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.

<table>
<thead>
<tr>
<th>Product Version</th>
<th>Document Version</th>
<th>Date Updated</th>
<th>Change Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.13.00</td>
<td>2.0</td>
<td>09/07/2021</td>
<td>Updated <a href="#">Prepare Virtual Machines to Monitor Traffic</a> with latest G-vTAP agent information.</td>
</tr>
<tr>
<td>5.13.00</td>
<td>1.0</td>
<td>08/13/2021</td>
<td>Added V Series 2 configuration information. Refer to <a href="#">Create Monitoring Domain</a> and <a href="#">Configure and Manage Resources using V Series 2</a> for details.</td>
</tr>
</tbody>
</table>
Contents

GigaVUE Cloud Suite for Azure Guide ......................................................... 1
  Change Notes ...................................................................................... 3
  Contents ............................................................................................. 4
GigaVUE Cloud Suite for Azure ..................................................................... 7
About GigaVUE Cloud Suite for Azure .......................................................... 8
  Components of GigaVUE Cloud Suite for Azure ........................................ 9
  Architecture of GigaVUE Cloud Suite for Azure ....................................... 11
    Hybrid Cloud ................................................................................ 11
    Multi-VNet Cloud ........................................................................ 11
  Shared Controller/GigaVUE V Series Node Configuration ..................... 12
  Ericsson 5G Core vTAP ...................................................................... 13
Get Started with GigaVUE Cloud Suite for Azure Deployment ..................... 18
  License Information ............................................................................. 18
    Bring Your Own License (BYOL) ......................................................... 18
    Pay-As-You-Go (PAYG) .................................................................. 19
    Volume Based License (VBL) ........................................................... 19
    Apply Licensing .............................................................................. 19
  Before You Begin ................................................................................ 19
    Network Requirements ...................................................................... 19
    VPN Connectivity ............................................................................ 23
    Obtain Image .................................................................................. 23
  Install and Upgrade GigaVUE-FM ......................................................... 24
Prepare Virtual Machines to Monitor Traffic .................................................. 25
  Linux G-vTAP Agent Installation .......................................................... 25
    Single NIC Configuration .................................................................. 25
    Dual NIC Configuration ..................................................................... 26
    Install G-vTAP Agents ...................................................................... 26
  Windows G-vTAP Agent Installation ......................................................... 28
    Windows G-vTAP Agent Installation Using MSI Package .................. 28
    Windows G-vTAP Agent Installation Using ZIP Package .................. 29
  Install IPSec on G-vTAP Agent ............................................................. 31
    Install G-vTAP from Ubuntu/Debian Package .................................... 31
    Install G-vTAP from Red Hat Enterprise Linux and Centos ............. 32
    Install G-vTAP from Red Hat Enterprise Linux and Centos with Selinux Enabled .......................................................... 32
Create Images with the Agent Installed ................................................................. 34

Deploy GigaVUE Cloud Suite for Azure ................................................................. 35
  Pre-Configuration Checklist .................................................................................. 35
  Launch GigaVUE-FM VM from Azure .................................................................. 36
  Establish Connection to Azure ............................................................................. 37
    Application ID with client secret ........................................................................ 37
    Managed Service Identity .................................................................................... 43
    Accept EULA and Enable Programmatic Deployment in Azure ......................... 45
  Create Monitoring Domain ................................................................................... 46
  Configure GigaVUE Fabric Components ............................................................... 50
    Configure G-vTAP Controller ............................................................................. 52
    Configure GigaVUE Cloud Suite V Series Proxy/Controller .............................. 54
    Configure GigaVUE Cloud Suite V Series Node ................................................. 55

Configure and Manage Resources using V Series 2 ............................................. 57
  Create a Monitoring Session ............................................................................... 57
  Create Ingress and Egress Tunnels ...................................................................... 58
  Create a New Map ................................................................................................ 59
  Add Applications to Monitoring Session .............................................................. 62
    Slicing ................................................................................................................ 62
    Masking .............................................................................................................. 63
    Dedup ................................................................................................................ 64
    Load Balancing ................................................................................................. 65
    PCAPng ............................................................................................................. 66
  Deploy Monitoring Session .................................................................................. 68
  View Monitoring Session Statistics ...................................................................... 69
  Visualize the Network Topology ......................................................................... 70

Configure and Manage Resources using V Series 1 ............................................. 72
  Create a Monitoring Session ............................................................................... 73
  Create Tunnel Endpoints ...................................................................................... 73
  Create Map .......................................................................................................... 75
    Agent Pre-filtering ............................................................................................. 77
  Add Applications to Monitoring Session .............................................................. 80
    Sampling ............................................................................................................ 81
    Slicing ................................................................................................................. 82
    Masking ............................................................................................................. 83
    NetFlow ............................................................................................................. 84
  Deploy Monitoring Session .................................................................................. 94
  Add Header Transformations ............................................................................... 96
  View Monitoring Session Statistics ..................................................................... 97

Administer GigaVUE Cloud Suite for Azure .......................................................... 99
  Set Up Email Notifications .................................................................................. 99
Configure Email Notifications .......................................................... 99
Configure Proxy Server ........................................................................ 100
Configure Azure Settings ...................................................................... 101
Role Based Access Control .................................................................... 102
About Events ....................................................................................... 103
About Audit Logs .................................................................................. 104

