GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide

GigaVUE Cloud Suite

Product Version: 6.1

Document Version: 1.0

(See Change Notes for document updates.)

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.1.00	1.0	11/30/2022	The original release of this document with 6.1.00 GA

Contents

GigaVUE Cloud Suite for Azure–GigaVUE V Series 1

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

Refer to the following sections for details:

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:

Component	Description
GigaVUE® Fabric Manager (GigaVUE-FM)	A web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud for Azure. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform. • G-vTAP Controllers (only if you are using G-vTAP Agent as the traffic acquisition method) • GigaVUE® V Series 1 nodes • GigaVUE® V Series Controllers
G-vTAP Agents	An agent that is installed in your virtual machines. This agent mirrors the selected traffic from the virtual machines to the GigaVUE V Series node.
G-vTAP Controllers	Manages multiple G-vTAP Agents and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more G-vTAP Controllers to communicate with the G-vTAP Agents.
GigaVUE V Series Controllers or Proxy	Manages multiple GigaVUE V Series nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Controllers to communicate with the GigaVUE V Series nodes.
GigaVUE V Series nodes	A visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to on premise device or tools. GigaVUE Cloud Suite for Azure uses the standard VXLAN tunnel to deliver traffic to tool endpoints.

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

You can choose the following option for configuring the components described above:

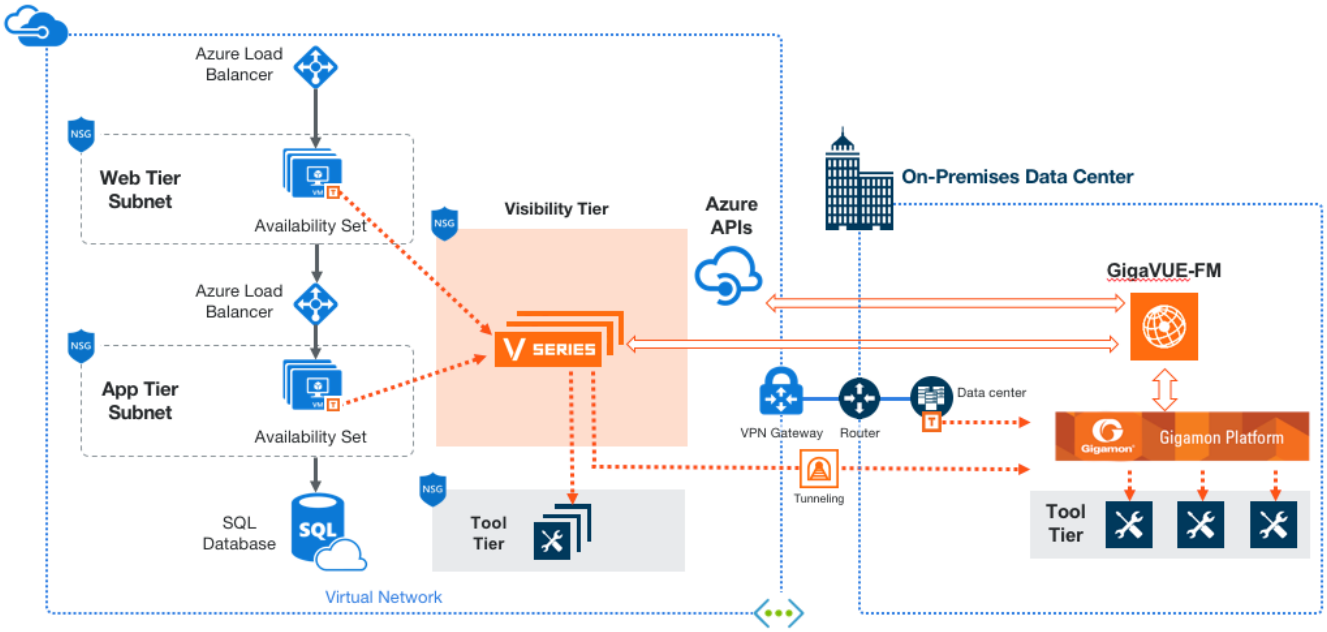
Standard Configuration	GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in all VNets

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

Architecture of GigaVUE Cloud Suite for Azure

Hybrid Cloud

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



Get Started with GigaVUE Cloud Suite for Azure

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

Refer to the following sections for details:

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

License Information

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

Refer to the following topics for detailed information:

- Bring Your Own License (BYOL)
- Apply Licensing

Bring Your Own License (BYOL)

BYOL is applicable only for V Series 1 node usage. The licenses for the BYOL option can be purchased based on the number of TAP points and the term of the license. Gigamon offers the following options for purchasing the license:

- Traffic visibility for up to 100 virtual TAP points (NICs/vNICs)
- Traffic visibility for up to 1000 virtual TAP points (NICs/vNICs)

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

The minimum term for the license is 3 months.

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

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

Apply Licensing

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

Before You Begin

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

- Prerequisites
- VPN Connectivity
- Obtain GigaVUE-FM Image

Prerequisites

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

- Resource Group
- Virtual Network
- Subnets for VNet
- Network Interfaces (NICs) for VMs
- Network Security Groups

Resource Group

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

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

Virtual Network

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

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

Subnets for VNet

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

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

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

Network Interfaces (NICs) for VMs

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

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

Network Security Groups

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

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

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

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

Network Security Groups for GigaVUE V Series 1 Node

Following are the Network Firewall Requirements for V Series 1 configuration.

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 V Series Controllers, and GigaVUE-FM administrators to communicate with GigaVUE-FM
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP Agents
GigaVUE V Series Controller					
Inbound	Custom TCP Rule	TCP	9902	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Controllers
GigaVUE V Series 1 node					

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

Access control (IAM)

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

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

VPN Connectivity

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

Obtain GigaVUE-FM Image

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

GigaVUE Cloud Suite Cloud Suite in Azure Public Cloud

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

GigaVUE Cloud Suite Cloud Suite in Azure Government

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

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

Install and Upgrade GigaVUE-FM

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

- Cloud—To install GigaVUE-FM inside your Azure environment, you can launch the GigaVUE-FM instance in your VNet. For installing the GigaVUE-FM instance, refer to Install GigaVUE-FM on Azure.
- On-premises—To install and upgrade GigaVUE-FM in your enterprise data center, refer to GigaVUE-FM Installation and Upgrade Guide available in the Gigamon Documentation Library.

Deploy GigaVUE Cloud Suite for Azure

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

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

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

Refer to the following topics for details:

- Establish Connection to Azure
- Prepare G-vTAP Agent to Monitor Traffic
- Create Monitoring Domain
- Configure GigaVUE Fabric Components in GigaVUE-FM

Establish Connection to Azure

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

Refer to the following topics.

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

Managed Identity (recommended)

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.Enable MSI for the GigaVUE-FM VM by using the Azure CLI command:
az vm assign-identity -g <Resource group where FM is deployed> -n <GigaVUE-FM name>

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

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

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

There are 2 steps to have MSI work:

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

Enable MSI on the VM running GigaVUE-FM

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

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

Enable MSI using the CLI

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

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

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

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

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

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

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

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

Enable MSI Using the Portal

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

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

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

Application ID with client secret

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

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

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

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

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

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

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

Custom Roles

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

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

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

Using CLI:

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

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

Example: Custom Role at Resource Group Level

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

```
{
"Name": "FM Custom Role RG Level",
"IsCustom": true,
"Description": "Minimum permissions for FM to operate",
"Actions": [
"Microsoft.Compute/virtualMachines/read",
```

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

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

```
"/subscriptions/6447xxx11-1x11-111x-11xx-11x11xx11111/resourceGroups/gvtap-rg"
]
}
```

