTAP agent** is an agent that is deployed in the VMs. This agent mirrors the selected traffic from the VMs (virtual machines), encapsulates it using GRE or VXLAN tunneling, and forwards it to the GigaVUE Cloud Suite® V Series node.

A G-vTAP agent consists of a source interface and a destination interface. The network packets collected from the source interface are sent to the destination interface. From the destination interface, the packets traverse through the L2 GRE or VXLAN tunnel interface to the GigaVUE Cloud Suite V Series node.

A source interface can be configured with one or more 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 or ingress or both.

Refer to the following sections for more information:

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

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

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.

Using a single NIC as the source and the destination interface can sometimes cause increased latency in sending the traffic out from the VM.

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

Example—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. One NIC can be configured as the source interface and another NIC 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 configuration:

Example—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
```

Windows Agent Installation

To install the Windows agent:

1. Download the Windows agent package.
2. Extract the contents of the .zip file into a convenient location.
3. Run 'NPCAP_4_1_3.exe' (located in the 'npcap' folder) as **Administrator**.
4. Run 'install.bat' as **Administrator**.
5. To start the Windows G-vTAP agent, perform one of the following actions:

   - Reboot the VM.
   - Run 'sc start gvtap' from the command prompt.
   - Start the G-vTAP Agent from the Task Manager.

Refer to Create Images with the Agent Installed.

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

Install IPSec on G-vTAP Agent

If IPSec is used to establish secure connection between G-vTAP agents and GigaVUE V Series nodes, then you must install IPSec on G-vTAP agent instances. To install IPSec on G-vTAP agent you need the following files:

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

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

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

- Install from Ubuntu/Debian Package
- Install from Red Hat Enterprise Linux and Centos
- Install from Red Hat Enterprise Linux and Centos with Selinux Enabled

Install from Ubuntu/Debian Package

1. Launch the Ubuntu/Debian image.
2. Copy the G-vTAP package files and strongSwan TAR file to the G-vTAP agent:
   - strongswan5.3.5-1ubuntu3.8_amd64-deb.tar.gz
   - gvtap-agent_1.7-1_amd64.deb
   - gvtap-ipsec_1.7-1_amd64.deb
3. Install the G-vTAP agent package file:
   ```
   sudo dpkg -i gvtap-agent_1.7-1_amd64.deb
   ```
4. Modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces:
   ```
   eth0# mirror-src-ingress mirror-src-egress mirror-dst
   sudo /etc/init.d/gvtap-agent restart
   sudo /etc/init.d/gvtap-agent status
   ```

> **NOTE:** You can view the G-vTAP log using `cat /var/log/gvtap-agent.log` command.

5. Install strongSwan:
   ```
   tar -xvf strongswan5.3.5-1ubuntu3.8_amd64-deb.tar.gz
   cd strongswan-5.3.5-1ubuntu3.8_amd64/
   sudo sh ./swan-install.sh
   ```
6. Install IPSec package:
   ```
   sudo dpkg -i gvtap-ipsec_1.7-1_amd64.deb
   ```

Install from Red Hat Enterprise Linux and Centos

1. Launch RHEL/Centos agent image.
2. Copy the following package files and strongSwan TAR files to the G-vTAP agent:
   - strongswan-5.7.1-1.el7.x86_64.tar.gz for rhel7/centos7
   - strongswan-5.4.0-2.el6.x86_64.tar.gz for rhel6/centos6
   - gvtap-agent_1.7-1_x86_64.rpm
   - gvtap-ipsec_1.7-1_x86_64.rpm
3. Install G-vTAP agent package:
   ```
   sudo rpm -ivh gvtap-agent_1.7-1_x86_64.rpm
   ```
4. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:
   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   # sudo /etc/init.d/gvtap-agent restart
   ```
5. Install strongSwan:
   ```
   tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
   cd strongswan-5.7.1-1.el7.x86_64
   sudo sh ./swan-install.sh
   ```

6. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_1.7-1_x86_64.rpm
   ```

> **NOTE:** You must install IPSec package after installing StrongSwan.

Install from Red Hat Enterprise Linux and Centos with Selinux Enabled

1. Launch the RHEL/Centos agent image.
2. Copy package files and strongSwan TAR file to G-vTAP agent.
   - strongswan-5.7.1-1.el7.x86_64.tar.gz for rhel7/centos7
   - strongswan-5.4.0-2.el6.x86_64.tar.gz for rhel6/centos6
   - gvtap-agent_1.7-1_x86_64.rpm
   - gvtap-ipsec_1.7-1_x86_64.rpm
   - gvtap.te and gvtap_ipsec.te files (type enforcement files)
3. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
4. Checkmodule -M -m -o gvtap_ipsec.mod gvtap_ipsec.te
   ```
   semodule_package -o gvtap_ipsec.pp -m gvtap_ipsec.mod
   sudo semodule -i gvtap_ipsec.pp
   ```
5. Install G-vTAP agent package:
   ```
   sudo rpm -ivh gvtap-agent_1.7-1_x86_64.rpm
   ```
6. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:
   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   # sudo /etc/init.d/gvtap-agent restart
   ```
7. Install strongSwan:
   ```
   tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
   cd strongswan-5.7.1-1.el7.x86_64
   sudo sh ./swan-install.sh
   ```
8. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_1.7-1_x86_64.rpm
   ```

Create Images with 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 an 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:

1. From the Azure console, click the VM.
2. Click **Image** > **Create Image**.
3. There may be extra steps required from Azure to deprovision the VM. Refer to Azure documentation for capturing an image: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/capture-image.

Configure Components of GigaVUE Cloud Suite for Azure

You must establish a connection between GigaVUE-FM and your Azure environment before you can perform the configuration steps. After a connection is established, you will be able to use GigaVUE-FM to specify a launch configuration for the G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE V Series nodes in the specified VNet and Resource Groups.

Refer to the following topics for details:

- Pre-Configuration Checklist
- Configure G-vTAP Controllers
- Configure GigaVUE Cloud Suite V Series Controllers
- Configure GigaVUE Cloud Suite V Series Nodes

Pre-Configuration Checklist

 Table 3: Pre-configuration Checklist provides information that you must obtain to ensure a successful and efficient configuration using the GigaVUE-FM user interface:

Table 3: Pre-configuration Checklist

	Required Information
☐	VNet ID(s) **NOTE:** In the portal, VNet ID is available under Properties as Resource ID. You can get the VNet ID from the URL https://resources.azure.com. You can also find the VNet ID from Azure PowerShell or use Azure CLI.
☐	VNet Peering **NOTE:** Peering must be active between VNets within the same monitoring domain. This is required only when shared controller option is chosen for configuring the components.
☐	Resource Group ID(s)
☐	VM ID of GigaVUE-FM
☐	Public or Private IP of GigaVUE-FM
☐	Static Public IP **NOTE:** If GigaVUE-FM is installed in the enterprise data center, a Public IP is required for G-vTAP controllers and GigaVUE Cloud Suite V Series controllers to communicate with GigaVUE-FM

	Required Information
☐	Region name for the VNet
☐	Application ID, Tenant ID, Application Secret and Subscription ID
☐	Subnets
☐	Network Security groups

Establish connection to Microsoft Azure

When you first connect GigaVUE-FM with 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 authentication with Azure:

- **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 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.
- **Managed Service Identity**—Managed Service 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.

Connect to Microsoft Azure

GigaVUE-FM connects to Azure using either an Application ID with the client secret or the MSI method of authentication. Once the connection is established, GigaVUE-FM launches the G-vTAP Controller, GigaVUE V Series Controller, and GigaVUE V Series node.

To connect to Azure using GigaVUE-FM:

1. Click **Cloud** in the top navigation link.
2. Under Azure, select **Configuration > Connections**, and then click the **New** drop-down menu. You can either create a new monitoring domain or a new connection.
   - If you select **Monitoring Domain**, then the **Create Monitoring Domain** dialog box is displayed. Enter the alias that is used to identify the monitoring domain.
   - If you select **Connection**, then the **Azure Connection** page is displayed. You can either create a new monitoring domain for the connection or select an existing monitoring domain that is already created.
3. Enter or select the appropriate information for the VNet and one or more Resource Groups. If the Authentication type of Application ID with Client Secret is used, have the **Subscription ID**, **Tenant ID**, **Application ID** and **Application Secret** information ready based on the Azure connectivity section mentioned above. Select the required **Tapping Method**.

> **NOTE:** If you select Azure vTAP as tapping method, then you need not configure the G-vTAP controller as described in section Configure G-vTAP Controllers.

4. Click **Save**.
5. If the connection is established, the status is displayed as 'Connected' in the Connections page. GigaVUE-FM discovers the inventory of the VNet in the background. If the connection fails, a 'Connection Failed' error message is displayed when **Save** is clicked.

Once the configuration in the Connections tab is complete, the rest of the tabs under **Cloud > Azure > Configuration** can be configured so that GigaVUE-FM can deploy the rest of the solution components. As a final step, configure the monitoring session.

GigaVUE-FM Supports two types of authentication with Azure, which are described in the following sections:

- Managed Service Identity (MSI)
- Custom Roles
- Pre-defined Roles
- Accept EULA and Enable Programmatic Deployment in Azure

Managed Service Identity (MSI)

> **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 service identity is only available for GigaVUE Cloud Suite-FMs launched inside Azure. 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, each of which is described below.

Enable MSI using the CLI

1. Custom role at resource group level using CLI (recommended) where you will deploy fabric to:

   ```
   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, (for fabric nodes, NOT the public images) then you have to assign permissions to the RG those live in as well. 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. Custom role at the subscription level using CLI. This will assign the role at the subscription level, you can see everything in the account:

   ```
   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
   ```

4. Assign role using the Portal:
    a. Enable MSI for the GigaVUE-FM VM and use the portal to assign a role later:

    ```
    az vm identity assign -g <your resource group> -n <your fm vm name>
    ```

    b. If needs to create resource groups, MSI permissions must be assigned at the subscription level.
        i. Subscriptions > Your subscription
        ii. Click Access Control (IAM)
        iii. Click Add (if Add button is not available, then you do not have the required permissions)
        iv. Select the GigaVUE-FM custom role Contributor role.
        v. Select Virtual Machine for Assign access to
        vi. Select your subscription
        vii. Select the Resource Group of the VM you would like to add permissions for
        viii. Select the instance running GigaVUE-FM.
    c. If all resource groups are pre-created, permissions for GigaVUE-FM managed service identity can be assigned at the resource group level.
        i. Go to the resource group you would like to add permissions for the MSI in the Azure portal
        ii. Click Access Control (IAM)
        iii. Click Add (if Add button is not there you do not have proper permissions)
        iv. Select Reader/Virtual Machine Contributor/Network Contributor/Storage Account Contributor role or whatever Role you want
        v. Select Virtual Machine for Assign access to
        vi. Select your subscription
        vii. Select the Resource Group of VM you would like to add permissions for
        viii. Select the instance running GigaVUE-FM
        ix. Fabric nodes can be deployed in different resource groups. Make sure you assign the proper permissions for each resource group.