**GigaVUE-FM Version Compatibility Matrix** ........................................... 106
  GigaVUE-FM Version Compatibility for V Series 2 Configuration ........... 106
  GigaVUE-FM Version Compatibility for V Series 1 Configuration ........... 106

**Additional Sources of Information** ..................................................... 107
  Documentation .................................................................................... 107
    How to Download Software and Release Notes from My Gigamon .......... 109
  Documentation Feedback ...................................................................... 110
  Contact Technical Support .................................................................... 111
  Contact Sales ...................................................................................... 111
    Premium Support ............................................................................... 111
  The Gigamon Community .................................................................... 111
GigaVUE Cloud Suite for Azure

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

Refer to the following sections for details:

- About GigaVUE Cloud Suite for Azure
- Get Started with GigaVUE Cloud Suite for Azure Deployment
- Prepare Virtual Machines to Monitor Traffic
- Deploy GigaVUE Cloud Suite for Azure
- Configure and Manage Resources using V Series 2
- Configure and Manage Resources using V Series 1
- Administer GigaVUE Cloud Suite for Azure
- Compatibility Matrix for Azure
About GigaVUE Cloud Suite for Azure

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

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

Refer to the following sections for details:

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

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigaVUE® Fabric Manager (GigaVUE-FM)</td>
<td>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.</td>
</tr>
<tr>
<td>G-vTAP Agents</td>
<td>An agent that is deployed in the Elastic Compute Cloud (EC2) instance. This agent mirrors the selected traffic from the instances (virtual machines) to the GigaVUE® V Series node.</td>
</tr>
<tr>
<td>GigaVUE V Series nodes</td>
<td>A visibility node that aggregates mirrored traffic from multiple GvTAP agents. 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 IP GRE or VXLAN tunnels to deliver traffic to tool endpoints. <strong>NOTE:</strong> With G-vTAP version 1.7-1 IPSec can be used to establish a secure tunnel between G-vTAP agents and GigaVUE V Series nodes, especially in a centralized controller and GigaVUE V Series node configuration where cross VNet tunneling may be required to be encrypted.</td>
</tr>
<tr>
<td>G-vTAP Controllers</td>
<td>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.</td>
</tr>
<tr>
<td>GigaVUE V Series Controllers</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

| Option 1: Standard Configuration | GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in all V Nets |
| Option 2: Shared Controller Configuration | GigaVUE V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in a shared VNet |

**NOTE:** Peering must be active between V Nets within the same monitoring domain if the shared controller and V Series option is chosen for configuring the components.
This guide provides instructions on launching GigaVUE-FM in Azure. For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation, Migration, and Upgrade Guide*. 
The GigaVUE Cloud Suite for Azure supports many deployment modes. Following are the most common cloud deployment models:

- Hybrid Cloud
- Multi-VNet Cloud
- Shared Controller/GigaVUE V Series Node Configuration
- Ericsson 5G Core vTAP

### Hybrid Cloud

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

### Multi-VNet Cloud

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

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

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

With this deployment model, it is easy to manage the controllers and nodes as they are launched from a shared Virtual Private Cloud (VNet) thereby, reducing the cost involved in the configuration and management of the controllers and nodes in each V Nets.
Ericsson 5G Core vTAP

The Ericsson 5G Core vTAP is a virtual tap that integrates with Ericsson’s 5G Packet Core Controller module and orchestrates the flow of traffic to the GigaVUE V Series nodes, where the traffic is processed and sent to monitoring tools. This allows 5G users who have deployed Ericsson’s Packet Core Controller to forward the traffic to the Gigamon Visibility & Analytics Fabric, perform any necessary transformations and deliver to the tools for 5G visibility.
Refer to the following sections for details:

- **About Ericsson 5G Core vTAP**
- **Rules and Notes**

### About Ericsson 5G Core vTAP

The Ericsson 5G Core vTAP receives the 3GPP messages (per the 3GPP protocol type) encapsulated within GRE and UDP (GRE-in-UDP) packets from the Core Controller module. The vTAP captured packets consist of:

- **Control Packets:** Contain JSON metadata common for the traffic (the blue part in the image below).
- **Data Packets:** Contain 3GPP packets in PCAPng file format (the red part in the image below). The PCAPng files are encapsulated within the GRE and UDP headers and are fragmented based on the Maximum Transmission Unit (MTU) value. The PCAPng file consists of a section header, an interface header, and an enhanced header that are part of the PCAPng headers. Refer to the [PCAPng Application](#) for details on the header information.

<table>
<thead>
<tr>
<th>Delivery Header</th>
<th>UDP Header</th>
<th>GRE Header</th>
<th>JSON Metadata</th>
<th>0x00</th>
</tr>
</thead>
</table>

#### Common metadata for the stream

<table>
<thead>
<tr>
<th>Delivery Header</th>
<th>UDP Header</th>
<th>GRE Header</th>
<th>Packet Data</th>
<th>Delivery Header</th>
<th>UDP Header</th>
<th>GRE Header</th>
<th>Packet Data</th>
<th>………</th>
</tr>
</thead>
</table>

#### Tapped data in pcapng format

The GigaVUE V Series node processes the PCAPng files as follows:

- Decapsulates the GRE-in-UDP headers.
- Parses the PCAPng file to send out the inner data packets either to the tools or to other applications.