Example: Custom Role for Subscription Level

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

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

```
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
 "Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
],
"NotActions": [

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

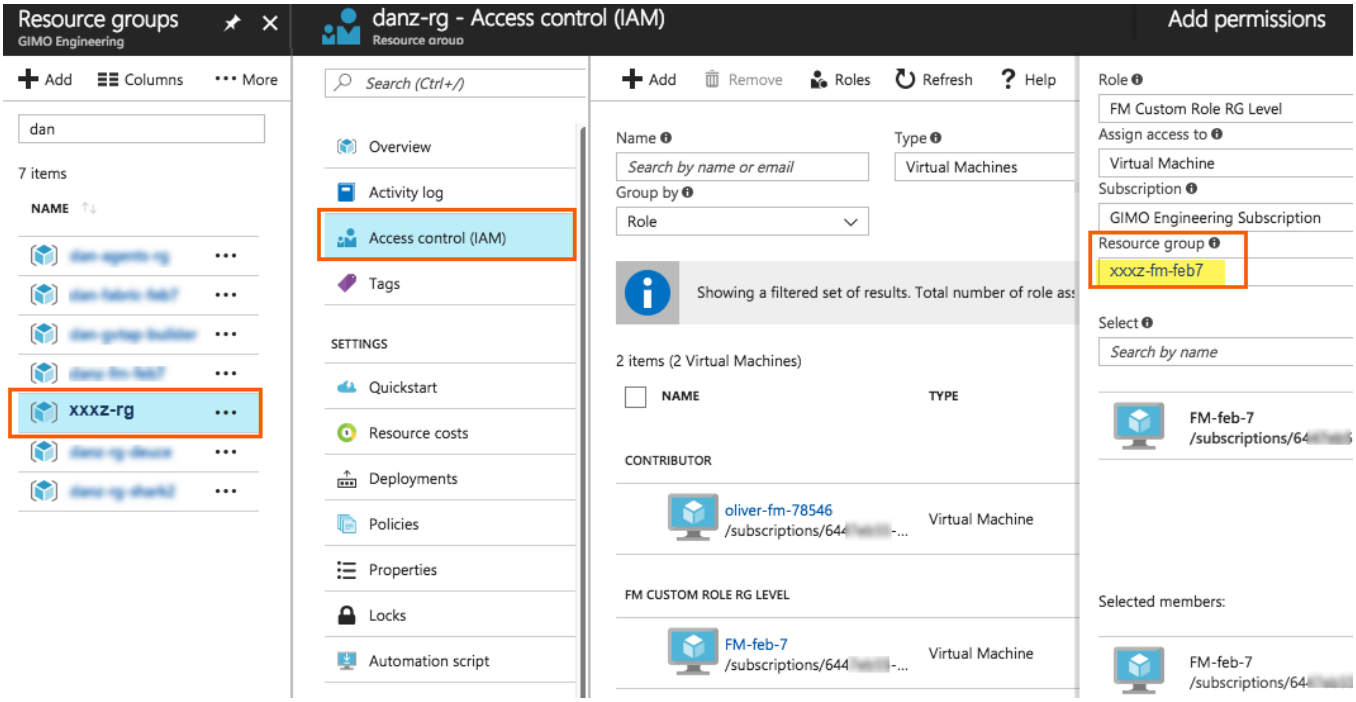
Add Custom Role to Subscription or Resource Group

After creating the custom role, you can add the role to either the Resource Group, or at the Subscription level in the Azure console. In this example, the role is added to my Resource Group. As the GigaVUE-FM connection gets connected to the VNET in the resource Group "xxxz-rg", the following permissions/roles are added to the Resource Group. If you want to have GigaVUE-FM create a resource group to launch fabric into, you must add these permissions to the subscription level instead.

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

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

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



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

CLI to add role to Resource Group

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

CLI for Subscription Level

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

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

update role

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

Pre-defined Roles

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

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

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

Accept EULA and Enable Programmatic Deployment in Azure

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

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

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

   b. BYOL FM:

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

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

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

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

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

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

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

Prepare G-vTAP Agent to Monitor Traffic

A G-vTAP Agent is the primary Gigamon monitoring module that is installed in your Virtual Machines (VMs). This agent mirrors the selected traffic from the VMs, encapsulates it using VXLAN tunneling, and forwards it to the GigaVUE Cloud Suite® V Series node.

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

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

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

Refer to the following sections for more information:

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

Linux G-vTAP Agent Installation

Refer to the following sections for the Linux agent installation:

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

Single NIC Configuration

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

For example, assume that there is only one interface eth0 in the monitoring VM. In the G-vTAP configuration, you can configure eth0 as the source and the destination interface, and specify both egress and ingress traffic to be selected for monitoring purpose. The egress and ingress traffic from eth0 is mirrored and sent out using the same interface.

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

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

Grant permission to monitor ingress and egress traffic at iface

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

Dual NIC Configuration

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

For example, assume that there is eth0 and eth1 in the monitoring VM. In the G-vTAP Agent configuration, eth0 can be configured as the source interface and egress traffic can be selected for monitoring purpose. The eth1 interface can be configured as the destination interface. So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series node.

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

Grant permission to monitor ingress and egress traffic at iface

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

Install G-vTAP Agents

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

For dual or multiple NIC/ENI configuration, you may need to modify the network configuration files to make sure that the extra NIC/ENI will initialize at boot time.

NOTE: Before installing G-vTAP Agent **.deb** or **.rpm** packages on your Linux VMs, you must install packages like Python3 and Python modules (netifaces, urllib3, and requests).

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

Refer to the following topics for details:

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

Install G-vTAP from Ubuntu/Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent **6.1.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gvtap-agent_6.1.00_amd64.deb
$ sudo dpkg -i gvtap-agent_6.1.00_amd64.deb
```

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

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

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

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

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

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

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

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

4. Save the file.

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

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

6. Reboot the instance.

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

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

Install G-vTAP from RPM package

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

1. Download the G-vTAP Agent **6.1.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Copy this package to your instance. Install the package with root privileges, for example:

```
$ ls gvtap-agent_6.1.00_x86_64.rpm
$ sudo rpm -i gvtap-agent_6.1.00_x86_64.rpm
```

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

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

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

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

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

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

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

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

4. Save the file.

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

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

6. Reboot the instance.

Check the status with the following command:

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

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

1. Launch the RHEL/CentOS agent AMI image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**6.1.00**_x86_64.rpm
   - gvtap.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
5. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_6.1.00_x86_64.rpm
   ```
6. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

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

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent **`6.1.00`** MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator**and the G-vTAP Agent service starts automatically.
3. Once the G-vTAP package is installed, modify the file **C:\ProgramData\Gvtap-agent\gvtap-agent.conf** to configure and register the source and destination interfaces.

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

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

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

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

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

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

4. Save the file.

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

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

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

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

Windows G-vTAP Agent Installation Using ZIP Package

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

1. Download the Windows G-vTAP Agent **`6.1.00`** ZIP package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Extract the contents of the .zip file into a convenient location.
3. Run ‘install.bat’ as an **Administrator**and the G-vTAP Agent service starts automatically.

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

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

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

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

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

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

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

5. Save the file.

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

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

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

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

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

Install IPSec on G-vTAP Agent

If IPSec is used to establish secure connection between G-vTAP Agents andGigaVUE 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 G-vTAP from Ubuntu/Debian Package
- Install G-vTAP from Red Hat Enterprise Linux and CentOS
- Install G-vTAP from Red Hat Enterprise Linux and CentOS with Selinux Enabled

Install G-vTAP from Ubuntu/Debian Package

1. Launch the Ubuntu/Debian image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**6.1.00**_amd64.deb
   - gvtap-ipsec_**6.1.00**_amd64.deb
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.
4. Install the G-vTAP Agent package file:
   ```
   sudo dpkg -i gvtap-agent_6.1.00_amd64.deb
   ```
5. Modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces:

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

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

   You can view the G-vTAP log using **`cat /var/log/gvtap-agent.log`** command.
6. Install strongSwan:
   ```
   tar -xvf strongswan5.3.5-1ubuntu3.8_amd64-deb.tar.gz
   cd strongswan-5.3.5-1ubuntu3.8_amd64/
   sudo sh ./swan-install.sh
   ```
7. Install IPSec package:
   ```
   sudo dpkg -i gvtap-ipsec_6.1.00_amd64.deb
   ```

Install G-vTAP from Red Hat Enterprise Linux and CentOS

1. Launch RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**6.1.00**_x86_64.rpm
   - gvtap-ipsec_**6.1.00**_x86_64.rpm
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.

4. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_6.1.00_x86_64.rpm
   ```
5. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   # sudo /etc/init.d/gvtap-agent restart
   ```
6. Install strongSwan:
   ```
   tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz
   cd strongswan-5.7.1-1.el7.x86_64
   sudo sh ./swan-install.sh
   ```
7. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_6.1.00_x86_64.rpm
   ```

NOTE: You must install IPSec package after installing StrongSwan.