Now you can enable MSI using the Portal.

Enable MSI Using the Portal

You can enable MSI at the time of launching GigaVUE-FM through the portal. In step 3 of VM creation, an option is available to enable MSI.

Click **Yes**. You still need to add permissions for the Resource Groups in this VM (which you want GigaVUE-FM to see):

If you already launched your GigaVUE-FM in the portal and did not enable MSI, you can still enable MSI in the portal. Click on your VM, open the blade for "Configuration," and then click **Yes** to Register the VM with AD:
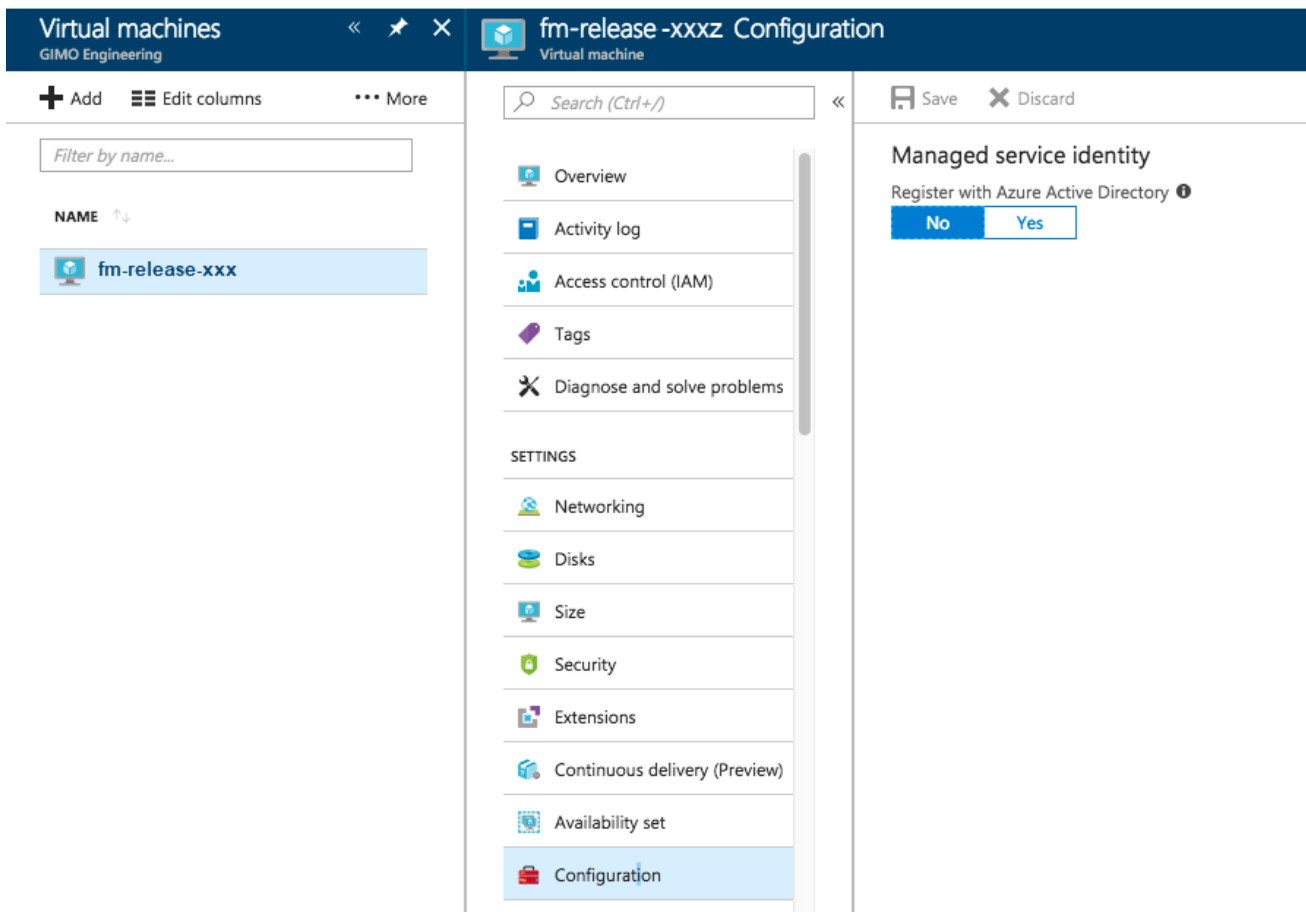
Once that is done, you can select the required resource for which you want to give the GigaVUE-FM permissions (Subscription level, resource group level, etc). Click the object and then select the "Access Control IAM" blade:
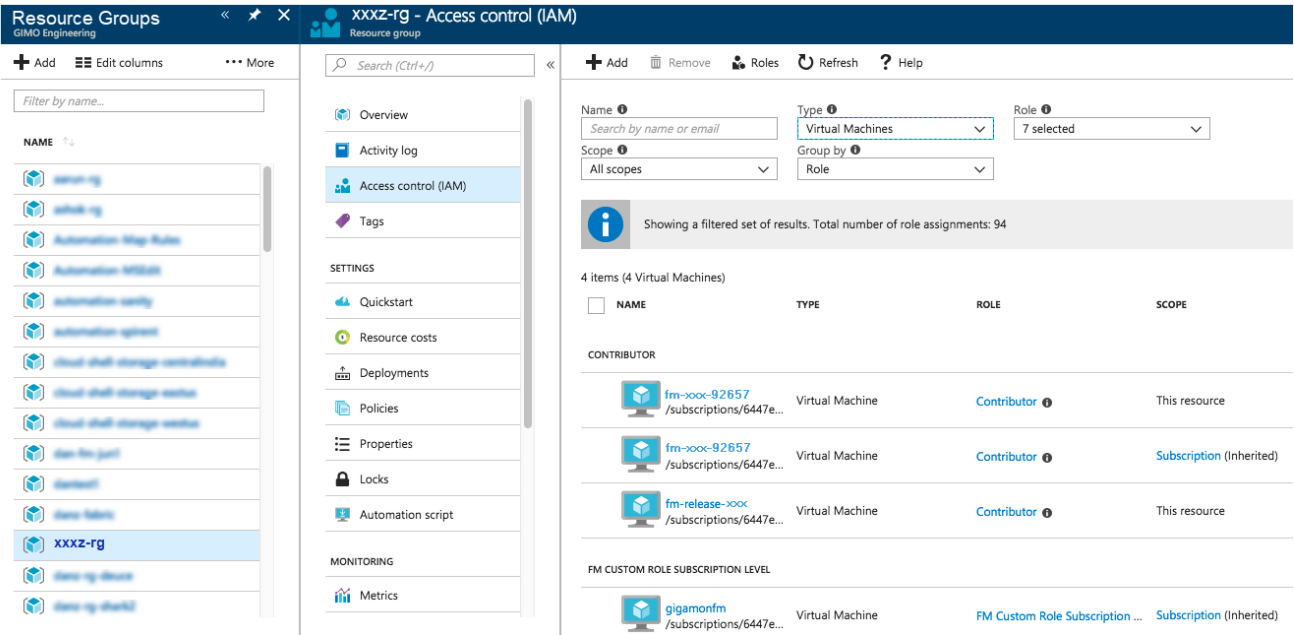
Search by Type "Virtual Machines". Your VM should not be there yet.

Click the Add button, and find your VM, select a Role, and Save. This will give the VM the required permissions the role has on the object you selected earlier. In the example above, a Resource Group.

Application ID with Client Secret

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.

> **NOTE:** GigaVUE-FM must be able to resolve "login.microsoftonline.com" in order to connect to Azure. So GigaVUE-FM must be configured with a valid DNS server.

Perform the following steps to create the service principal and get the required information to create the Azure connection in GigaVUE-FM:

1. Create a service principal using the Azure CLI: az ad sp create-for-rbac --name myRealName-app.

> **NOTE:** Azure generates the password automatically for the service principle.

  This will return an output similar to:

```
{
"appId": "a487e0c1-82af-47d9-9a0b-af184eb87646d",
"displayName": "myRealName-app",
"name": "http://myRealName-app",
"password": "6266bc73-4b33-4651-8652-298c7180fffa",
"tenant": "tttttttt-tttt-tttt-tttt-tttttttttttt"
}
```

Note the appId and password from the output.

2. Azure CLI: az account show -o json (you have to use the "-o json" option to display the full details)

This will return output similar to:

```
{
"environmentName": "AzureCloud",
"id": "6447xxx11-1x11-111x-11xx-11x11xx11111",
"isDefault": true,
"name": "XYZ Subscription",
"state": "Enabled",
"tenantId": "ad46cbb4-441b-4e7d-a40e-c08ff7dedaf0",
"user": {
"name": "name@yourcompany.com",
"type": "user"
}
}
```

Note the id and tenantId.

3. The Azure connection POST should be populated with the following fields:

```
{
"alias": "<yourConnectionName>",
"authType": "clientSecret",
"regionName": "westus",
"subscriptionId": "<id from az account show>",
"tenantId": "<tenantId from az account show>",
"applicationClientId": "<appId from service principal creation>",
"applicationSecretKey": "<password from the service principal creation>",
"virtualNetworkName":"<virtual network name for connection domain>"
}
```

Example of the UI input:

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 Cloud Suite V series controller and G-vTAP controllers are placed. Without the GigaVUE Cloud Suite V series controller and G-vTAP controllers you would only see images in the marketplace.

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.