This feature provides the following functionalities:

- **GRE-In-UDP Tunnel Decapsulation:** New tunnel type that decapsulates the GRE and UDP header files and routes the ingress traffic to the PCAPng application.
- **PCAPng Application:** New GigaSMART application to parse the PCAPng files.
GRE-In-UDP Tunnel Decapsulation

The GRE-In-UDP tunnel is a new tunnel type that supports decapsulating the GRE-in-UDP headers in the vTAP captured data packets. The decapsulation of the tunnel headers is common for both control and data packets. However, the control packets (with JSON metadata format) are dropped based on the GRE Key value '0'. The data packets (either fragmented or unfragmented) are handled as follows:

<table>
<thead>
<tr>
<th>S. No</th>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1     | Reassembly of fragmented data packets (if fragmented packets are received) | The fragmented packets are reassembled based on standard IP header-based reassembly using the following fields:  
  - More Fragments (MF) field in IPv4 packets  
  - Identification field in IPv6 packets |
| 2     | Decap tunnel lookup                          | The ingress packet fields are parsed to find a matching Tunnel End Point (TEP) based on the following header fields:  
  - Destination IP  
  - Source IP  
  - UDP port numbers  
  - GRE key |
| 3     | Decapsulation of headers                     | If a matching TEP is found, the encapsulation headers in the packet are removed and the packet is forwarded to the PCAPng application. |

Refer to the PCAPng section for the detailed configuration steps.

PCAPng Application

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

- Mandatory Blocks
  - Section Header Block (SHB)
- Optional Blocks
  - Interface Description Block (IDB)
  - Enhanced Packet Block (EPB)
  - Simple Packet Block
  - Name Resolution Block
  - Interface Statistics Block

The actual packets are present in the Enhanced Packet Block. The block data is parsed to find the start and end offset of the valid packets and the packet is sent out to the next application.
NOTE: Only one EPB in a PCAPng file is supported.

The PCAPng application processes the data depending on the packet type that contains a combination of the blocks mentioned above:

<table>
<thead>
<tr>
<th>Block Combination</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHB+IDB+EPB+data</td>
<td>Packets are parsed, validated, and the data packet is sent out.</td>
</tr>
<tr>
<td>SHB+IDB</td>
<td>Packets are dropped.</td>
</tr>
<tr>
<td>EPB+Data</td>
<td>Packets are parsed, validated, and the data packet is sent out.</td>
</tr>
</tbody>
</table>

The PCAPng application validates if the incoming data matches any of the above three formats in the same order, and processes the packets accordingly.

The following figure shows a sample PCAPng file format that contains one section header block:

Rules and Notes

- This feature is supported only in GigaVUE V Series 2 nodes of medium instance type (4 vCPU, 8GB RAM).
• This feature is limited to PCAPng file format.
• In case of unfragmented IP packets, this feature supports processing of a single PCAPng file per packet.
• In case of fragmented IP packets, this feature supports processing of a single PCAPng file after reassembly.
• GRE or UDP checksum validation is not performed as part of this feature.
Get Started with GigaVUE Cloud Suite for Azure Deployment

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

Refer to the following sections for details:

- License Information
- Before You Begin
- 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 and the hourly Pay-As-You-Go (PAYG) model that you can avail from the Azure Marketplace.

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.
Pay-As-You-Go (PAYG)

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

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

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

Volume Based License (VBL)

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

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

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.

- **Network Requirements**
- **Network Security Groups**

Network Requirements

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

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

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

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Subnet</td>
<td>Subnet that the GigaVUE-FM uses to communicate with the GigaVUE Cloud Suite V Series nodes and controllers.</td>
</tr>
<tr>
<td>Data Subnet</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Ingress is VXLAN from agents</td>
</tr>
<tr>
<td></td>
<td>- Egress is either VXLAN tunnel to tools or to GigaVUE H Series tunnel port, or raw packets through a NAT when using NetFlow.</td>
</tr>
</tbody>
</table>