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

1. Launch the RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**6.1.00**_x86_64.rpm
   - gvtap-ipsec_**6.1.00**_x86_64.rpm
   - gvtap.te and gvtap_ipsec.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
5. Checkmodule -M -m -o gvtap_ipsec.mod gvtap_ipsec.te
   ```
   semodule_package -o gvtap_ipsec.pp -m gvtap_ipsec.mod
   sudo semodule -i gvtap_ipsec.pp
   ```
6. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_6.1.00_x86_64.rpm
   ```

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

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

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

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

9. Install IPSec package:
   ```
   sudo rpm -i gvtap-ipsec_6.1.00_x86_64.rpm
   ```

10. Reboot the instance.

Create Images with the Agent Installed

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

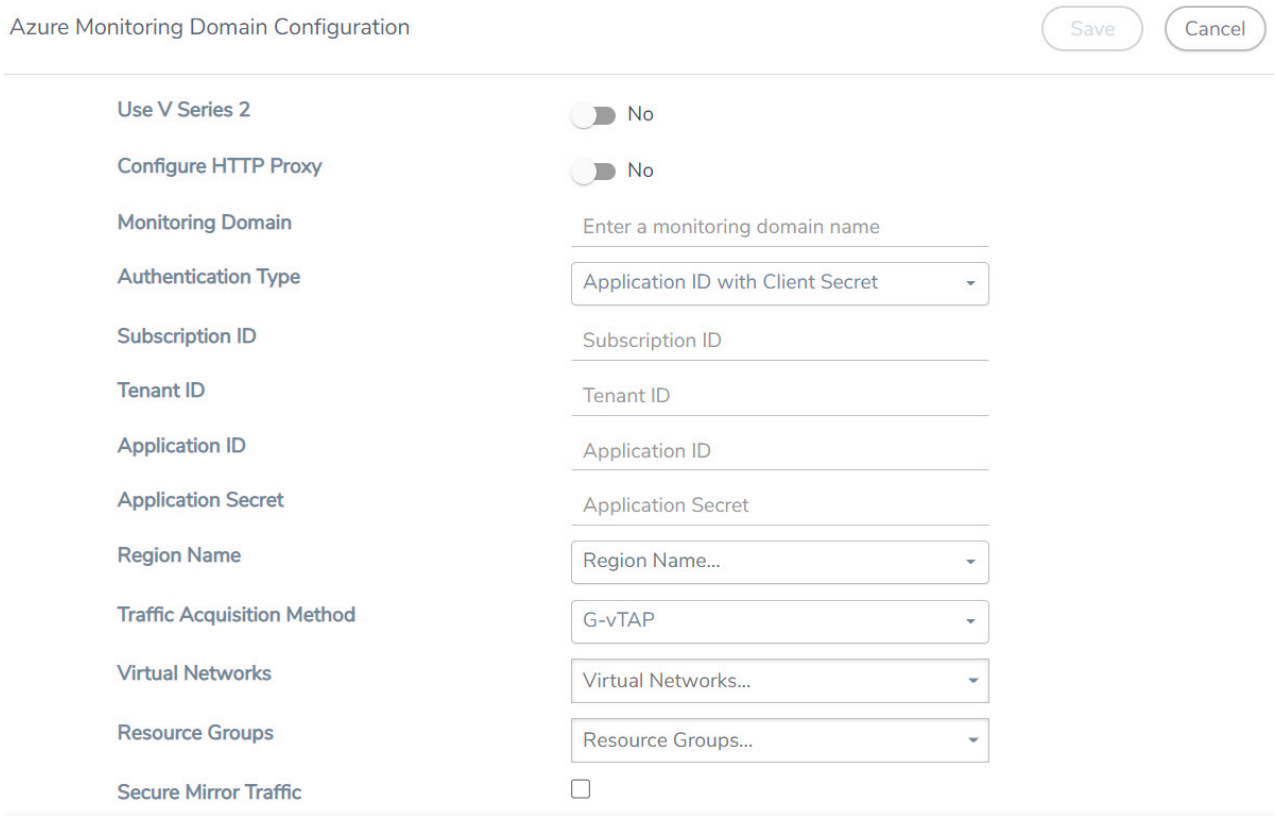
To save the G-vTAP Agent as an image, refer to Capture VM to managed image topic in the Microsoft Azure Documentation.

Create Monitoring Domain

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. GigaVUE-FM connects to Azure using either an Application ID with the client secret or the MSI method of authentication. After the connection establishment, GigaVUE-FM launches the G-vTAP Controller, GigaVUE V Series Controller, and GigaVUE V Series 1 node.

To create a monitoring domain for GigaVUE Cloud Suite for Azure in GigaVUE-FM:

1. From the left navigation pane, select **Inventory > VIRTUAL > Azure > Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, click New. The **Azure Monitoring Domain Configuration** wizard appears.



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

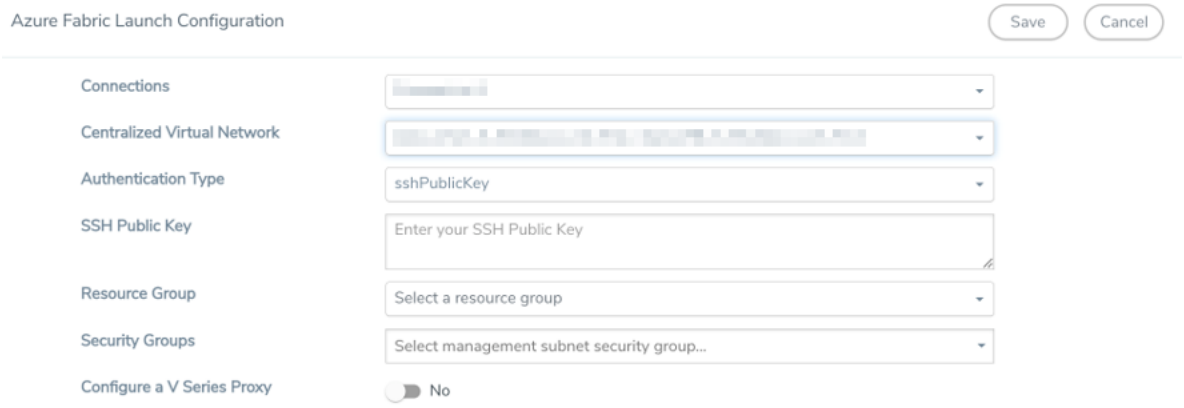
Field	Description
Use V Series 2	Select **No** for V Series 1 configuration.
Configure HTTP Proxy	Select **Yes** to add a proxy server. Proxy server enables communication from GigaVUE-FM to the Internet, if GigaVUE-FM is deployed in a private network. On selecting a Proxy Server, enter the following information: • **Proxy Server**—Select a list of proxy servers already configured in GigaVUE-FM. For more information on adding the proxy servers before configuring the Azure connection, refer to Configure Proxy Server. • **Add Proxy Server**—Add a new Proxy Server. For field information, refer to Configure Proxy Server.
Monitoring Domain	An alias used to identify the monitoring domain.
Authentication Type	Select an authentication type for the connection. • **Managed Services Identity**: MSI registered with required roles assigned for the resource group in your Azure platform. Refer to Managed Identity (recommended) for detailed information. • **Application ID with Client Secret**: Connection with Azure with a service principal. Enter the values for **Subscription ID**, **Tenant ID, Application ID**, and **Application Secret** values required for GigaVUE-FM to connect to Azure. Refer to Application ID with client secret for detailed information.
Region Name	Azure region for the monitoring domain. For example, West India.
Traffic Acquisition Method	▪ **G-vTAP**: G-vTAP Agents are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP Agents.
Virtual Networks	Select one or more Virtual Networks (VNets) required.
Resource Groups	Select the Resource Groups of the corresponding VMs to monitor.
Secure Mirror Traffic	Check box to establish secure tunnel between G-vTAP Agents and GigaVUE V Series nodes for traffic across VNets.

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

Configure GigaVUE Fabric Components in GigaVUE-FM

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

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



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

Fields	Description
Connections	A connection that you created in the monitoring domain page. Refer to Create Monitoring Domain for more information.
Centralized Virtual Network	Alias of the centralized VNet in which the G-vTAP Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.
Authentication Type	Select Password or SSH Public Key as the Authentication Type to connect with the Centralized VNet.