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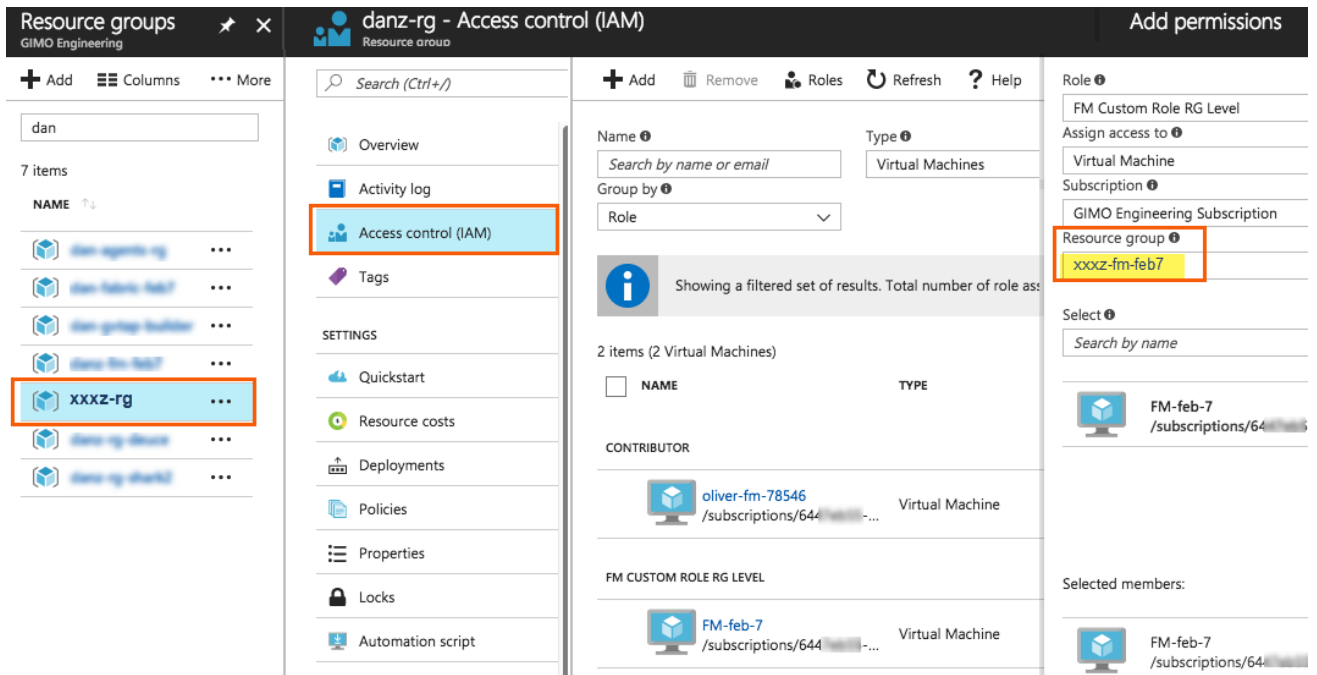
You can also use the CLI to perform the same process. This adds the GigaVUE-FM instance in RG "xxx-feb8-fm" to have access to another RG called "xxxz-rg":

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-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -
   Product "gigamon-fm-5_4_00_hourly" -Name "GigaSECURE Cloud 5.4.00
   Hourly (100 pack)" | Set-AzureRmMarketplaceTerms -Accept
   ```
   b. BYOL FM:

   ```
   Azure:/

   PS Azure:\> Get-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -
   Product "gigamon-fm-5_4_00" -Name "GigaSECURE Cloud 5.4.00" | Set-
   AzureRmMarketplaceTerms -Accept
   ```
   c. Fabric Images (need to accept on all 3):

   ```
   Azure:/

   PS Azure:\> Get-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -
   Product "gigamon-fm-5_4_00" -Name "gvtap-cntlr" | Set-
   AzureRmMarketplaceTerms -Accept


   Azure:/

   PS Azure:\> Get-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -
   Product "gigamon-fm-5_4_00" -Name "vseries-cntlr" | Set-
   AzureRmMarketplaceTerms -Accept


   Azure:/

   PS Azure:\> Get-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -
   Product "gigamon-fm-5_4_00" -Name "vseries-node" | Set-
   AzureRmMarketplaceTerms -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.

Configure G-vTAP Controllers

A G-vTAP Controller manages multiple G-vTAP agents and orchestrates the flow of mirrored traffic to GigaVUE Cloud Suite 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. For example, the G-vTAP Controller v1.7 can only manage G-vTAP agents v1.7. So, if you have G-vTAP agents v1.6 still deployed in the VM machines, you must configure both G-vTAP Controller v1.7 and v1.6.

While configuring the G-vTAP Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the G-vTAP agents to the GigaVUE Cloud Suite V Series nodes. The tunnel type must be VXLAN.

To configure the G-vTAP Controllers:

1. Click **Cloud** in the top navigation link.
2. Under Azure, click **Configuration > G-vTAP Controllers**.
3. Click **New**. The G-vTAP Configuration page is displayed.

Connection	conn1
Virtual Network ID	/subscriptions/6447eb55-9d09-481b-89bc-52e96bb52823/resourceGroups/mapruletraffic/providers/Microsoft.Network/virtualNetworks/mapruletraffic-vnet
Authentication Type	sshPublicKey
SSH Public Key	Enter your SSH Public Key
Resource Group	○ Create New ◉ Use Existing
	Select a resource group
Disk Type	SSD
Controller Version(s)	Add

Image	gigamon-inc-gvtap-cntlr-1.7-1	
Size	Standard_B1s	
Number of Instances	1	

Management Subnet		
Subnet	Select management subnet	
Network Security Groups	Select network security group	
Accelerated Networking	☐	

Additional Subnet(s)	Add
Tag(s)	Add
Use Public IP	☐
Agent Tunnel Type	VxLAN
G-vTAP Agent Tunnel MTU	1450

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

Fields	Description
Connection	The name of the Azure connection. **NOTE:** For shared controller configuration, you must select the required connection for configuring the G-vTAP Controller. Peering must be active in the selected connection to allow the rest of the connections containing the V-series nodes to be monitored.
Authentication Type	Enter the password or SSH Key.
SSH Public Key	Paste in the SSH public key.
Resource Group	Select Create New or Use Existing. To use Existing, select the existing resource group you wish to use.
Disk Type	SSD or HDD (SSD is the default and recommended disk type)

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. This is because the G-vTAP Controller v1.7 can only manage G-vTAP agents v1.7. Similarly, the G-vTAP Controller v1.6 can only manage G-vTAP agents v1.6.
	
	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 multiple versions of G-vTAP Controllers:
	
	   a. Under **Controller Versions**, click **Add**.
	   b. From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP agents installed in the instances.
	   c. From the **Size** down-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.

Controller Version (s) (continued)	An older version of G-vTAP Controller can be deleted once all the G-vTAP agents are upgraded to the latest version. To delete a specific version of G-vTAP Controller, click **x** (delete) next to its G-vTAP Controller image. Once you delete a G-vTAP Controller image from the G-vTAP Configuration page, all the G-vTAP Controller instances of that version are deleted from Azure.
Management Subnet	**Subnet**: 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. This is a required field. Every fabric node (both controllers and the nodes) need a way to talk to each other and FM. So they should share at least one management plane/subnet. **Network Security Groups**: The security group created for the G-vTAP Controller. For example, sg_gvtap-controller. For more information, refer to Network Security Groups. **Accelerated Networking**: If you select this option, GigaVUE-FM will filter out the supported

Fields	Description
	VM sizes in the list to choose from. **NOTE:** Some instance types are supported in Azure platform. Refer to Microsoft 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.
Use Public IP	The IP address type. Select one of the following: • Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the G-vTAP Controller 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.
Agent Tunnel Type	The type of tunnel used for sending the traffic from G-vTAP agents to GigaVUE Cloud Suite V Series nodes. Azure only supports VXLAN tunneling.
G-vTAP Agent MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP agent to the GigaVUE Cloud Suite 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. If Secure Mirror Traffic option is enabled, then to minimize fragmentation you must configure MTU value for G-vTAP agent as follows: With agent tunnel type L2GRE: • If secure tunnel is enabled, MTU must be set as 1405. • If secure tunnel is not enabled, MTU must be set as 1447 With agent tunnel type VXLAN: • If secure tunnel is enabled, MTU must be set as 1397 • If secure tunnel is not enabled, MTU must be set as 1450. **NOTE:** For Azure, platform MTU is 1500.

5. Click **Save**.
6. To view the G-vTAP Controllers connection status, click **Visibility Fabric > G-vTAP Controllers**.

The G-vTAP Controller instance takes a few minutes to fully initialize. After the initialization is complete, the connection status is displayed as **OK**.

The G-vTAP Controller launch is displayed as an event in the **Cloud > Events** page.

To view the G-vTAP Controllers launched in your VNet:

1. Login to the Azure account and select **Services > VM**.
2. In the left navigation pane, click **Instances**. The G-vTAP Controllers launched in your VNet is displayed in the Instances page.

Configure GigaVUE Cloud Suite V Series Controllers

GigaVUE Cloud Suite V Series Controller manages multiple GigaVUE Cloud Suite V Series nodes and orchestrates the flow of traffic from GigaVUE Cloud Suite V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Cloud Suite V Series Controllers to communicate with the GigaVUE Cloud Suite V Series nodes.

> **NOTE:** A single GigaVUE Cloud Suite V Series Controller can manage up to 100 GigaVUE Cloud Suite V Series nodes. The recommended minimum instance type is Standard_B1s for V Series Controller.

To configure the GigaVUE Cloud Suite V Series Controller, do the following:

1. Select **Azure > Configuration > V Series Controllers**.
2. Click **New**. The V Series Controller Configuration page opens.

V Series Controller Configuration	
Connection	conn1
Virtual Network ID	/subscriptions/6447eb55-9d09-481b-89bc-52e96bb52823/resourceGroups/mapruletraffic/providers/Microsoft.Network/virtualNetworks/mapruletraffic-vnet
Authentication Type	sshPublicKey
SSH Public Key	Enter your SSH Public Key
Resource Group	○ Create New ● Use Existing Select a resource group
Image	gigamon-inc-vseries-cntlr-1.5-1
Disk Type	SSD
Size	Standard_B1s
Management Subnet	Subnet: Select management subnet Network Security Groups: Select network security group Accelerated Networking: ☐
Additional Subnet(s)	Add
Tag(s)	Add
Number of Instances	1
Use Public IP	☐

> **NOTE:** For shared controller configuration, you must select the required connection for configuring the V Series Controller. Peering must be active in the selected connection to allow the rest of the connections to be monitored.

3. Follow Step , Step , and Step as described in Configure G-vTAP Controllers and select the appropriate information for GigaVUE Cloud Suite V Series Controllers.

To view the GigaVUE V Series Controller configured in your VNet:

1. Login to the Azure account and select **Services > VM**.
2. In the left navigation pane, click **Instances**. The *GigaVUE V Series Controller* configured in your VNet is displayed in the Instances page.

Configure GigaVUE Cloud Suite V Series Nodes

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

GigaVUE Cloud Suite V Series nodes can be successfully launched only after GigaVUE Cloud Suite V Series Controller is fully initialized and the status is displayed as OK. The recommended minimum instance type for GigaVUE Cloud Suite V series node is Standard_DS2_v2.