**NOTE:** If you are using a single subnet, then the Management subnet will also be used as a Data Subnet.

Network Interfaces (NICs) for VMs

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

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

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

Network Security Groups

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

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

**Network Security Groups for V Series 2 Node**

Following is the Network Firewall Requirements for V Series 2 node deployment.
<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Port</th>
<th>Source/Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GigaVUE-FM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>443</td>
<td>Administrator Subnet</td>
<td>Management connection to GigaVUE-FM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9900</td>
<td>GigaVUE-FM IP</td>
<td>Allows G-vTAP Controller to communicate with GigaVUE-FM</td>
</tr>
<tr>
<td>Outbound (optional)</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8890</td>
<td>V Series Controller/Proxy IP</td>
<td>Allows GigaVUE-FM to communicate with V Series Controller/Proxy</td>
</tr>
<tr>
<td>Outbound (configuration without V Series Proxy)</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8889</td>
<td>V Series 2 Node IP</td>
<td>Allows GigaVUE-FM to communicate with V Series node</td>
</tr>
<tr>
<td><strong>G-vTAP Controller</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9900</td>
<td>GigaVUE-FM IP</td>
<td>Allows G-vTAP Controller to communicate with GigaVUE-FM</td>
</tr>
<tr>
<td>Outbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9901</td>
<td>G-vTAP Controller IP</td>
<td>Allows G-vTAP Controller to communicate with G-vTAP Agents</td>
</tr>
<tr>
<td><strong>G-vTAP Agent</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9901</td>
<td>G-vTAP Controller IP</td>
<td>Allows G-vTAP agents to communicate with G-vTAP Controller</td>
</tr>
<tr>
<td>Outbound</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>UDP (VXLAN)</td>
<td>VXLAN (default 4789)</td>
<td>G-vTAP Agent or Subnet IP</td>
<td>Allows G-vTAP agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes</td>
</tr>
<tr>
<td></td>
<td>IP</td>
<td>IP (L2GRE)</td>
<td>L2GRE</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>V Series Controller/Proxy (optional)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8890</td>
<td>GigaVUE-FM IP</td>
<td>Allows GigaVUE-FM to communicate with V Series Controller/Proxy</td>
</tr>
<tr>
<td>Outbound</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8889</td>
<td>V Series 2 node IP</td>
<td>Allows V Series Controller/Proxy to communicate with V Series node</td>
</tr>
<tr>
<td><strong>V Series 2 node</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>8889</td>
<td></td>
<td>Allows V Series Controller/Proxy or GigaVUE-FM to communicate with V Series node</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigaVUE-FM IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V Series Controller/Proxy IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### GigaVUE Cloud Suite for Azure Guide

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Port</th>
<th>Source/Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>UDP</td>
<td>UDP (VXLAN)</td>
<td>VXLAN (default 4789)</td>
<td>G-vTAP Agent or Subnet IP</td>
<td>Allows G-vTAP agents to (VXLAN) tunnel traffic to V Series nodes</td>
</tr>
<tr>
<td>Inbound</td>
<td>UDP</td>
<td>UDPGRE</td>
<td>4754</td>
<td>Ingress Tunnel</td>
<td>Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes</td>
</tr>
<tr>
<td>Outbound</td>
<td>Custom UDP Rule</td>
<td>UDP (VXLAN) • IP Protocol (L2GRE)</td>
<td>VXLAN (default 4789)</td>
<td>Tool IP</td>
<td>Allows V Series node to communicate and tunnel traffic to the Tool</td>
</tr>
<tr>
<td>Outbound (optional)</td>
<td>ICMP</td>
<td>ICMP</td>
<td>• echo request • echo reply</td>
<td>Tool IP</td>
<td>Allows V Series node to health check tunnel destination traffic</td>
</tr>
</tbody>
</table>

### Network Security Groups for V Series 1 Node

<table>
<thead>
<tr>
<th>Direction</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source and CIDR, IP, or Security Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>G-vTAP Controller</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9900 Custom GigaVUE-FM IP</td>
<td>Allows GigaVUE-FM to communicate with G-vTAP Controllers</td>
</tr>
<tr>
<td>G-vTAP Agent</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9901 Custom G-vTAP Controller IP</td>
<td>Allows G-vTAP Controllers to communicate with G-vTAP agents</td>
</tr>
<tr>
<td>GigaVUE Cloud Suite V Series Controller</td>
<td>Custom TCP Rule</td>
<td>TCP</td>
<td>9902 Custom GigaVUE-FM IP</td>
<td>Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite V Series Controllers</td>
</tr>
</tbody>
</table>
### VPN Connectivity

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

### Obtain Image

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

#### GigaVUE Cloud Suite Cloud in Azure Public Cloud

GigaVUE Cloud Suite Cloud is available in the Azure Marketplace for both the Bring Your Own License (BYOL) options.

#### GigaVUE Cloud Suite Cloud in Azure Government

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

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

---

**Table: GigaVUE Cloud Suite V Series 1 node**

<table>
<thead>
<tr>
<th>Direction</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source and CIDR, IP, or Security Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP 9903</td>
<td>Custom GigaVUE V Series Controller IP</td>
<td>Allows GigaVUE Cloud Suite V Series Controllers to communicate with GigaVUE Cloud Suite V Series nodes</td>
</tr>
</tbody>
</table>

**VXLAN Traffic**

<table>
<thead>
<tr>
<th>Direction</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Source and CIDR, IP, or Security Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Custom UDP Rule</td>
<td>VXLAN 4789</td>
<td></td>
<td>Allows mirrored traffic from G-vTAP agents to be sent to GigaVUE Cloud Suite V Series nodes using VXLAN tunnel. Allows monitored traffic to be sent from GigaVUE Cloud Suite V Series nodes to the tools using VXLAN tunnel.</td>
</tr>
</tbody>
</table>
Install and Upgrade GigaVUE-FM

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

- **Cloud**—To install GigaVUE-FM inside your Azure environment, you can simply launch the GigaVUE-FM instance in your VNet. For installing the GigaVUE-FM instance, refer to Get Started with GigaVUE Cloud Suite for Azure Deployment.