SSH Public Key	The SSH public key for the GigaVUE fabric nodes.
Resource Group	The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM. This is a required field.
Security Groups	The security group created for the GigaVUE fabric nodes.
Click **Yes** to configure GigaVUE V Series Controller for the monitoring domain. Refer to Configure GigaVUE V Series Controller	

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

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

Refer to the following topics for details:

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

Configure G-vTAP Controller

A G-vTAP Controller manages multiple G-vTAP Agents and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes.

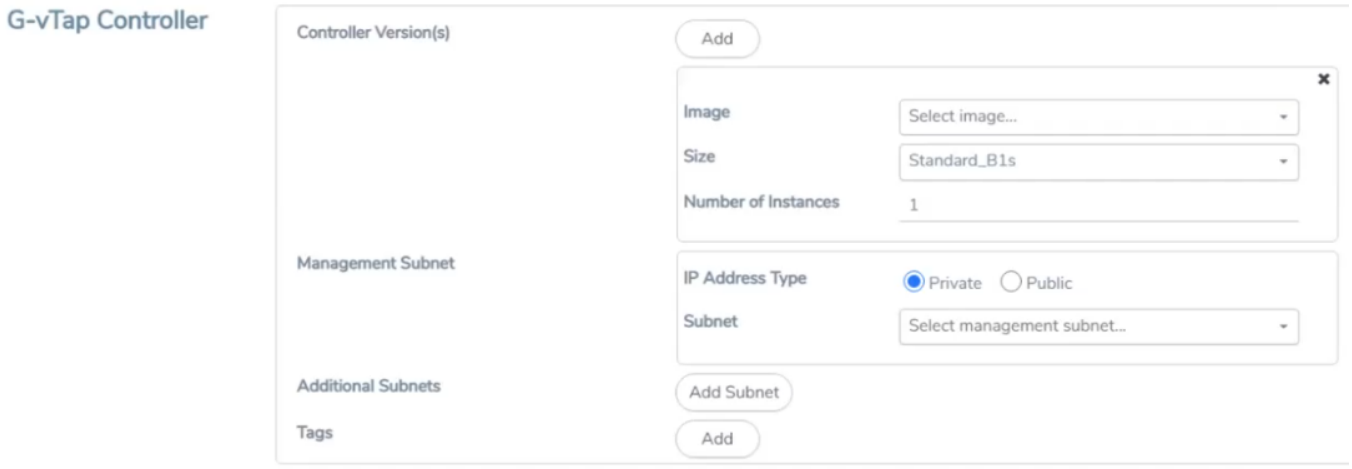
NOTE: A single G-vTAP Controller can manage up to 1000 G-vTAP Agents. The recommended minimum instance type is Standard_B1s for G-vTAP Controller.

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

To configure the G-vTAP Controllers:

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

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



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

Configure GigaVUE V Series Controller

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

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

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

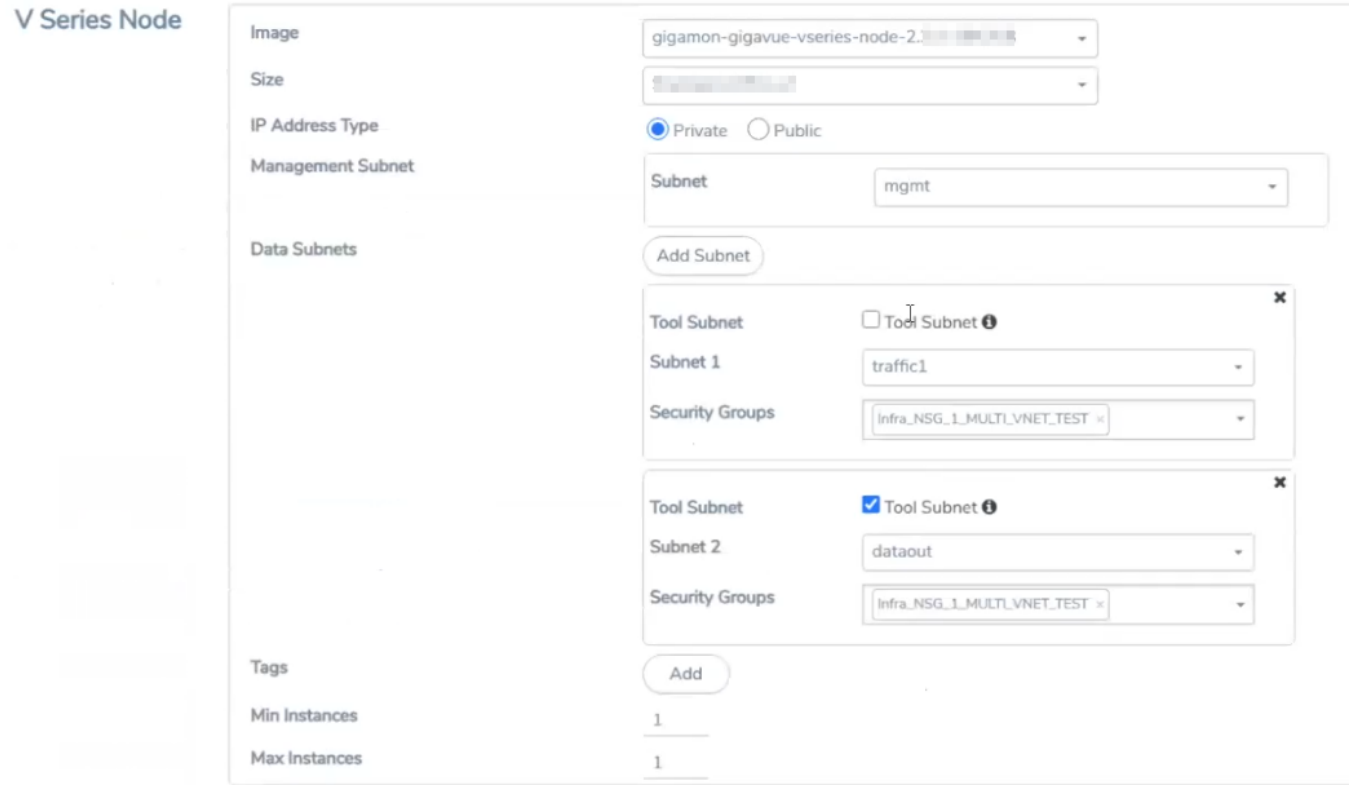
1. In the **Azure Fabric Launch Configuration** page, Select **Yes** to **Configure a V Series Controller** and the V Series Controller fields appears.
2. Enter or select the appropriate values for the GigaVUE V Series Controller. Refer to the G-vTAP Controller field descriptions for detailed information.

Configure GigaVUE V Series Node

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

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

In the **Azure Fabric Launch Configuration** page, Enter or select the appropriate values for theGigaVUE V Series.



Fields	Description
Image	From the **Image** drop-down list, select aGigaVUE V Series image.
Size	From the **Size** down-down list, select a size for theGigaVUE V Series. The default size for the GigaVUE V Series 1 configuration is **Standard_DS2_v2**.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between theGigaVUE V Series instances and GigaVUE-FM instances in the same network.

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

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

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

Configure Monitoring Session

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

Refer to the following sections for details:

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

Create a 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.

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

To create a new session:

1. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > Azure**. The Monitoring Session page appears.
2. Click **New**. The Create A New Monitoring Session window appears.
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.

4. Click **Create**.

Create Tunnel Endpoints

The customized traffic from the GigaVUE V Series node is distributed to the tunnel endpoints using a standard Virtual Extensible LAN (VXLAN) tunnel.

To create a new tunnel endpoint:

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

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

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

4. Click **Save**.

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

Create Map

Each map can have up to 32 rules associated with it. The following table 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	
EtherType	The packets are filtered based on the selected ethertype. The following conditions are displayed: ▪ IPv4 ▪ IPv6 ▪ ARP ▪ RARP ▪ Other **L3 Filters** If you choose IPv4 or IPv6, the following L3 filter conditions are displayed: ▪ Protocol

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

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

When you select a condition with either source or destination specified, it determines the direction based on the selection. For example, if only IP source is selected, 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 EtherType and Pass All.