> **NOTE:** GigaVUE Cloud Suite V series nodes configuration depends on a number of factors. Refer to the Microsoft Azure site for details.

To launch a GigaVUE Cloud Suite V Series node, do the following:

1. Select **Azure > Configuration > V Series Nodes**.
2. Click **New**. The V Series Node Configuration page is displayed as shown in the following figure.

V Series Node Configuration

Connection	Azure-VNET1-WestUS
Virtual Network ID	/subscriptions/6447e...../resourceGroups/ xxxz-rg/providers/Microsoft.Network/virtualNetworks/ xxxz
Authentication Type	sshPublicKey
SSH Public Key	Enter your SSH Public Key
Resource Group	○ Create New ● Use Existing
	vseries-rg
Image	gigamon-inc-vseries-node-1.4-1
Disk Type	SSD
Size	Standard_DS2_v2

Management Subnet

Subnet	xxxz-mgmt
Network Security Groups	xxxz-secGroup ×
Accelerated Networking	☐

Data Subnet(s) [Add]

Subnet 1	xxxz-mgmt
Network Security Groups	xxxz-secGroup ×
Accelerated Networking	☐

Tag(s) [Add]

Min Instances	0
Max Instances	1
Tunnel MTU	1450

> **NOTE:** Make sure the GigaVUE Cloud Suite V Series node version matches with the GigaVUE Cloud Suite V Series Controller version that is already configured.

3. Enter or select the appropriate information as shown in Configure G-vTAP Controllers.

Fields	Description
Connection	The name of the Azure connection.
Authentication Type	Enter the password or SSH Key.
SSH Public Key	Paste in the SSH public key.
Resource Group	Select **Create New** or **Use Existing**. To use Existing, select the existing resource group you wish to use.
Image	The GigaVUE Cloud Suite V Series node image. NOTE: For GigaVUE-FM 5.2 and above, only the GigaVUE Cloud Suite V Series node v1.3 is supported. The version number of GigaVUE Cloud Suite V Series node must match with the version number of the GigaVUE Cloud Suite V Series Controller.
Disk Type	SSD or HDD (SSD is the default and recommended disk type)
Size	*Standard_DS1_v2* is the default and recommended minimum.
Management Subnet	The public subnet that is used for communication between the GigaVUE Cloud Suite V Series Controller and the GigaVUE Cloud Suite V Series node. This is a required field. Every fabric node (both controllers and the nodes) need a way to talk to each other and FM. So they should share at least one management plane/subnet. Specify the following **Subnet**: The public subnet that is used for communication between the GigaVUE Cloud Suite V Series Controller and the GigaVUE Cloud Suite V Series node. This is a required field. Every fabric node (both controllers and the nodes) needs a way to talk to each other and GigaVUE-FM. Consequently, they should share at least one management plane/subnet. **Network Security Groups**: The security group created for the GigaVUE Cloud Suite V Series node. For example, sg_gigavue-vseries-node. For more information, refer Network Security Groups. **Accelerated Networking:** If you select this option, GigaVUE-FM will filter out the supported VM sizes in the list to choose from. NOTE: ● Some instance types support this in Azure platform. Refer to Microsoft documentation to learn which ones are supported. ● For Azure Government regions, **Accelerated Networking** is not supported and do not enable in the deployment.
Data Subnet(s)	The subnet that receives the mirrored VXLAN tunnel traffic from the G-vTAP agents. 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 GigaVUE Cloud Suite V Series node instances in your Azure environment. For example, you might have GigaVUE Cloud Suite V Series node deployed in many regions. To distinguish these GigaVUE Cloud Suite V Series node based on the regions, you can provide a name that is easy to identify such as us-west-2-vseries. To add a tag:

Fields	Description
	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-vseries.
Min Instances	The minimum number of GigaVUE Cloud Suite V Series nodes to be launched in the Azure connection. The minimum number of instances that can be entered is 0. When 0 is entered, no GigaVUE Cloud Suite V Series nodes are launched. **NOTE:** Nodes will be launched when a monitoring session is deployed as long as 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 Cloud Suite 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.
Tunnel MTU	The Maximum Transmission Unit (MTU) on the outgoing VXLAN tunnel endpoints of the GigaVUE Cloud Suite V Series node when a monitoring session is deployed. The default value is 1450.

To view the GigaVUE V Series nodes launched in your VNet:

1. Login to the Azure account and select **Services > VM**.
2. In the left navigation pane, click **Instances**. The GigaVUE V Series nodes launched in your VNet is displayed in the Instances page.

NOTE:
- The recommended minimum instance type for the GigaVUE Cloud Suite V Series node is DS2_v2.
- Certain availability zones may sometimes throw an insufficient instance capacity error. This is because Azure does not currently have enough capacity to service your request. When this error is displayed, you can launch the instance using a different instance type and resize at a later stage.
- The insufficient instance capacity error can be viewed only on Events page. Refer to About Events.
- To change the instance type at a later stage, the active monitoring sessions must be undeployed and the GigaVUE V Series nodes must be relaunched with the new configuration settings.

Configure and Manage Resources for Traffic flow

This chapter describes how to setup the tunnel endpoints to receive and send traffic from the GigaVUE Cloud Suite V Series node, and how to filter, manipulate, and send the traffic from the GigaVUE Cloud Suite V Series node to the monitoring tools or GigaVUE Cloud Suite H Series node.

Refer to the following sections for details:

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

Overview of Visibility Components

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

Table 1: Components of Traffic Visibility Sessions lists the components of the monitoring session:

Table 1: Components of Traffic Visibility Sessions

Parameter	Description
Map	A map (M) is used to filter the traffic flowing through the GigaVUE Cloud Suite V Series node. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.
Rule	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic. The rules must contain the appropriate Layer 2 (L2) to Layer 4 (L4) filters defined in them. For example, if you want to filter the traffic for HTTP Port 80, you must select the following criteria: • Layer 2—Ethertype IPv4 or IPv6 • Layer 3—Protocol TCP • Layer 4—Port Destination 80 By default, a rule always displays conditions based on the attributes of L2. A rule is also associated with priority and action set.

Parameter	Description
Priority	A priority determines the order in which the rules are executed. The greater the value, the higher the priority. The priority value can range from 0 to 99.
Action Set	An action set is an exit point in a map that you can drag and create links to the other maps, applications, and the monitoring tools. A single map can have multiple action sets. A single action set can have multiple links connecting to maps and applications. In the following example, the packets that match the rules in Action Set 0 are forwarded to a tunnel endpoint. The packets that match the rules in Action Set 1 are forwarded to another map.A single action set can have up to 8 links connecting the same destination point. The same packets from the map are replicated in 8 different links.
Link	A link directs the packets to flow from a map to the destination. The destination could be the other maps, applications, and the monitoring tools., the link originating from action set 0 is moving the traffic from MAP_1 to Monitoring_Tools. A link lets you add header transformation to the packets passing through it before they are sent to the destination. This transformation is supported only with GigaVUE V Series node v1.2-1 and above. For more information about Header Transformation, refer to Add Header Transformations.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.
Application	An application performs operations such as sampling, slicing, and masking on the traffic.
Inclusion Map	An inclusion map determines the instances or ENIs to be included for monitoring. This map is used only for target selection.
Exclusion Map	An exclusion map determines the instances or ENIs to be excluded from monitoring. This map is used only for target selection.
Target	A target determines the instances that are to be monitored. Targets are determined based on the following formula:
Automatic Target Selection (ATS)	A built-in feature that automatically selects the Virtual Machines and ENIs based on the rules defined in the maps, inclusion maps, and exclusion maps in the monitoring session. For example, if you create a rule determining the MAC source address in a map and a subnet in the inclusion map, the egress traffic from all instances or ENIs matching the MAC address in the specified subnet is selected for tapping the traffic.
Tunnel	A tunnel lists the monitoring tools to which the traffic matching the filtered criteria is routed.

Create Tunnel Endpoints

The customized traffic from the GigaVUE Cloud Suite V Series node is distributed to the tunnel endpoints using a standard L2 Generic Routing Encapsulation (GRE) or Virtual Extensible LAN (VXLAN) tunnel.

To create the tunnel endpoints:

1. Select **Azure > Configuration > Tunnel Spec Library**.
2. Click **New**. The Add Tunnel page is displayed as shown in the following figure.
3. Select or enter the appropriate information as shown in the following table.

Field	Description
Alias	The name of the tunnel endpoint. NOTE: Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint.
Type	The type of the tunnel. Select L2GRE or VXLAN to create a tunnel. If you choose VXLAN, you must enter the remote tunnel port.
Traffic Direction	The direction of the traffic flowing through the GigaVUE Cloud Suite V Series node. Choose **Out** for creating a tunnel from the GigaVUE Cloud Suite V Series node to the destination endpoint. NOTE: Traffic Direction **In** is not supported in the current release.
Remote Tunnel IP	The IP address of the tunnel destination endpoint. NOTE: You cannot create two tunnels from a GigaVUE Cloud Suite V Series node to the same IP address.

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

Create Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances and ENIs available in your Azure 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 Azure environment, GigaVUE-FM automatically detects and adds the instance into your monitoring session. Similarly, when an instance is removed, it updates the monitoring sessions to show the removed instance.

> **NOTE:** In vTAP connections, Tool VM instances (Source and Destination IP) must be excluded using Exclusion Map.

To design your monitoring session, refer to the following sections:

- Create New Session
- Clone Monitoring Session

Create New Session

You can create multiple monitoring sessions within a single VNet connection.

To create a new session:

1. Select **Azure > Monitoring Session**.
2. Click **New**. The Monitoring Sessions page is displayed.
3. Enter the appropriate information in the Monitoring Session Info as shown in the following table.

Field	Description
Alias	The name of the monitoring session.
Monitoring Domain	The name of the monitoring domain.
Connection	The azure 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.
Agent Pre-filtering	When enabled, traffic is filtered at the G-vTAP agent-level, before mirroring to the V Series Nodes, which reduces the load on the V Series Nodes and the Cloud networks. Refer to Agent Pre-filtering.

4. Click **Create**.

Clone Monitoring Session

You can clone an existing monitoring session.

To clone a monitoring session:

1. Select the monitoring session that you need to clone from the **Monitoring Sessions** page.
2. Click **Clone**.
3. Enter the appropriate information in the **Clone Monitoring Session** dialog box as described in the following table.

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

4. Click **Create** to create the cloned monitoring session.
5. Click **Edit** to add the connections to the cloned monitoring session.