- **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.
Prepare Virtual Machines to Monitor Traffic

A G-vTAP agent is the primary Gigamon monitoring module that is deployed in the Virtual Machines (VMs). This agent mirrors the selected traffic from the VMs, encapsulates it using L2GRE or VXLAN tunneling, and forwards it to the GigaVUE Cloud Suite® V Series node.

A G-vTAP agent consists of a source interface and a destination interface. The network packets collected from the source interface are sent to the destination interface. From the destination interface, the packets traverse through the L2GRE or VXLAN tunnel interface to the GigaVUE Cloud Suite V Series node.

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

Refer to the following sections for more information:

- Linux G-vTAP Agent Installation
- Windows Agent Installation
- 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.

**Install G-vTAP from Ubuntu/Debian Package**

To install from a Debian package:
1. Download the G-vTAP Agent 1.8-2 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:

   ```
   ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_1.8-2_amd64.deb
   ubuntu@ip-10-0-0-246:~$ sudo dpkg -i gvtap-agent_1.8-2_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:

   **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 eth1; 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. Reboot the instance.

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

   ```
   ubuntu@ip-10-0-0-246:~$ sudo /etc/init.d/gvtap-agent status
   ```

Install G-vTAP from RPM package

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

1. Download the G-vTAP Agent 1.8-2 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:

   ```
   [user@ip-10-0-0-214 ~]$ lsgvtap-agent_1.8-2_x86_64.rpm [user@ip-10-0-0-214 ~]$ sudo rpm -i
gvtap-agent_1.8-2_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:

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

```bash
# 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

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

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

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

4. Save the file.
5. Reboot the instance.

Check the status with the following command:

```bash
[user@ip-10-0-0-214 ~] $ sudo service gvtap-agent status G-vTAP Agent is running
```

## Windows G-vTAP Agent Installation

**NOTE:** 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.

### Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent 1.8-2 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. The following examples registers 192.168.1.0/24 as the mirror source for both ingress and egress traffic and 192.168.1.0/24 as the destination for this traffic:

   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:
     - 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 interface 192.168.1.2/32 to send out the mirrored packets
   ```
   # 192.168.1.0/24  mirror-src-ingress  mirror-src-egress
   # 192.168.1.2/32  mirror-dst
   ```

   **Example 2**—Configuration example to monitor ingress traffic at interface 192.168.1.0/24 and egress traffic at interface 192.168.2.0/24; use the interface 192.168.1.2/32 to send out the mirrored packets
   ```
   # 192.168.1.0/24  mirror-src-ingress
   # 192.168.2.0/24  mirror-src-egress
   # 192.168.1.2/32  mirror-dst
   ```

4. Save the file.
5. Reboot the instance.

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

**Windows G-vTAP Agent Installation Using ZIP Package**

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

1. Download the Windows G-vTAP Agent 1.8–2 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. The following examples registers 192.168.1.0/24 as the mirror source for both ingress and egress traffic and 192.168.1.0/24 as the destination for this traffic:

```
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:
  - 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 interface 192.168.1.2/32 to send out the mirrored packets

```
# 192.168.1.0/24  mirror-src-ingress  mirror-src-egress
# 192.168.1.2/32  mirror-dst
```

**Example 2**—Configuration example to monitor ingress traffic at interface 192.168.1.0/24 and egress traffic at interface 192.168.2.0/24; use the interface 192.168.1.2/32 to send out the mirrored packets

```
# 192.168.1.0/24  mirror-src-ingress
# 192.168.2.0/24  mirror-src-egress
# 192.168.1.2/32  mirror-dst
```

5. Save the file.
6. Reboot the instance.

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 and GigaVUE V Series nodes, then you must install IPSec on G-vTAP agent instances. To install IPSec on G-vTAP agent you need the following files:

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

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

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

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

**Install G-vTAP from Ubuntu/Debian Package**

1. Launch the Ubuntu/Debian image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_1.8-2_amd64.deb
   - gvtap-ipsec_1.8-2_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:
   ```sh
dpkg -i gvtap-agent_1.8-2_amd64.deb
   ```
5. Modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces:
   ```sh
   eth0# mirror-src-ingress mirror-src-egress mirror-dst
   sudo /etc/init.d/gvtap-agent restart
   sudo /etc/init.d/gvtap-agent status
   ```

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

7. Install IPSec package:
   `sudo dpkg -i gvtap-ipsec_1.8-2_amd64.deb`

**Install G-vTAP from Red Hat Enterprise Linux and Centos**

1. Launch RHEL/Centos agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_1.8-2_x86_64.rpm
   - gvtap-ipsec_1.8-2_x86_64.rpm
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP agent.
4. Install G-vTAP agent package:
   `sudo rpm -ivh gvtap-agent_1.8-2_x86_64.rpm`
5. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:
   ```
   # eth0 mirror-src-ingress mirror-src-egress mirror-dst
   #
   # sudo /etc/init.d/gvtap-agent restart
   ```
6. Install strongSwan:
   `tar -xvf strongswan-5.7.1-1.el7.x86_64.tar.gz`
   `cd strongswan-5.7.1-1.el7.x86_64`
   `sudo sh ./swan-install.sh`
7. Install IPSec package:
   `sudo rpm -i gvtap-ipsec_1.8-2_x86_64.rpm`