To create a new map:

1. In the Monitoring Session canvas, from **Maps** section, 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 appears.
2. 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.

3. 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.

4. Click **Save**.

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

Agent Pre-filtering

The G-vTAP Agent pre-filtering option filters traffic before mirroring it from G-vTAP Agent to the GigaVUE 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 GigaVUE 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 thatGigaVUE V Series currently accepts. Non L2-L4 filters are used purely by ATS to select the targets; not for G-vTAP.
- Both egress and ingress maps with filters are supported on G-vTAP.
- Both single and dual network interfaces for G-vTAP Agent VMs are supported.

Agent Pre-filtering Rules and Notes

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

- The agent pre-filtering option can be enabled or disabled at the monitoring-session level and is enabled by default.
- When enabled, traffic is filtered at the G-vTAP Agent-level, before mirroring to the GigaVUE V Series Nodes. Consequently, traffic flow to the GigaVUE 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 theGigaVUE V Series; 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. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > Azure**. The Monitoring Session page appears.
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.
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

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

- Sampling
- Slicing
- Masking
- NetFlow

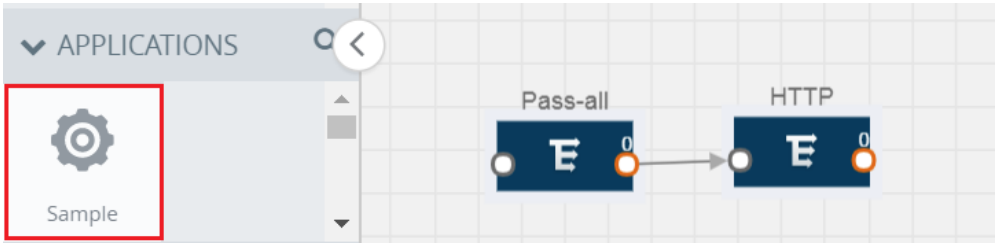
You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools.

Sampling

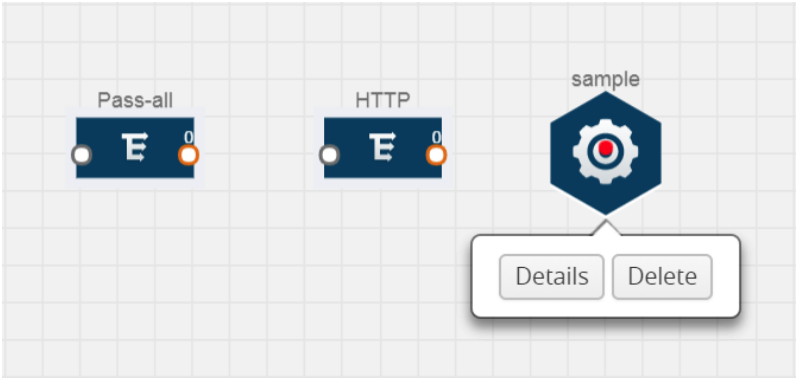
Sampling lets you sample the packets randomly based on the configured sampling rate and then forwards the sampled packets to the monitoring tools.

To add a sampling application:

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



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



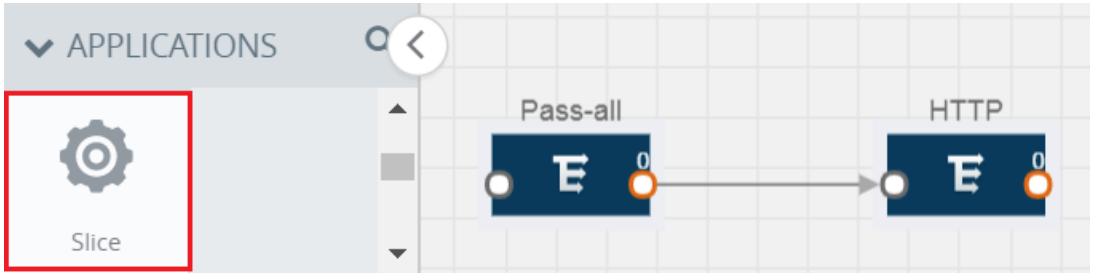
3. In the **Alias** field, enter a name for the sample.
4. For State, select the **On** check box to determine that the application is sampling packets randomly. Select the **Off** check box to determine that the application is not currently sampling the packets. The state can be changed at anytime whenever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

Slicing

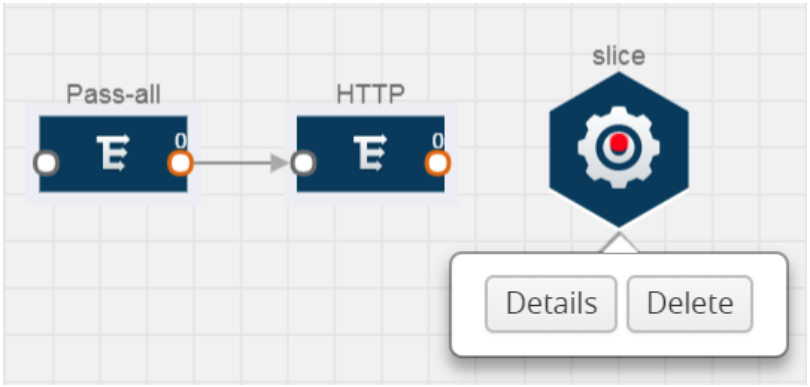
Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes.

To add a slicing application:

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



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



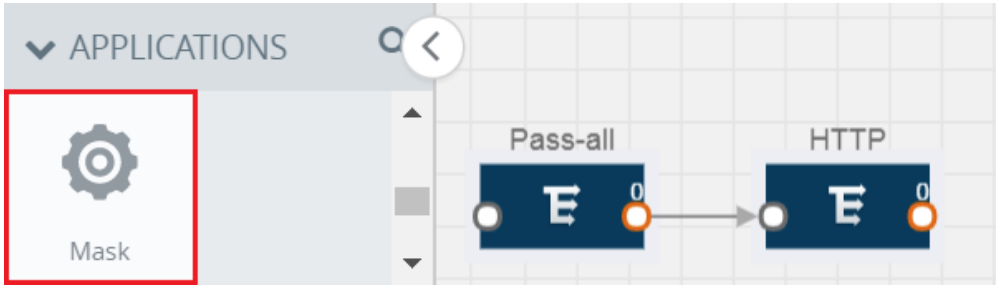
3. In the **Alias** field, enter a name for the slice.
4. For State, select **On** or **Off** check box to enable or disable slicing. The state can be changed at a later time whenever required.
5. In the Slice Length field, specify the length of the packet that must be sliced.
6. From the Protocol drop-down list, specify an optional parameter for slicing the specified length of the protocol. The options are as follows:
   - None
   - IPv4
   - IPv6
   - UDP
   - TCP
7. Click **Save**.

Masking

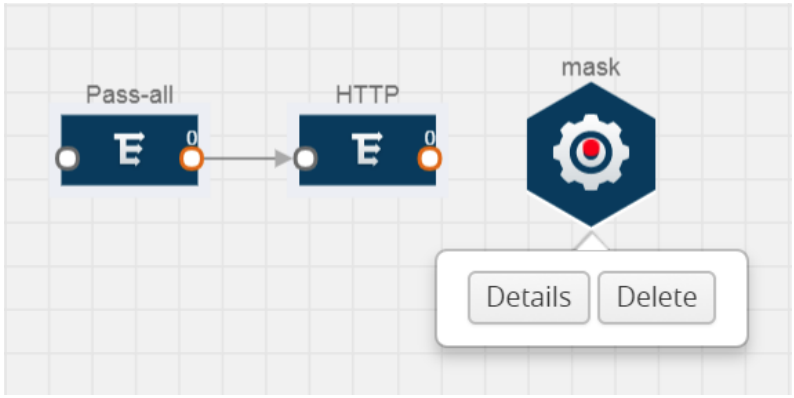
Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.

To add a masking application:

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



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



3. In the **Alias** field, enter a name for the mask.
4. For State, select **On** or **Off** check box to enable or disable masking. The state can be changed at anytime whenever required.
5. In the Mask offset field, enter the offset from which the application should start masking data following the pattern specified in the Pattern field.The value can be specified in terms of either a static offset, that is, from the start of the packet or a relative offset, that is, from a particular protocol layer as specified in the Protocol field.
6. In the Mask length field, enter the length of the packet that must be masked.