Create Map

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

Conditions	Description
L2, L3, and L4 Filters	
Ether Type	The packets are filtered based on the selected ethertype. The following conditions are displayed:
	• IPv4
	• IPv6
	• ARP
	• RARP
	• Other
	L3 Filters
	If you choose IPv4 or IPv6, the following L3 filter conditions are displayed:
	• Protocol
	• IP Fragmentation
	• IP Time to live (TTL)
	• IP Type of Service (TOS)
	• IP Explicit Congestion Notification (ECN)
	• IP Source

Conditions	Description
	• IP Destination
	L4 Filters
	If you select TCP or UDP protocol, the following L4 filter conditions are displayed:
	• Port Source
	• Port Destination
MAC Source	The egress traffic from the instances or ENIs matching the specified source MAC address is selected.
MAC Destination	The ingress traffic from the instances or ENIs matching the specified destination MAC address is selected.
VLAN	All the traffic matching the specified IEEE 802.1q Virtual LAN tag is filtered. Specify a number from 0 to 4094.
VLAN Priority Code Point (PCP)	All the traffic matching the specified IEEE 802.1q Priority Code Point (PCP) is filtered. Specify a value between 0 to 7.
VLAN Tag Control Information (TCI)	All the traffic matching the specified VLAN TCI value is filtered. Specify the exact TCI value.
Pass All	All the packets coming from the monitored instances are passed through the filter. When Pass All is selected, the L3 and L4 filters are disabled.

When you select a condition without source or destination specified, then both egress and ingress traffic is selected for monitoring the traffic. For example, if you select IPv4 as the Ether Type, TCP as the protocol, and do not specify IP source or destination, then both egress and ingress traffic is selected for monitoring purpose.

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

> **NOTE:** You can create Inclusion and Exclusion Maps using all default conditions except Ether Type and Pass All.

To create a new map:

1. Select **Azure > Monitoring Session**.

2. Click **New**. The Monitoring Sessions page is displayed.

3. Create a new session. Refer to Create New Session.

4. From **Maps**, drag and drop a new map template to the workspace. If you are creating an exclusion or inclusion map, drag and drop a new map template to their respective section at the bottom of the workspace. The new map page is displayed as shown in Figure 1Creating a New Map.

Figure 1   *Creating a New Map*

5. Enter the appropriate information for creating a new map as described in the following table.

Parameter	Description
Alias	The name of the new map. **NOTE:** The name can contain alphanumeric characters with no spaces.
Comments	The description of the map.
Map Rules	The rules for filtering the traffic in the map. To add a map rule: a. Click **Add a Rule**. b. Select a condition from the **Search L2 Conditions** drop-down list and specify a value. Based on this selection, the Search L3 Conditions drop-down list is automatically updated. c. Select a condition from the **Search L3 Conditions** drop-down list and specify a value. d. (Optional) If you have selected TCP or UDP as the protocol in the L3 conditions, then select Port Source or Port Destination from the Search L4 Conditions drop-down list and specify a value. If you have selected conditions other than TCP or UDP, then the Search L4 Conditions drop-down list is disabled.
Map Rules	e. (Optional) In the Priority and Action Set box, assign a priority and action set. f. (Optional) In the Rule Comment box, enter a comment for the rule. **NOTE:** Repeat steps **b** through **f** to add more conditions. **NOTE:** Repeat steps **a** through **f** to add nested rules.

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

6. To reuse the map, click **Add to Library**. Save the map using one of the following options:

   - Select an existing group from the **Select Group** list and click **Save**.
   - Enter a name for the new group in the **New Group** field and click **Save.**

NOTE: The maps saved in the Map Library can be reused in any monitoring session present in the VNet.

7. Click **Save**.

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

Click the **Show Targets** button to view the monitoring targets highlighted in orange.

Click on to expand the **Targets** dialog box. Click on to change the view from topology to viewing the instance names. To view more details about the instance tag name, direction of tapping, and so on, click the arrow next to the instance name.

Filter the instances based on the Instance Name Prefix, IP address, or the MAC address.

Agent Pre-filtering

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

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

Agent Pre-filtering Guidelines

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

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

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

Agent Pre-filtering Capabilities and Benefits

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

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

- Only rules from first-level maps are pushed to the agents.

- Pass rules are supported 100%.

- Drop rules are supported for only simple cases or single-drop rules with a pass all case.

- Rules that span all monitoring sessions will be merged for an G-vTAP agent, if applicable.

- If the max-rule limit of 16 is reached, then all the traffic is passed to the V Series node; no filtering will be performed.

Enable/Disable G-vTAP Agent Pre-filtering

Agent pre-filtering can be enabled or disabled by the user at the monitoring-session level. This ensures that we provide a knob to the user to turn it on or off at the G-vTAP level according to the requirements.

To change the G-vTAP Agent Pre-filtering option setting:

1. **Cloud > Azure > Monitoring Session**

2. Open a monitoring session by doing one of the following:

   a. Click **New** to create a new session.

   b. Click the check box next to a session and then click **Edit** to edit an existing session.

    Figure 2   *Enable/disable G-vTAP Agent Pre-filtering*

3. Select or deselect the **Agent Pre-filtering** check box in the Monitoring Session info box to change the setting. It is enabled by default.

   a. Deselect the check box to disable it.

   b. Select the check box to enable it.

4. Click **OK**.

5. The Monitoring Session view displays the setting in the Agent Pre-filtering column.

Add Applications to Monitoring Session

Gigamon supports the following GigaSMART applications with GigaVUE Cloud Suite Cloud for AWS:

- • Sampling
- • Slicing
- • Masking
- • NetFlow

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

Sampling

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

To add a sampling application:

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

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

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

4. For State, select the **On** check box to determine that the application is sampling packets randomly. Select the **Off** check box to determine that the application is not currently sampling the packets. The state can be changed at anytime whenever required.
5. From the Sampling Type drop-down list, select the type of sampling:
   - **Random Simple** — The first packet is selected randomly. The subsequent packets are also selected randomly based on the rate specified in the **Sampling Rate** field.
     For example, if the first packet selected is 5 and the sampling rate is 1:10, after the 5th packet a random 10 packets are selected for sampling.
   - **Random Systematic** —The first packet is selected randomly. Then, every nth packet is selected, where n is the value specified in the **Sampling Rate** field.
     For example, if the first packet selected is 5 and the sampling rate is 1:10, then every 10th packet is selected for sampling: 15, 25, 35, and so on.
6. In the **Sampling Rate** field, enter the ratio of packets to be selected. The default ratio is 1:1.
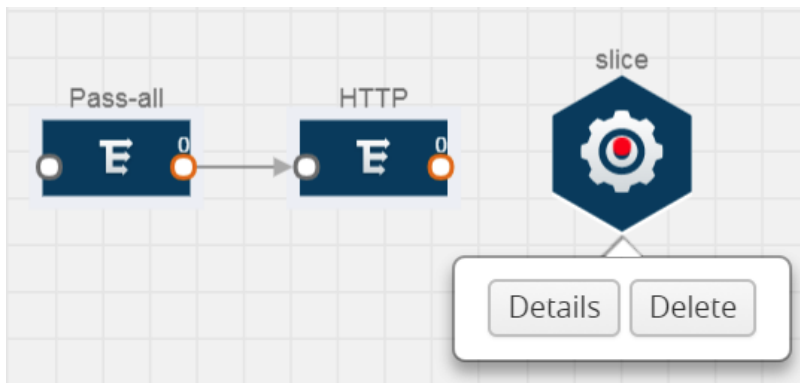7. Click **Save**.

Slicing

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

To add a slicing application:

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

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

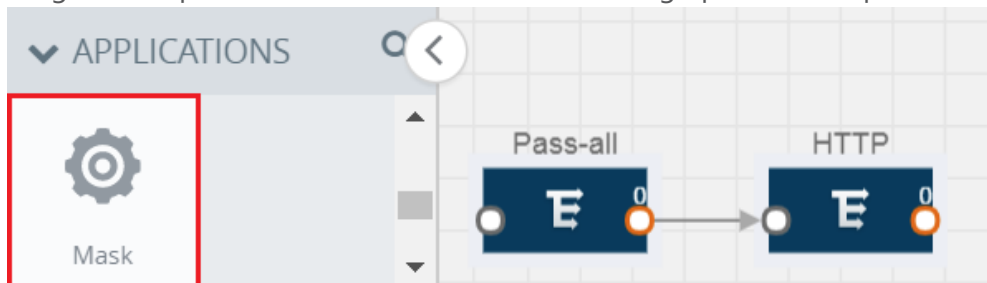3. In the **Alias** field, enter a name for the slice.

4. For State, select the **On** check box to determine that the application is slicing packets. Select the **Off** check box to determine that the application is not currently slicing the packets. The state can be changed at a later time whenever required.

5. In the Slice Length field, specify the length of the packet that must be sliced.

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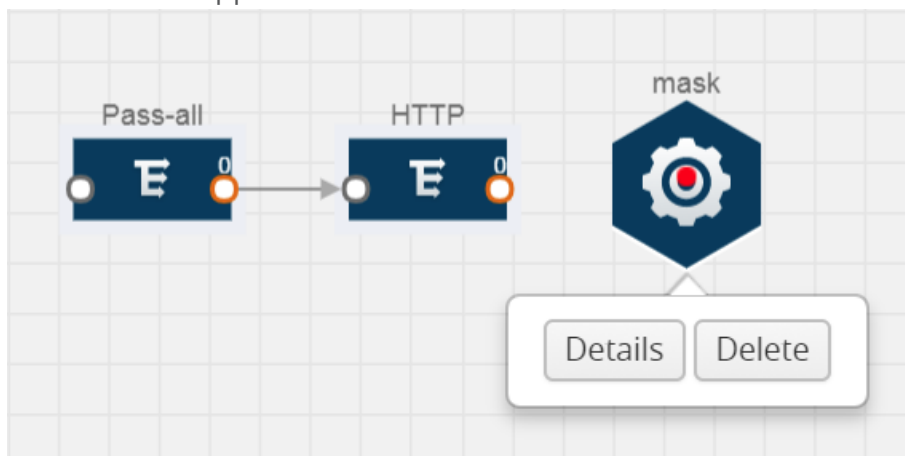   - TCP

7. Click **Save**.

Masking

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

To add a masking application:

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

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

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

4. For State, select the **On** check box to determine that the application is masking packets. Select the **Off** check box to determine that the application is not currently masking the packets. The state can be changed at anytime whenever required.
5. In the Mask offset field, enter the offset from which the application should start masking data following the pattern specified in the Pattern field.
   The value can be specified in terms of either a static offset, that is, from the start of the packet or a relative offset, that is, from a particular protocol layer as specified in the Protocol field.
6. In the Mask length field, enter the length of the packet that must be masked.
7. In the Mask pattern field, enter the pattern for masking the packet. The value of the pattern is from 0 to 255.
8. From the Protocol drop-down list, specifies an optional parameter for masking packets on the data coming from the selected protocol.
9. Click **Save**.