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

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

1. Launch the RHEL/Centos agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_1.8-2_x86_64.rpm
   - gvtap-ipsec_1.8-2_x86_64.rpm
   - gvtap.te and gvtap_ipsec.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   `semodule_package -o gvtap.pp -m gvtap.mod`
   `sudo semodule -i gvtap.pp`

5. Checkmodule -M -m -o gvtap_ipsec.mod gvtap_ipsec.te
   `semodule_package -o gvtap_ipsec.pp -m gvtap_ipsec.mod`
   `sudo semodule -i gvtap_ipsec.pp`

6. Install G-vTAP agent package:
   `sudo rpm -ivh gvtap-agent_1.8-2_x86_64.rpm`

7. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:
   `# eth0 mirror-src-ingress mirror-src-egress mirror-dst`
   `# sudo /etc/init.d/gvtap-agent restart`

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

9. Install IPSec package:
   `sudo rpm -i gvtap-ipsec_1.8-2_x86_64.rpm`
Create Images with the Agent Installed

If you want to avoid downloading and installing the G-vTAP agents every time there is a new VM to be monitored, you can save the G-vTAP agent running on 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.
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 both the Bring Your Own License (BYOL) and the Pay-As-You-Go (PAYG) 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:

- Pre-Configuration Checklist
- Launch GigaVUE-FM VM from Azure
- Establish Connection to Azure
- Create Monitoring Domain
- Configure GigaVUE Fabric Components

**Pre-Configuration Checklist**

The following table provides information that you must obtain to ensure a successful and efficient configuration using the GigaVUE-FM user interface:

<table>
<thead>
<tr>
<th>Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNet ID(s)</td>
</tr>
<tr>
<td><strong>NOTE</strong>: In the portal, VNet ID is available under Properties as Resource ID. You can get the VNet ID from the URL <a href="https://resources.azure.com">https://resources.azure.com</a>. You can also find the VNet ID from Azure PowerShell or use Azure CLI.</td>
</tr>
<tr>
<td>VNet Peering</td>
</tr>
<tr>
<td><strong>NOTE</strong>: Peering must be active between VNets within the same monitoring domain. This is required only when shared controller option is chosen for configuring the components.</td>
</tr>
</tbody>
</table>
### Required Information

- Resource Group ID(s)
- VM ID of GigaVUE-FM
- Public or Private IP of GigaVUE-FM
- Static Public IP

**NOTE:** If GigaVUE-FM is installed in the enterprise data center, a Public IP is required for G-vTAP controllers and GigaVUE Cloud Suite V Series controllers to communicate with GigaVUE-FM.

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

### Launch GigaVUE-FM VM from Azure

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compute Resources</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Compute                  | Ensure that the required GigaVUE-FM image is available. | • Refer to Create VM -Azure Portal topic in the Microsoft Azure Documentation.  
|                          |                                                  | • Obtain Image                                |

**Configure Virtual Network**

- Configure the virtual network with the required parameters:
  - Virtual Network
  - Subnet
  - Public IP Address

  • Network Requirements

**Configure Storage**

- Virtual Machine Size
  - For V Series 2 configuration, the recommended virtual machine size is **D4S_V3 Standard** and for the V Series 1 configuration, the recommended virtual machine size is **Standard**

  • Refer to VM sizes topic in the Microsoft Azure Documentation.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS2_v2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configure Network Security**

<table>
<thead>
<tr>
<th>Basic Settings</th>
<th>Choose the required authentication type:</th>
<th>Refer to Create VM - Azure Portal topic in the Microsoft Azure Documentation.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• SSH public key</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password authentication</td>
<td></td>
</tr>
</tbody>
</table>

| Network Security Group | Configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components. | Network Security Groups |

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

If GigaVUE-FM is deployed in Azure, use admin123All as the password for the admin user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

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

## 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 authentication with Azure.

Refer to the following topics.

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

### Application ID with client secret

GigaVUE-FM supports application id with client secret authentication. When using GigaVUE-FM to connect to Azure, it uses a service principal. A service principal is an account for a non-human such as an application to connect to Azure. The key fields required for GigaVUE-FM to connect to Azure are: Subscription ID, Tenant ID, Application ID and Application Secret.
When creating the service principal using the Azure CLI, the output of that command will display the "appId" and "password" fields. These two are the Application ID and Application Secret fields that are required for GigaVUE-FM to connect to Azure. Copy them.

Now, using the Azure CLI again, do an ‘account show’ command and copy the Subscription ID and the Tenant ID of your subscription.

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

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

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

1. Create a service principal using the Azure CLI: 

   ```
   az ad sp create-for-rbac --name myRealName-app.
   ```

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

   This will return an output similar to:

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

   Note the appId and password from the output.

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

   This will return output similar to:

   ```
   {
   "environmentName": "AzureCloud",
   "id": "6447xxx11-lx11-11lx-11x11xx11ll11",
   "isDefault": true,
   "name": "XYZ Subscription",
   "state": "Enabled",
   "tenantId": "ad46cbb4-441b-4e7d-a40e-c08ff7dedaf0",
   "user": {
   "name": "name@yourcompany.com",
   "type": "user"
   }
   ```
Note the id and tenantId.