7. In the Mask pattern field, enter the pattern for masking the packet. The value of the pattern is from 0 to 255.
8. From the Protocol drop-down list, specifies an optional parameter for masking packets on the data coming from the selected protocol.
9. Click **Save**.

NetFlow

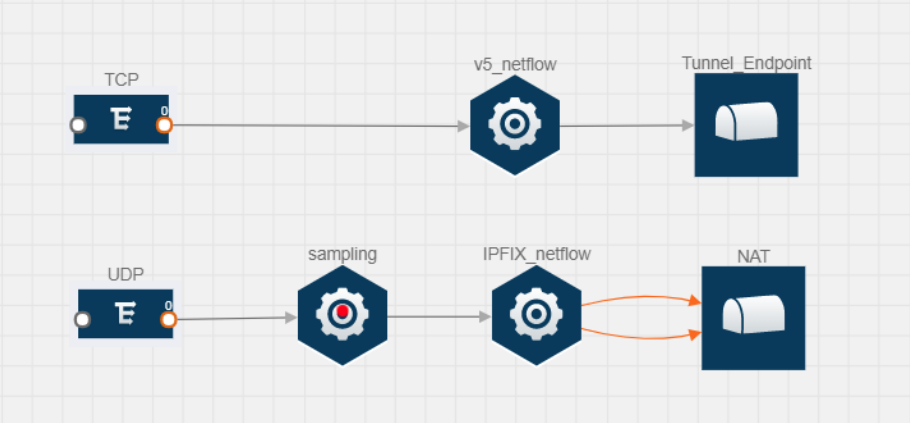
NetFlow collects IP network traffic on all interfaces where NetFlow monitoring is enabled. It gathers information about the traffic flows and exports the NetFlow records, which includes data and templates, to at least one NetFlow collector. The application that serves as a NetFlow collector receives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

The following are the key benefits of NetFlow application:

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

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

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



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

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

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

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

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

Match/Key Fields

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

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

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

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

Collect/Non-Key Fields

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

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

	Description	Supported NetFlow Versions
Counter		
Byte Count	Configures the number of octets since the previous report in incoming packets for the current flow as a non-key field.	v9 and IPFIX
Packet Count	Configures the number of incoming packets since the previous report for this flow as a non-key field.	v9 and IPFIX
Data Link		
Destination MAC	Configures the destination MAC address as a non-key field.	v9 and IPFIX
Egress Des MAC	Configures the post source MAC address as a non-key field.	IPFIX
Ingress Des MAC	Configures the IEEE 802 destination MAC address as a non-key field.	IPFIX
Source MAC	Configures the IEEE 802 source MAC address as a non-key field.	v9 and IPFIX
Timestamp		
Flow End Millisec	Configures the absolute timestamp of the last packet of current flow in milliseconds as a non-key field.	IPFIX
Flow End Sec	Configures the flow start SysUp time as a non-key field.	IPFIX
Flow End Time	Configures the flow end SysUp time as a non-key field.	v9 and IPFIX
Flow Start Millisec	Configures the value of the IP Precedence as a non-key field.	IPFIX
Flow Start Sec	Configures the absolute timestamp of the first packet of this flow as a non-key field.	IPFIX
Flow Startup Time	Configures the flow start SysUp time as a non-key field.	v9 and IPFIX
Flow		
Flow End Reason	Configures the reason for Flow termination as a non-key field.	IPFIX
IPv4		
ICMP Type Code	Configures the type and code of the IPv4 ICMP	v9 and IPFIX

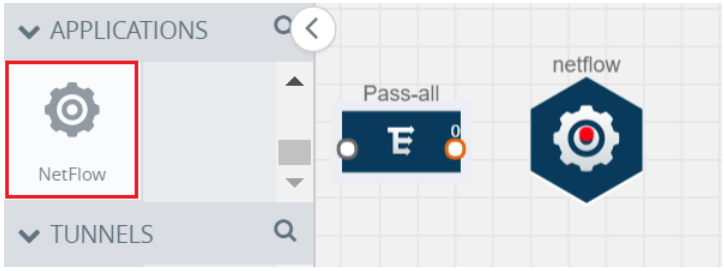
	Description	Supported NetFlow Versions
	message as a non-key field.	
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 ICMP Type	Configures the type of 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 header as a non-key field.	v9 and IPFIX
TCP AcK Number	Configures the acknowledgment number in the TCP header as a non-key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a non-key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a non-key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a non-key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP	IPFIX

	Description	Supported NetFlow Versions
	header as a non-key field.	
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

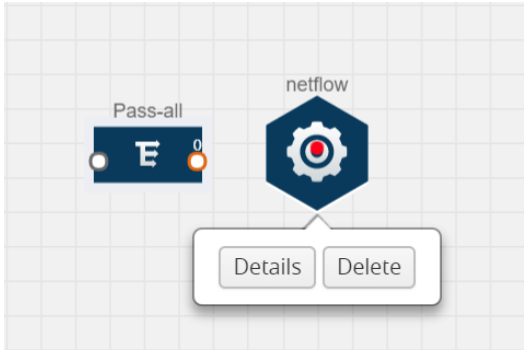
Add Version 5 NetFlow Application

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.

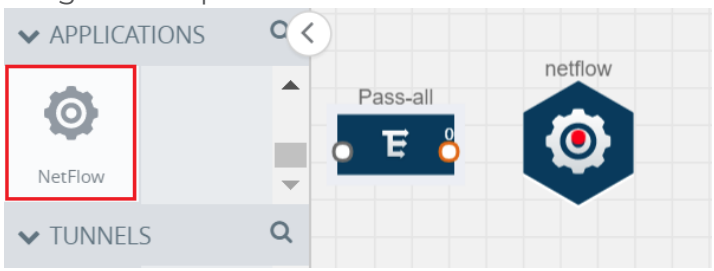
6. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.
7. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it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

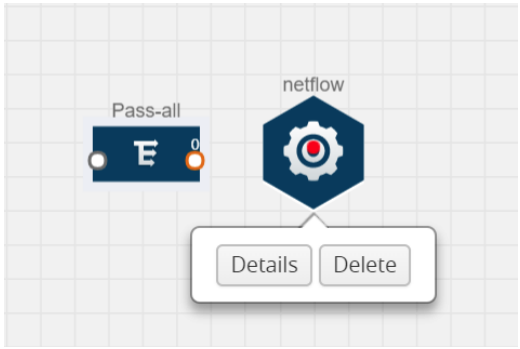
Add Version 9 and IPFIX NetFlow Application

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