NetFlow

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

The following are the key benefits of NetFlow application:

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

The NetFlow application contains key elements that specify what to match in the flow, such as all packets with the same source and destination port, or the packets that come in on a particular interface. For information about Match/Key fields, refer to Match/Key Fields. A NetFlow record is the

output generated by NetFlow. A flow record contains non-key elements that specify what information to collect for the flow, such as when the flow started or the number of bytes in the flow. For information about Match/Key fields, refer to Collect/Non-Key Fields.

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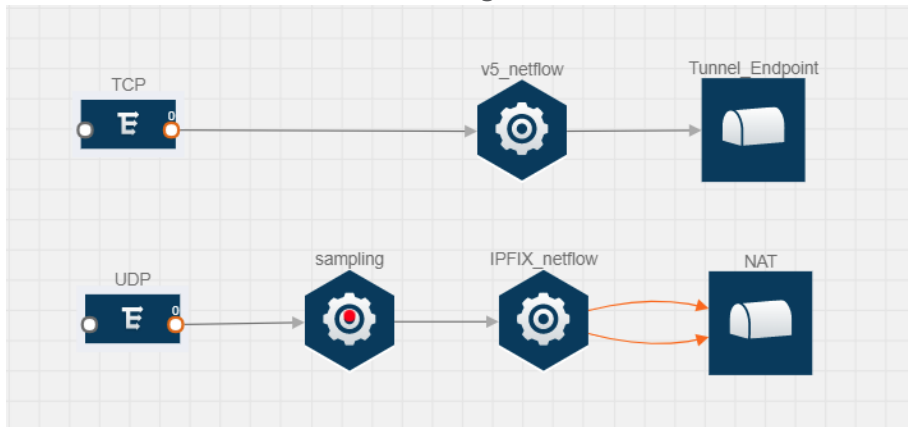

Figure 3   *NetFlow on GigaVUE Cloud Suite V Series Node*

The NetFlow record generation is performed on GigaVUE Cloud Suite V Series node running the NetFlow application. In Figure 3NetFlow on GigaVUE Cloud Suite V Series Node, incoming packets from G-vTAP agents are sent to the GigaVUE Cloud Suite V Series node. In the GigaVUE V Series node, one map sends the TCP packet to the version 5 NetFlow application. Another map sends the UDP packet to a sampling application. The map rules and applications such as slice, mask, and sample can only be applied prior to sending the data to NetFlow.

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

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

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

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

> is sent periodically based on the configuration.
- IPFIX—The extended version of version 9 supports variable length fields as well as enterprise-defined fields.

Match/Key Fields

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

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

Table 2: Match/Key Elements

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

	Description	Supported NetFlow Versions
IP Header Length	Configures the length of the IP header as a key field.	IPFIX
IP Precedence	Configures the value of the IP Precedence as a key field.	IPFIX
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9 and IPFIX
IP Total Length	Configures the total length of the IP packet as a key field.	IPFIX
IP TTL	For IPv4, configures the value of Time to Live (TTL) as a key field. For IPv6, configures the value of the Hop Limit field as a key field.	IPFIX
IP Version	Configures the IP version field in the IP packet header as a key field.	v9 and IPFIX
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9 and IPFIX
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9 and IPFIX
IPv6 ICMP Code	Configures the code of the IPv6 ICMP message as a key field.	IPFIX
IPv6 ICMP Type	Configures the type of the IPv6 ICMP message as a key field.	IPFIX
IPv6 ICMP Type Code	Configures the type and code of the IPv6 ICMP message as a key field.	IPFIX
IPv6 Payload Length	Configures the value of the payload length field in the IPv6 header as a key field.	IPFIX
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9 and IPFIX
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport header as a key field.	v9 and IPFIX
TCP AcK Number	Configures the acknowledgment number in the TCP header as a key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP header	IPFIX

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

Collect/Non-Key Fields

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

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

Table 3: Collect/Non-Key Elements

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

	Description	Supported NetFlow Versions
Flow Start Millisec	Configures the value of the IP Precedence as a non-key field.	IPFIX
Flow Start Sec	Configures the absolute timestamp of the first packet of this flow as a non-key field.	IPFIX
Flow Startup Time	Configures the flow start SysUp time as a non-key field.	v9 and IPFIX
Flow		
Flow End Reason	Configures the reason for Flow termination as a non-key field.	IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP message as a non-key field.	v9 and IPFIX
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 ICMP Type	Configures the type of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a non-key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a non-key field.	IPFIX
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9
IP Version	Configures the IP version field in the IP packet header as a key field.	v9
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a non-key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport	v9 and IPFIX

|	Description	Supported NetFlow Versions
	header as a non-key field.	
TCP AcK Number	Configures the acknowledgment number in the TCP header as a non-key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a non-key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a non-key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a non-key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP header as a non-key field.	IPFIX
TCP Src Port	Configures the source port identifier in the TCP header as a non-key field.	IPFIX
TCP Urgent	Configures the urgent pointer in the TCP header as a non-key field.	IPFIX
TCP Window Size	Configures the window field in the TCP header as a non-key field.	IPFIX
UDP Dest Port	Configures the destination port identifier in the UDP header as a non-key field.	IPFIX
UDP Src Port	Configures the source port identifier in the UDP header as a non-key field.	IPFIX

Add Version 5 NetFlow Application

To add a version 5 NetFlow application:

1. Drag and drop **NetFlow** from **APPLICATIONS** to the graphical workspace.
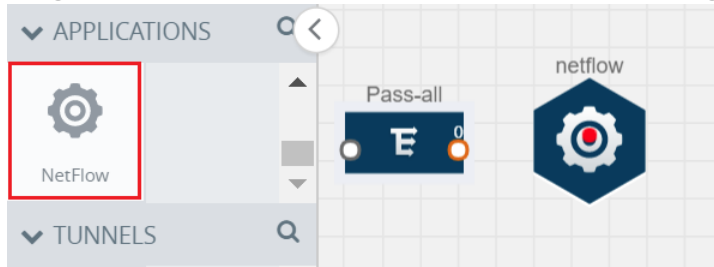
2. Click the NetFlow application and select **Details**. A quick view is displayed for configuring the NetFlow application.
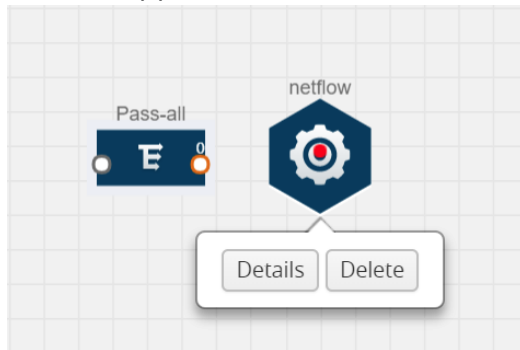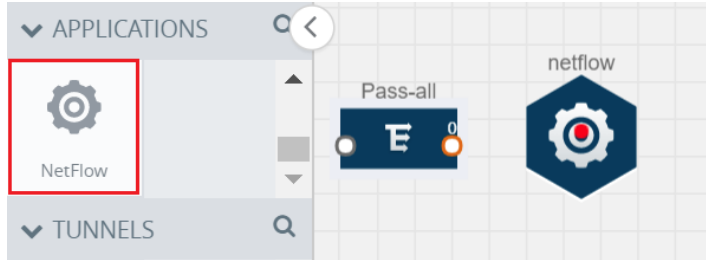

3. In the **Alias** field, enter a name for the v5 NetFlow application.

4. For State, select the **On** check box to determine that the application is currently running. Select the **Off** check box to determine that the application is currently not running. The state can be changed at anytime whenever required.

5. From the **NetFlow version** drop-down list, select v5.

6. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.

7. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.

8. Click **Save**.

For more examples demonstrating the NetFlow application configuration in the GigaVUE V Series nodes, refer to NetFlow Examples.
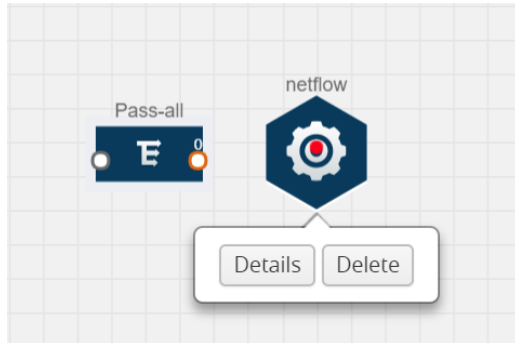
Add Version 9 and IPFIX NetFlow Application

To add a v9 and IPFIX NetFlow application:

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

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

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

4. For State, select the **On** check box to determine that the application is generating NetFlow records from the packets coming from the G-vTAP agents. Select the **Off** check box to determine that the application is not currently generating NetFlow records. The state can be changed at anytime whenever required.

5. From the **NetFlow version** drop-down list, select the version you want to use to generate the NetFlow records. The default version selected is v5.

6. In the **Source ID** field, enter the observation domain to isolate the traffic. The NetFlow application uses source ID to segregate the records into categories. For example, you can assign source ID 1 for traffic coming over TCP. This results in generating a separate NetFlow record for TCP data. Similarly, you can assign Source ID 2 for traffic coming over UDP. This results in generating a separate NetFlow record for UDP data.

7. From the **Match fields** drop-down list, select the parameters that identify what you want to collect from the incoming packets. The Match fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to Match/Key Fields.

8. From the **Collect fields** drop-down list, select the parameters that identify what you want to collect from the NetFlow records. The Collect fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to Collect/Non-Key Fields.

9. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.