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

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

### Custom Roles

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

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

Using CLI:

```bash
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:

```json
{
    "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/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/6447xxx11-1x11-11xx-11x11xx1111/resourceGroups/xxxz-rg",
"/subscriptions/6447xxx11-1x11-11xx-11x11xx1111/resourceGroups/vseries-rg",
"/subscriptions/6447xxx11-1x11-11xx-11x11xx1111/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/publicIPAddresses/read",
  "Microsoft.Network/publicIPAddresses/write",
  "Microsoft.Network/publicIPAddresses/delete",
  "Microsoft.Network/publicIPAddresses/join/action",
  "Microsoft.Resources/subscriptions/locations/read",
]
Add Custom Role to Subscription or Resource Group

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

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

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

![Diagram of Azure console showing resource groups and access control (IAM)]
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/6447xxx11-1x11-1lx-1lx-1lx11xx1111/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/6447xxx11-1x11-1lx-1lx-1lx11xx1111
```

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

Managed Service Identity

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

```
az vm assign-identity -g <Resource group where FM is deployed> -n <GigaVUE-FM name> The above command enables MSI for the GigaVUE-FM for the entire subscription. If more restrictions are needed, use "-scope <resource group id>" as an extension to the command to restrict the MSI permissions for GigaVUE-FM to a resource group.
```

**NOTE:** It may take up to 10 minutes or more for Azure to propagate the permissions. GigaVUE-FM will fail during this time to connect to Azure.
Managed Service Identity (MSI) is only available for GigaVUE Cloud Suite-FM launched inside Azure. You can run these commands in the Azure Portal in a cloud shell (icon in the 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"

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/6447xxx11-1x11-11lx-11xx-11lx11xx1111/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/6447xxx11-1x11-11lx-11xx-11lx11xx1111/resourceGroups/vseries-rg

   az vm identity assign -g xxx-fm-feb15 -n xxx-fm-feb15 --role "FM Custom Role RG Level" --scope /subscriptions/6447xxx11-1x11-11lx-11xx-11lx11xx1111/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/6447xxx11-1x11-11lx-11xx-11lx11xx1111

For more information, refer to **Configure managed identities on VMs** topic in the Microsoft 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 **Configure managed identities on VMs** topic in the Microsoft Azure Documentation.
Accept EULA and Enable Programmatic Deployment in Azure

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

1. **Accept the Gigamon EULAs for each SKU.** These examples show accepting the EULAs from a PowerShell terminal in the Azure Portal:
   
a. **HOURLY FM:**
   
   Azure:
   
   ```
   PS Azure:\> Get-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -Product "gigamon-fm-5_4_00_hourly" -Name "GigaSECURE Cloud 5.4.00 Hourly (100 pack)" | Set-AzureRmMarketplaceTerms -Accept
   ```

   b. **BYOL FM:**
   
   Azure:
   
   ```
   PS Azure:\> Get-AzureRmMarketplaceTerms -Publisher "gigamon-inc" -Product "gigamon-fm-5_4_00" -Name "GigaSECURE Cloud 5.4.00" | Set-AzureRmMarketplaceTerms -Accept
   ```

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

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

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

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

2. **Configure programmatic deployment through the Azure portal so that GigaVUE-FM can launch these images:**
   
a. Find the images in the Azure Marketplace.

   b. Click the "Want to deploy programmatically? Get started" link.

   c. Review the terms of service and the subscription name and then click **Enable**.

**DISCLAIMER:** These are general guidelines for enabling a deployment in Azure. Since the Azure interface is subject to change and is outside Gigamon’s purview, please see Azure documentation for instructions on using Azure.
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 or 2 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.
## Azure Monitoring Domain Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use V Series 2</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring Domain</td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Application ID with Client Secret</td>
</tr>
<tr>
<td>Subscription ID</td>
<td>Subscription ID</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Tenant ID</td>
</tr>
<tr>
<td>Application ID</td>
<td>Application ID</td>
</tr>
<tr>
<td>Application Secret</td>
<td>Application Secret</td>
</tr>
<tr>
<td>Region Name</td>
<td>Region Name</td>
</tr>
<tr>
<td>Traffic Acquisition Method</td>
<td>G-VTAP</td>
</tr>
<tr>
<td>Virtual Networks</td>
<td>Virtual Networks</td>
</tr>
<tr>
<td>Resource Groups</td>
<td>Resource Groups</td>
</tr>
<tr>
<td>Traffic Acquisition Tunnel MTU</td>
<td>1450</td>
</tr>
<tr>
<td>Use Proxy Server</td>
<td>No</td>
</tr>
</tbody>
</table>
3. Enter or select the appropriate information for the monitoring domain as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use V Series 2</td>
<td>Select <strong>Yes</strong> for V Series 2 configuration. Select <strong>No</strong> for V Series 1 configuration.</td>
</tr>
<tr>
<td>Monitoring Domain</td>
<td>An alias used to identify the monitoring domain.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select an authentication type for the connection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Managed Services Identity</strong>: MSI registered with required roles assigned for the resource group in your Azure platform. Refer to <a href="#">Managed Service Identity</a> for detailed information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Application ID with Client Secret</strong>: 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 <a href="#">Application ID with client secret</a> for detailed information.</td>
</tr>
<tr>
<td>Region Name</td>
<td>Azure region for the monitoring domain. For example, West India.</td>
</tr>
<tr>
<td>Traffic Acquisition Method</td>
<td>For <strong>V Series 2</strong> configuration:</td>
</tr>
<tr>
<td></td>
<td>Select a Tapping method. The available options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>G-vTAP</strong>: If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP agents.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tunnel</strong>: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to V Series nodes without deploying G-vTAP agents or G-vTAP controllers.</td>
</tr>
<tr>
<td></td>
<td>For <strong>V Series 1</strong> configuration:</td>