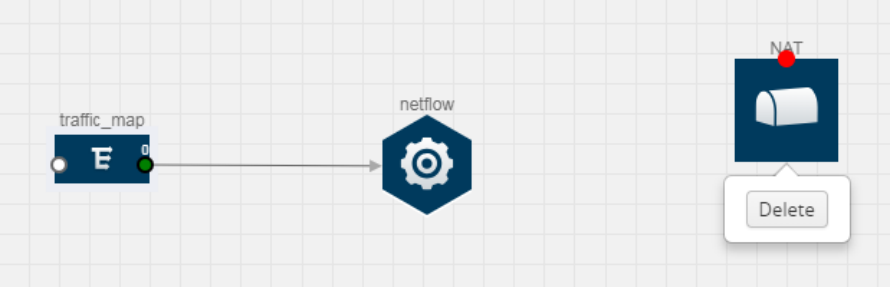
The NetFlow records are exported to the collector over UDP protocol with the configurable source IP and destination IP.

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

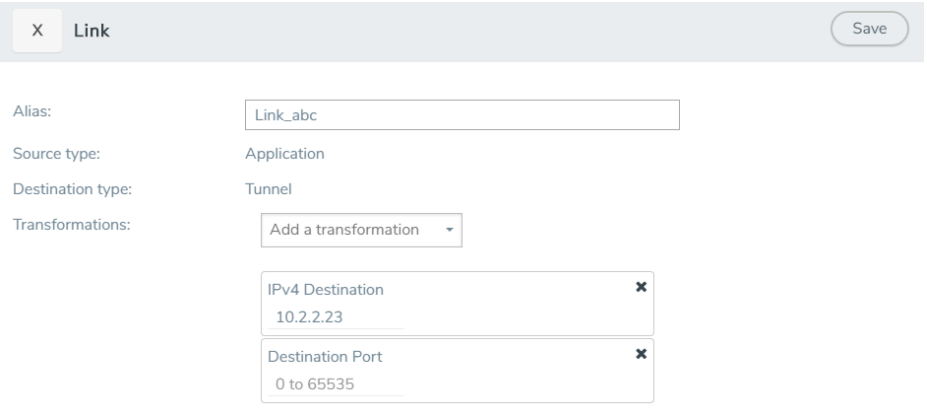
Add NAT and Link NetFlow Application to NAT

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

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



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



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

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

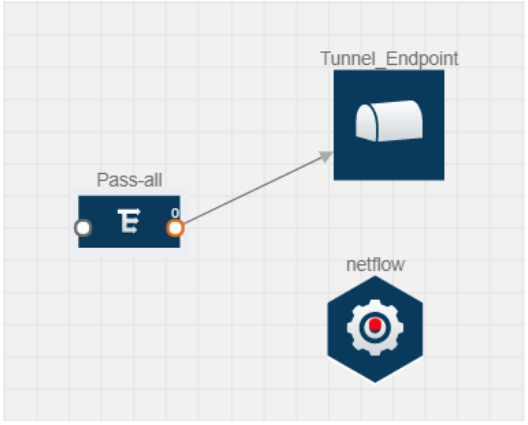
NetFlow Examples

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

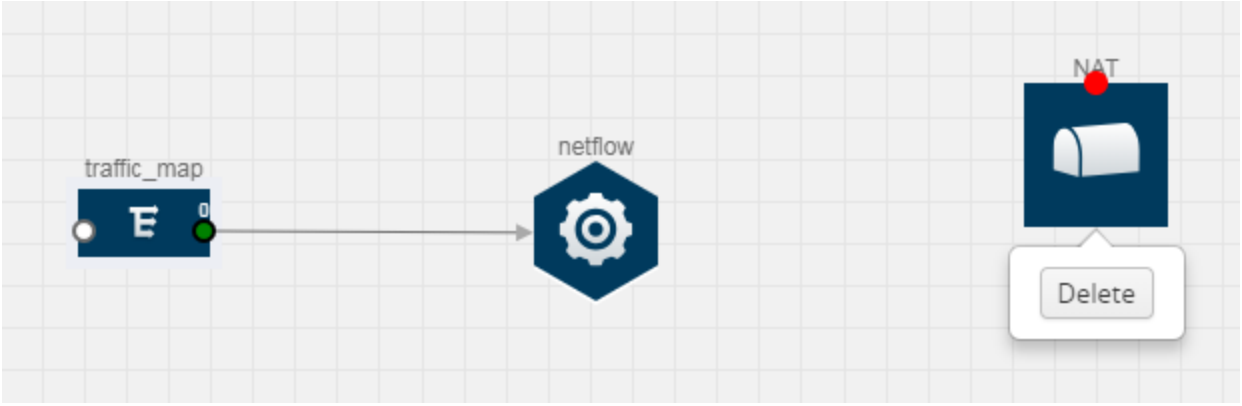
Example 1

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

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



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



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

Deploy Monitoring Session

To deploy the monitoring session:

1. Drag and drop one or more maps from the **MAP Library** to the workspace.
2. (Optional) To add Inclusion and Exclusion maps, drag and drop the maps from the Map Library to their respective section at the bottom of the workspace.
3. (Optional) Drag and drop one or more applications from the APPLICATIONS section to the workspace.

   NOTE: For information about adding applications to the workspace, refer to Add Applications to Monitoring Session.
4. Drag and drop one or more tunnels from the TUNNELS section. The 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 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 V Series node failure.
- Failure—The session is not deployed on any of the GigaVUE V Series nodes and G-vTAP Agents.

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

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

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

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

Add Header Transformations

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

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

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

In addition to header transformation, GigaVUE V Series node allows you to add multiple links to the same destination. Using multiple links, you can send duplicate packets or various transformed packets to the same destination. For example, you can add different 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.

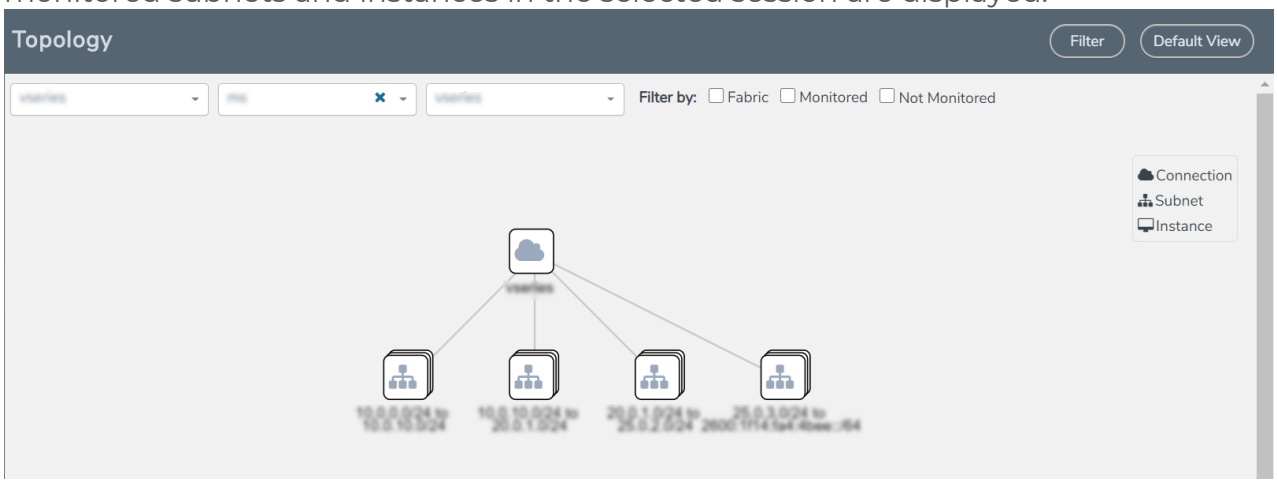
Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

1. On the Monitoring Session page, select **Topology** tab. The Topology page appears.
2. Select a monitoring domain from the **Select monitoring domain...** list.
3. Select a connection from the **Select monitoring session...**list.

4. Select a monitoring session from the **Select connection...** list. The topology view of the monitored subnets and instances in the selected session are displayed.



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

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

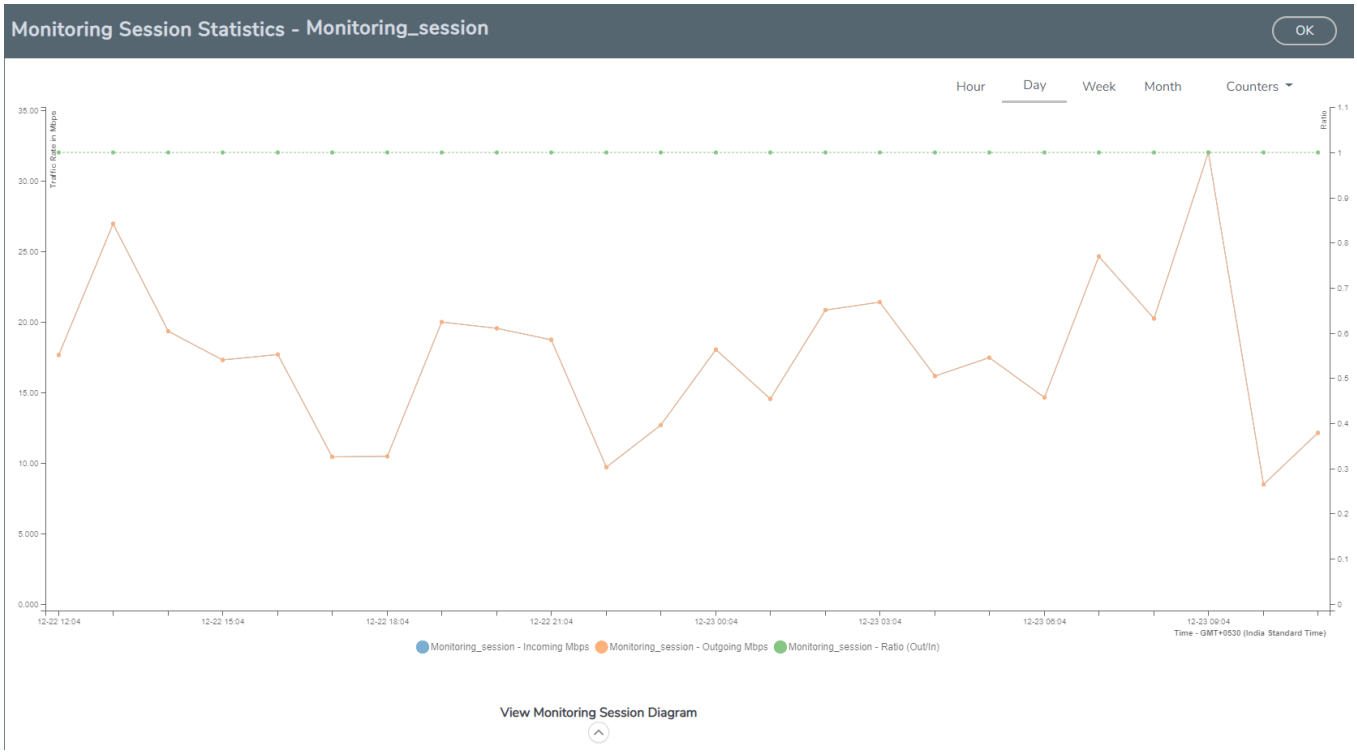
- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the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

View Monitoring Session Statistics

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

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

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



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

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

Administer GigaVUE Cloud Suite for Azure

You can perform the following administrative tasks:

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

Set Up Email Notifications

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

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

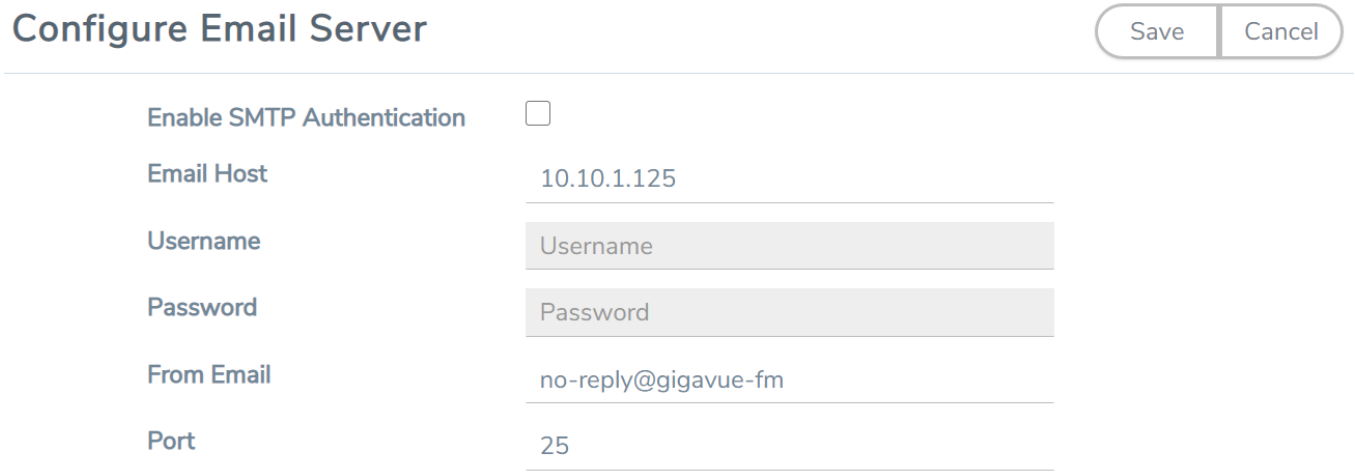
- Azure License Expire
- Fabric Node Down
- Fabric Node Reboot Failed
- Fabric Node Rebooted
- Fabric Node Replacement Launch Failed
- Fabric Node Replacement Launched
- Fabric Node Restart Failed
- Fabric Node Restarted
- Fabric Node Unreachable
- Fabric Node Up

Configure Email Notifications