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

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

Network Address Translation (NAT)

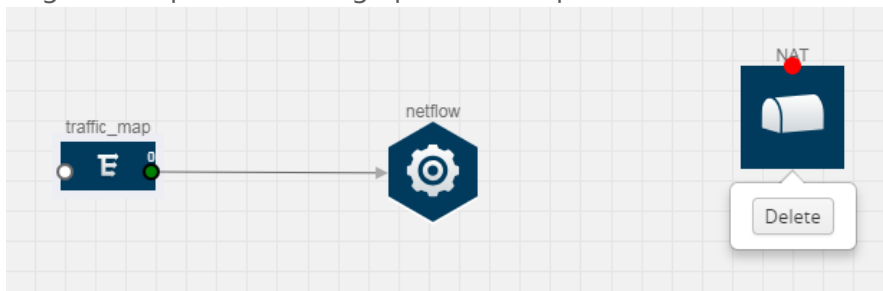NAT allows the NetFlow records to be directly transmitted to a collector without a tunnel

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

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

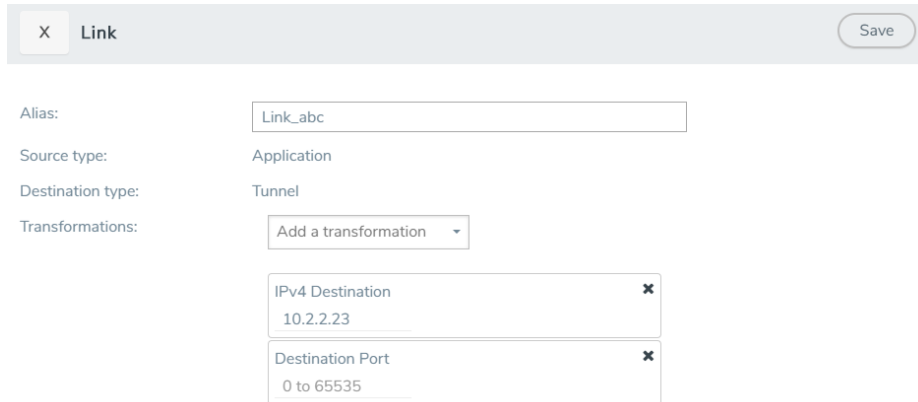**Add NAT**

To add a NAT device:

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

Link NetFlow Application to NAT

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

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

Figure 4   *Creating a Link from NetFlow to NAT*

2. In the **Alias** field, enter a name for the link.

3. From the **Transformations** drop-down list, select any one of the header transformations:

   - IPv4 Destination
   - ToS
   - Destination Port

> **NOTE:** Only the above three header transformations are allowed on the link from the NetFlow application to a NAT device.

4. In **IPv4 Destination**, enter the IP address of the NetFlow collector.

5. (Optional) By default, the Destination Port is 2055. To change the destination port, enter a port number.

6. Click **Save**. The transformed link is displayed in Orange.

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

NetFlow Examples

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

Example 1

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

1. Create a monitoring session. For steps, refer to Create Monitoring Session.
2. In the monitoring session, create a Pass all map. A pass all map sends all the traffic received from the G-vTAP agents to the tunnel endpoint or NAT. For steps, refer to Clone Monitoring Session.
3. Drag and drop a tunnel from **Tunnels**. A tunnel encapsulates the flow records and then sends them to the tools for full packet inspection.
4. Create a link from the Pass-all map to the tunnel endpoint. The traffic from the Pass-all map is forwarded to the tunnel endpoint that is connected to a tool.
5. Drag and drop a v5 NetFlow application.
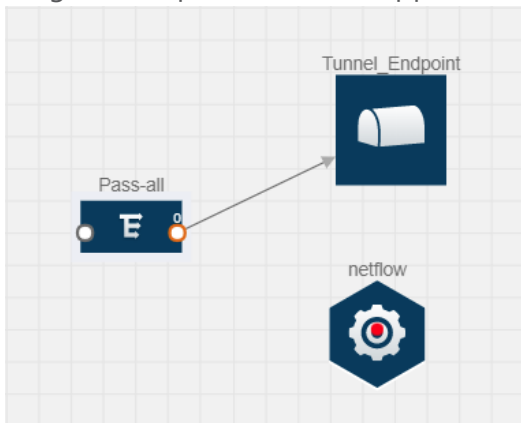
6. Click the NetFlow application and select **Details**. The Application quick view is displayed. For steps to configure the v5 NetFlow application, refer to Add Version 5 NetFlow Application.
7. Create a link from the Pass all map to the v5 NetFlow application.
8. Drag and drop **NAT** to the graphical workspace.
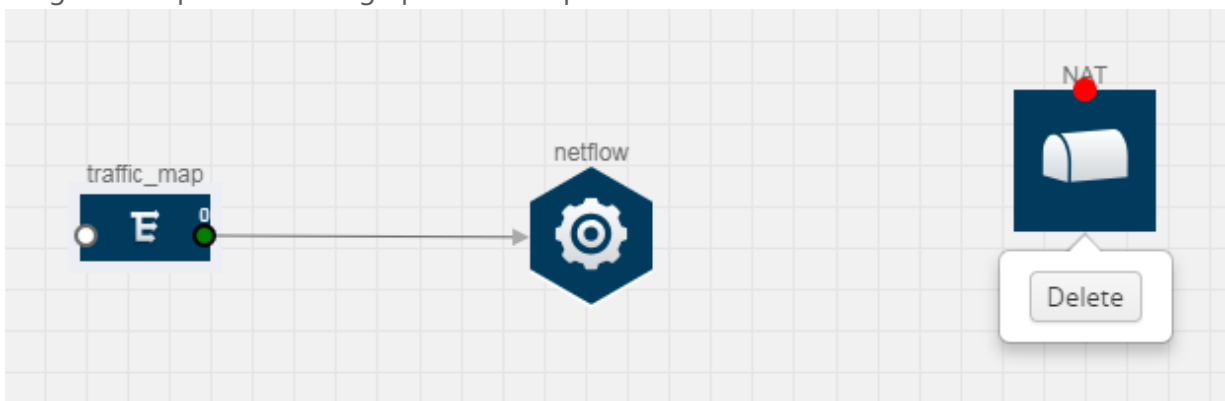
9. Create a link from the v5 NetFlow application to NAT. The link must be configured with the destination IP address of the NetFlow collector and the GigaVUE Cloud Suite V Series node interface. For steps to configure the link, refer to Link NetFlow Application to NAT.

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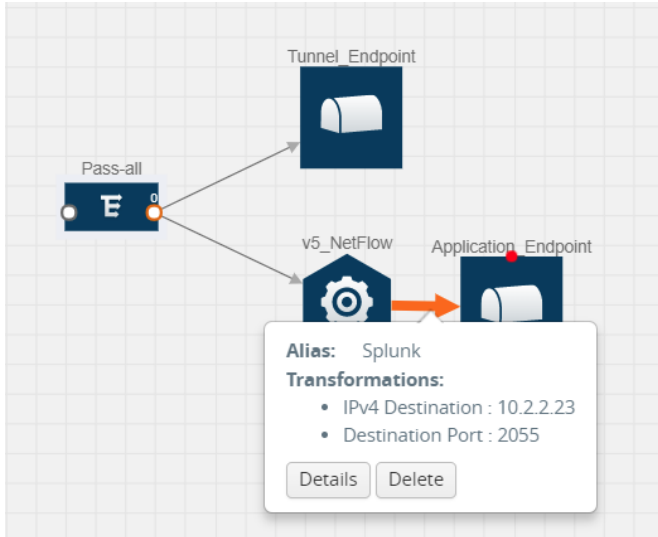
Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop one or more maps from the **MAP Library** to the workspace.

2. (Optional) To add Inclusion and Exclusion maps, drag and drop the maps from the Map Library to their respective section at the bottom of the workspace.

3. (Optional) Drag and drop one or more applications from the APPLICATIONS section to the workspace.

> **NOTE:** For information about adding applications to the workspace, refer to Add Applications to Monitoring Session.

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

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

5. Hover your mouse on the map, click the red dot, and drag the link over to another map, application, or tunnel. You can drag more than one link from a map to the destination. On these links, you can apply link transformation to alter the packets. For information about adding link transformation, refer to Add Header Transformations.

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

7. Click **Show Targets** to view details about the subnets and monitoring instances. The instances and the subnets that are being monitored are highlighted in orange.

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

   The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all GigaVUE Cloud Suite V Series nodes and G-vTAP agents.

   If the monitoring session is not deployed properly, then one of the following errors is displayed:
   - Partial Success—The session is not deployed on one or more instances due to G-vTAP or GigaVUE Cloud Suite V Series node failure.
   - Failure—The session is not deployed on any of the GigaVUE Cloud Suite V Series nodes and G-vTAP agents.

   Click on the status link to view the reason for the partial success or failure.

9. Click **View** under Statistics to view and analyze the incoming and outgoing traffic.

You can also do the following in the Monitoring Session page:

- Use the **Redeploy** button to redeploy a monitoring session that is not deployed or partially successful.
- Use the **Undeploy** button to undeploy the selected monitoring session.
- Use the **Clone** button to duplicate the selected monitoring session.
- Use the **Edit** button to edit the selected monitoring session.
- Use the **Delete** button to delete the selected monitoring session.

Add Header Transformations

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

Header transformations are used to perform many simple operations on the network packets. The source and destination MAC addresses, port numbers, and IP addresses can be masked to prevent the information from being exposed to the monitoring tools.

The monitoring tools cannot always distinguish the traffic coming from multiple VNets with the same subnet range. You can add VLAN ID, VLAN priority, and DSCP bits to the header for distinguishing the traffic coming from multiple VNets with the same subnet range.

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

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

GigaVUE Cloud Suite V Series node supports the following header transformations:

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

To add a header transformation:

1. On the Monitoring Session, click the link and select **Details.** The Link quick view is displayed.

2. From the **Transformations** drop-down list, select one or more header transformations.

> **NOTE:** Do not apply VLAN Id and VLAN PCP transformation types with the Strip VLAN ID transformation type on the same link.