To configure the automatic email notifications:

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

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



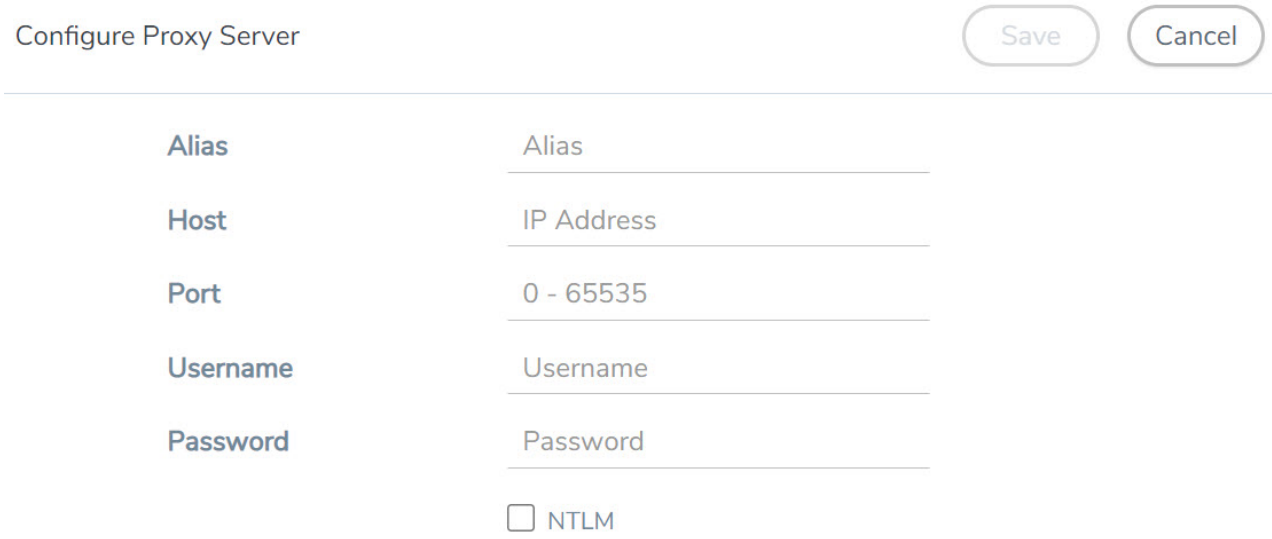
3. Click **Save**.

Configure Proxy Server

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

To create a proxy server:

1. From the left navigation pane, select **Inventory > VIRTUAL > Azure > Settings**. The Configuration page appears.
2. Under **Proxy Server** tab, click **Add**. The **Add Proxy Server** page appears.



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

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

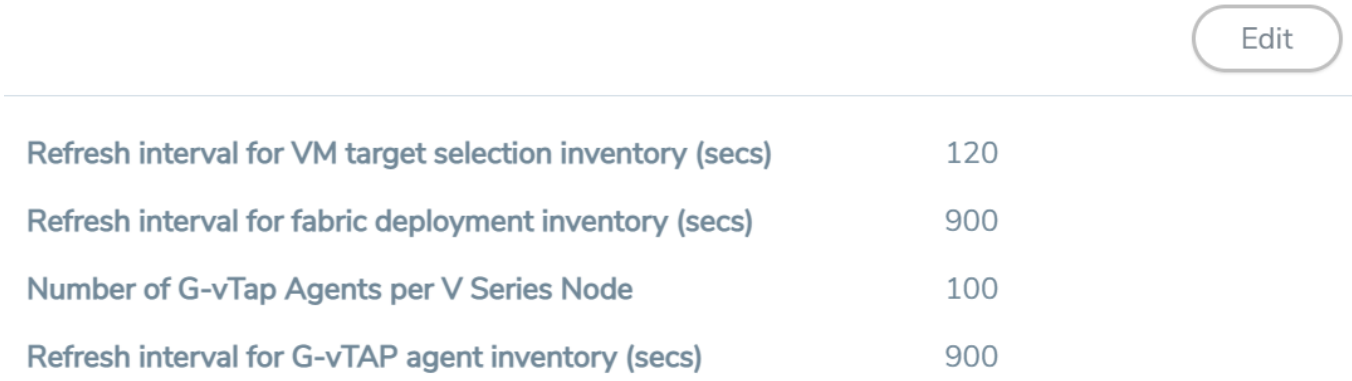
4. Click **Save**. The new proxy server configuration is added to the Proxy Server Configuration page. The proxy server is also listed in the Azure Connection page in GigaVUE-FM.

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

Configure Azure Settings

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

Navigate to **Inventory > VIRTUAL > Azure > Configuration > Settings** to edit the Azure settings.



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

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

Role Based Access Control

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

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

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

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

Resource Category	Cloud Configuration Task
• Threshold Template • Stats • Map library • Tunnel library • Tools library • Inclusion/exclusion Maps	• View Statistics • Create Tunnel End Points

NOTE: Cloud APIs are also RBAC enabled.

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

About Events

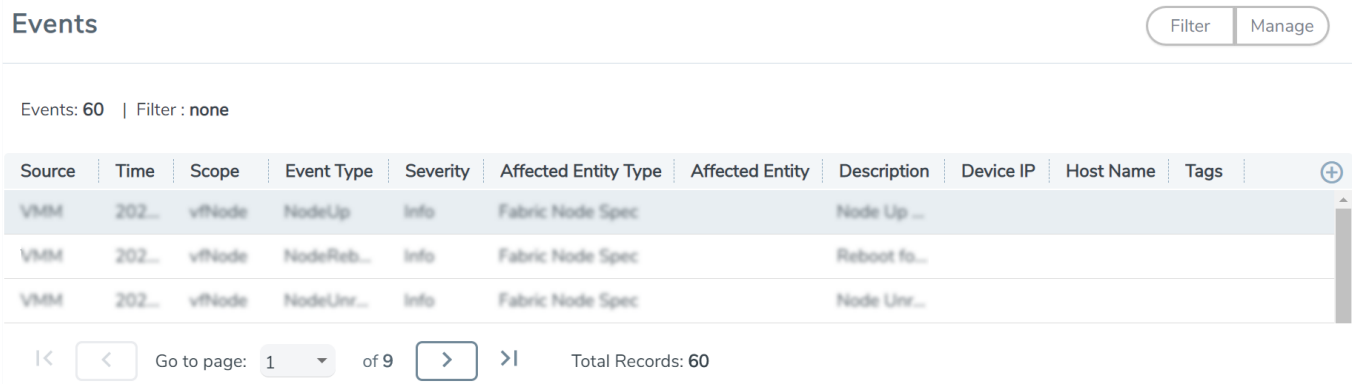
The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

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

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

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

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



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

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

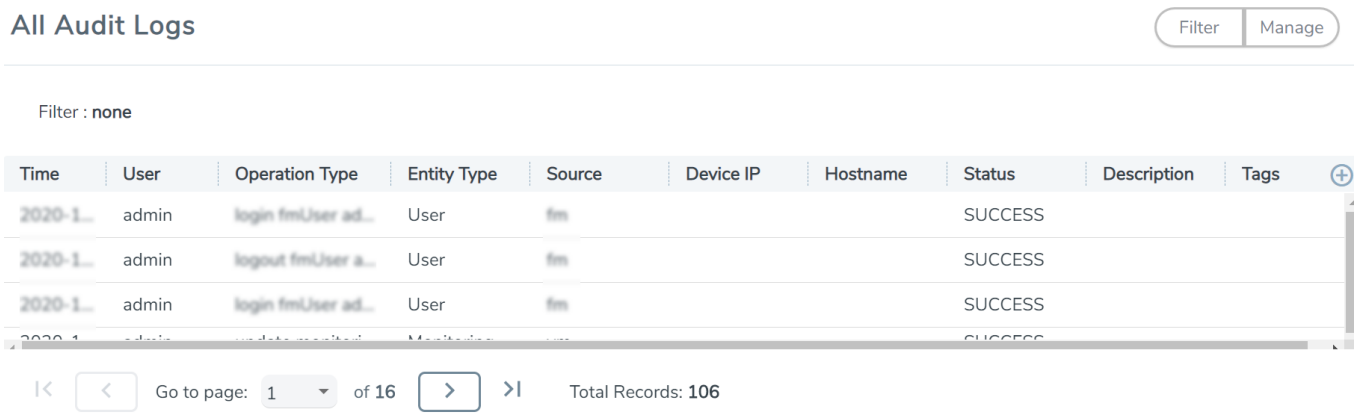
To filter the alarms and event:

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

About Audit Logs

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

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



The Audit Logs have the following parameters:

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

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

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

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

To filter the audit logs, do the following:

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

GigaVUE-FM Version Compatibility Matrix

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

NOTE: GigaVUE-FM version 6.1 supports the latest fabric components version as well as earlier versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

GigaVUE-FM Version Compatibility for V Series 1 Configuration

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Controller	GigaVUE V Series 1 Nodes
6.1.00	v6.1.00	v6.1.00	v1.7-4	v1.7-4
6.0.00	v1.8-7	v1.8-7	v1.7-4	v1.7-4
5.16.00	v1.8-5	v1.8-5	v1.7-3	v1.7-3
5.15.00	v1.8-5	v1.8-5	v1.7-2	v1.7-2
5.14.00	v1.8-4	v1.8-4	v1.7-1	v1.7-1
5.10.01, 5.11.00, 5.11.01, 5.12.00, 5.13.00, 5.13.01	v1.7-1	v1.7-1	v1.7-1	v1.7-1

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.1 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
***GigaVUE-TA25E Hardware Installation Guide**
***GigaVUE-TA200E Hardware Installation Guide**
GigaVUE-TA25 Hardware Installation Guide

GigaVUE Cloud Suite 6.1 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA10 Hardware Installation Guide
GigaVUE-TA40 Hardware Installation Guide
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA100-CXP Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for AnyCloud Guide

GigaVUE Cloud Suite 6.1 Hardware and Software Guides
Universal Container Tap Guide
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for OpenStack–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)