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

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

View Monitoring Session Statistics

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

> **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.
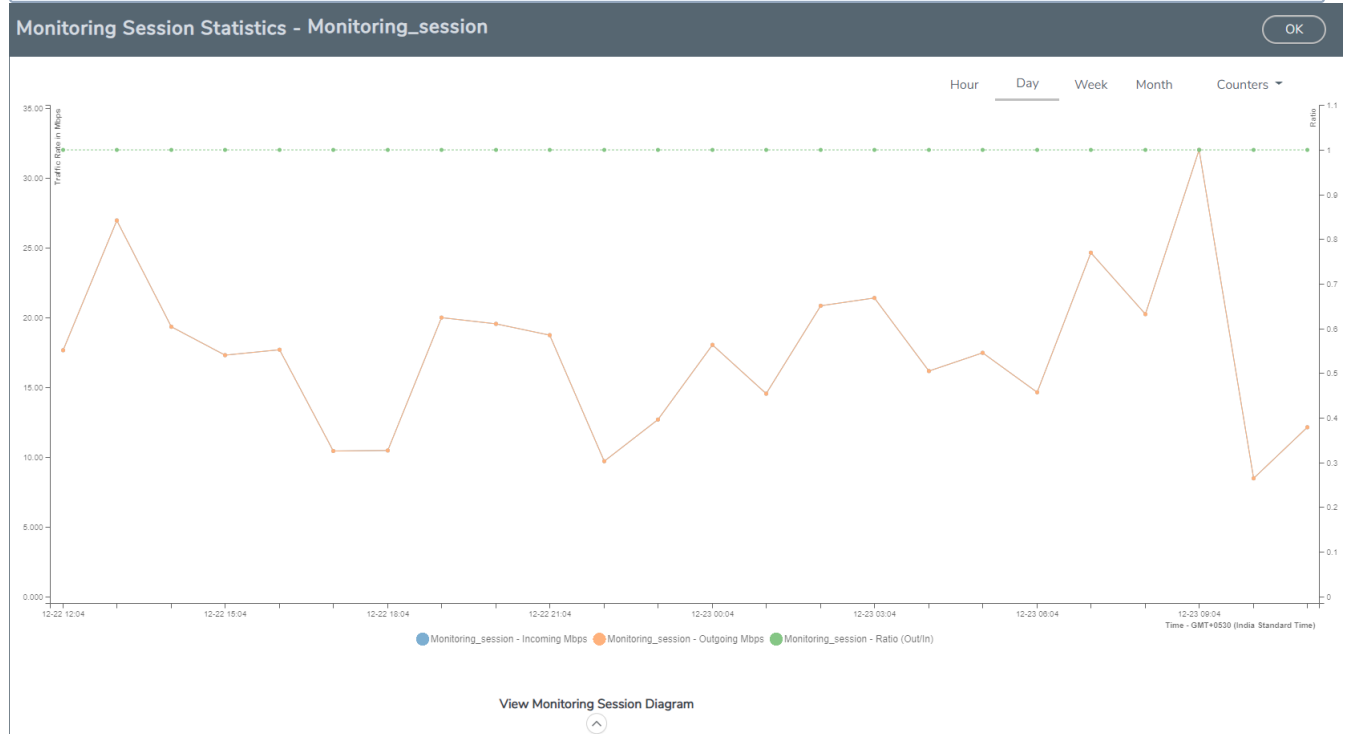
You can click on Incoming Maps, Outgoing Maps, and Ratio at the bottom of the graph to view the statistics individually.

You can expand the **View Monitoring Session Diagram** and click on each individual map, application, and tunnel to view more details about the incoming and outgoing traffic on the selected statistics page. The Map Statistics page lets you choose the map rules to view the traffic matching the selected rule.

Visualize the Network Topology

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

To view the topology diagram:

1. Select **Azure > Topology**.
2. Select a connection from the **Select connection...** list. The topology view of the subnets and instances is displayed.
3. (Optional) Select a monitoring session from the **Select Monitoring Session...**list. The topology view of the monitored subnets and instances in the selected session are displayed.
4. Select one of the following check boxes:
    - **Source**: Displays the topology view of the source target interfaces that are being monitored.
    - **Destination**: Displays the topology view of the destination target interfaces where the traffic is being mirrored.
    - **Other**: Displays the topology view of the non-G-vTAP agents such as GigaVUE Cloud Suite V Series Controllers, G-vTAP Controllers, monitoring tools, and instances that are being used in the connection.
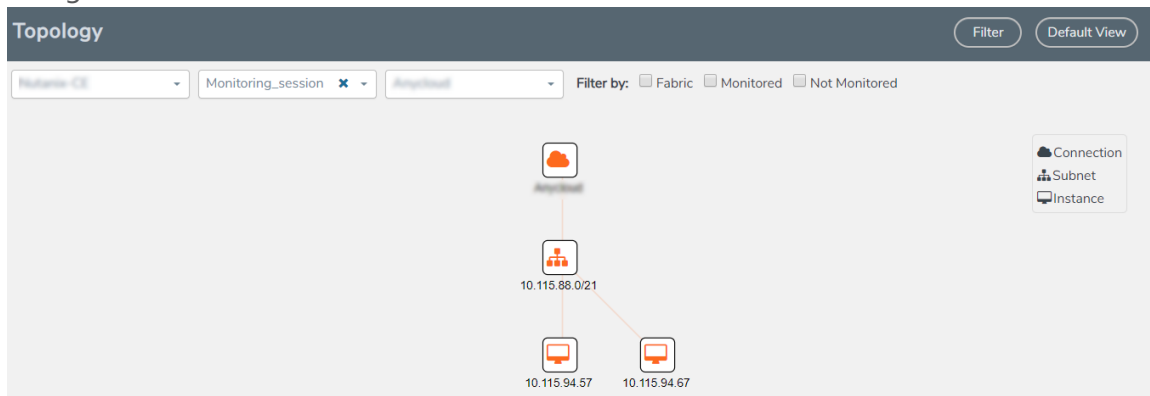
5. (Optional) Hover over or click the subnet or VM Group icons to view the subnets or instances present within the group.

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 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.

Use the **Azure > Configurations > Azure Settings** to edit these Azure settings. Refer to the following table for more information about the settings:

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of VNet connections you can establish in GigaVUE-FM.
Refresh interval for instance inventory (secs)	Specifies the frequency for updating the state of Virtual Machines in Azure.
Refresh interval for non-instance inventory (secs)	Specifies the frequency for updating the state of non-instance information such as subnets, security groups, images, and VNets.
Number of instances per GigaVUE Cloud Suite V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE Cloud Suite V Series node.
Refresh interval for G-vTAP agent inventory (secs)	Specifies the frequency for discovering the G-vTAP agents available in the VNet.

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. Select **Azure > Configuration > Proxy Server**.

2. Click **Add**. The Add Proxy Server page is displayed as shown in Figure 5Adding a Proxy Server.

   Figure 5   *Adding a Proxy Server*

3. Select or enter the appropriate information as shown in Table 4: Fields for Proxy Sever Configuration

Table 4: Fields for Proxy Sever Configuration

Field	Description
Alias	The name of the proxy server.
Host	The host name or the IP address of the proxy server.
Host IP Address Type	The type of the Host IP address that indicate whether the proxy server IP address is private or public to the VNet.
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. Refer to Figure 6Proxy 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. Refer to Connect to Microsoft Azure.

Figure 6   *Proxy Server Configuration Page*

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 to 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 the right side of the top navigation bar, Click ⚙.
2. On the left navigation pane, select **System** and then **Notifications**.
3. In the Notifications page, select the event and click **Configure**.
4. In the Recipient(s) box, enter one or multiple email IDs separated by a comma.
5. Click **Save**.

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:

- Azure License Expire
- G-vTAP Agent Inventory Update Completed
- Azure 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 Azure license expiry.

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

Click **Cloud** on the top navigation bar. On the left navigation pane, click **Events**.

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.
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.

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that are logged by the system such as: • Log in and Log out based on users. • Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details on whether the user was in FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	In the case of a failure, provides a brief update on the reason for the failure.

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

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

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

To filter the audit logs, do the following:

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

3. Click **OK** to apply the selected filters to the Audit Logs page.

Compatibility Matrix for Azure

This appendix provides information about GigaVUE-FM version compatibility and the features supported in various versions of GigaVUE Cloud Suite V Series nodes and G-vTAP agents.

Refer to the following sections for details:

- GigaVUE-FM Version Compatibility
- Supported Features in GigaVUE Cloud Suite V Series Nodes
- Supported Features in G-vTAP Agents

GigaVUE-FM Version Compatibility

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

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Controller	GigaVUE Cloud Suite-V Series Nodes
5.3.01	v1.4-1	v1.4-1	v1.4-1	v1.4-1
5.4.00	v1.4-1	v1.4-1	v1.4-1	v1.4-1

Supported Features in GigaVUE Cloud Suite V Series Nodes

The following table lists the features supported in various versions of GigaVUE Cloud Suite V Series nodes:

Features	GigaVUE Cloud Suite V Series v1.0	GigaVUE Cloud Suite V Series v1.2	GigaVUE Cloud Suite V Series v1.3
Header Transformation	No	No	Yes
Multi-link Support	No	No	Yes
NetFlow Application	No	No	Yes
NAT Support	No	No	Yes

Supported Features in G-vTAP Agents

The following table lists the features supported in various versions of G-TAP Agents:

Features	G-vTAP Agent v1.2	G-vTAP Agent v1.3	G-vTAP Agent v1.4
Dual ENI Support	Yes	Yes	Yes
Single ENI Support	No	Yes	Yes
VXLAN Support	No	Yes	Yes
Agent Pre-filtering	No	No	Yes

Additional Sources of Information

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

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

Documentation

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.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
Hardware
how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
*G-TAP A Series 2 Installation Guide
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide *(now including TA25)*
*GigaVUE-OS Installation Guide for DELL S4112F-ON how to install GigaVUE-OS and configure ports on COTS DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide how to install GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM how to migrate GigaVUE-FM on VMware ESXi, Hardware Appliance, and AWS
GigaVUE-OS Upgrade Guide how to upgrade the embedded GigaVUE-OS on GigaVUE H Series and GigaVUE TA Series nodes
Administration
GigaVUE-OS and GigaVUE-FM Administration Guide

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
how to administer the GigaVUE-OS and GigaVUE-FM software (note, new file name for PDF)
Fabric Management

GigaVUE-FM User's Guide
    how to install, deploy, and operate GigaVUE-FM
    how to configure GigaSMART operations
    includes instructions for GigaVUE-FM and GigaVUE-OS features

Cloud Configuration and Monitoring   how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the respective cloud platform
GigaVUE Cloud Suite for AnyCloud Configuration Guide   how to deploy the GigaVUE Cloud Suite solution in any cloud platform
GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS Quick Start Guide   quick view of AWS deployment used in conjunction with the GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS SecretRegions Configuration Guide
GigaVUE Cloud Suite for Azure Configuration Guide
GigaVUE Cloud Suite for Kubernetes Configuration Guide
GigaVUE Cloud Suite for Nutanix Configuration Guide
GigaVUE Cloud Suite for OpenStack Configuration Guide
GigaVUE Cloud Suite for VMware Configuration Guide
Gigamon Containerized Broker
Reference
GigaVUE-OS-CLI Reference Guide   library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide   guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix   compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide   samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes

GigaVUE Cloud Suite 5.10 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 .
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Docs** 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 & Documentation** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," 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

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

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

Contact Technical Support

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

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

- Submit and vote on feature enhancements and share product feedback. (Customers only)

- Open support tickets (Customers only)

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

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

Register today at community.gigamon.com

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