</tr>
<tr>
<td></td>
<td>Select a Tapping method. The available options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>G-vTAP</strong>: If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP agents.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tunnel</strong>: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to V Series nodes without deploying G-vTAP agents or G-vTAP controllers.</td>
</tr>
<tr>
<td>Virtual Networks</td>
<td>Select one or more Virtual Networks (VNETs) required.</td>
</tr>
<tr>
<td>Resource Groups</td>
<td>Select the Resource Groups of the corresponding VMs to monitor.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Traffic Acquisition Tunnel MTU (applicable for V Series 2 solution only)</td>
<td>The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP agent to the GigaVUE Cloud Suite V Series node. For VXLAN, the default value is 1450. The G-vTAP agent tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.</td>
</tr>
</tbody>
</table>
| Use Proxy Server | Select **Yes** to add a proxy server. if GigaVUE-FM is deployed in a private network, proxy server enables communication from GigaVUE-FM to the V Series nodes. 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 more information, refer to Configure Proxy Server. |
| Secure Mirror Traffic (applicable for V Series 1 solution only) | 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

After configuring the Monitoring Domain, you will be navigated to the AWS 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.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Virtual Network</td>
<td>Alias of the centralized VNet in which the G-vTAP Controllers, V Series Proxies, and the GigaVUE V Series nodes are launched.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select Password or SSH Public Key as the Authentication Type to connect with the Centralized VNet.</td>
</tr>
<tr>
<td>NOTE: SSH Public Key</td>
<td>SSH Public Key is the only supported authentication type for V Series 2 solution.</td>
</tr>
<tr>
<td>SSH Public Key</td>
<td>The SSH public key for the GigaVUE fabric nodes.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>The Resource Groups created in Azure for communication between the controllers, nodes, and GigaVUE-FM. This is a required field.</td>
</tr>
<tr>
<td>Security Groups</td>
<td>The security group created for the GigaVUE fabric nodes.</td>
</tr>
</tbody>
</table>

Click Yes to configure V Series Proxy/Controller for the monitoring domain. Refer to [Configure GigaVUE Cloud Suite V Series Proxy/Controller](Configure%20GigaVUE%20Cloud%20Suite%20V%20Series%20Proxy/Controller)

Refer to the following topics for details:

- Configure G-vTAP Controllers
- Configure GigaVUE Cloud Suite V Series Proxy/Controller
- Configure GigaVUE Cloud Suite 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 Cloud Suite V Series nodes.

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

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

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.
<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 multiple versions of G-vTAP Controllers:                                                                                                                                                                                                                                                                                        |
|                        |   a. Under **Controller Versions**, click **Add**.                                                                                                                                                                                                                                                                                      |
|                        |   b. From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP agents installed in the instances.                                                                                                                                                                                                 |
|                        |   c. From the **Size** down-down list, select a size for the G-vTAP Controller. The default size is **Standard_B1s**.                                                                                                                                                                                                                      |
|                        |   d. In **Number of Instances**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1.                                                                                                                                                                                                           |
| 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 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 Cloud Suite V Series Proxy/Controller


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

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

1. In the **Azure Fabric Launch Configuration** page, Select **Yes** to **Configure a V Series Proxy** and the V Series Proxy fields appears.

![V Series Proxy](image)

2. Enter or select the appropriate values for the V Series Proxy. Refer to the **G-vTAP Controller field descriptions** for detailed information.
Configure GigaVUE Cloud Suite 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 Cloud for Azure using the standard VXLAN tunnels.

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

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

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image</strong></td>
<td>From the <strong>Image</strong> drop-down list, select a V Series node image.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>From the <strong>Size</strong> down-down list, select a size for the V Series node. The default size for V Series 2 configuration is <strong>Standard_D4s_v4</strong> and for the V Series 1 configuration is <strong>Standard_DS2_v2</strong>.</td>
</tr>
</tbody>
</table>
| **IP Address Type** | Select one of the following IP address types:  
- Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the V Series node instances and GigaVUE-FM instances in the same network. |
### Fields

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>Public</strong> 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 Minimum Instance.</td>
<td><strong>Management Subnet</strong></td>
</tr>
<tr>
<td><strong>Subnet:</strong> Select a management subnet for V Series node. The subnet that is used for communication between the G-vTAP agents and the V Series nodes, as well as to communicate with GigaVUE-FM. Every fabric node (both controllers and the nodes) need a way to talk to each other and GigaVUE-FM. So they should share at least one management plane/subnet.</td>
<td><strong>Data Subnet(s)</strong></td>
</tr>
<tr>
<td>The subnet that receives the mirrored VXLAN tunnel traffic from the G-vTAP agents. Select a <strong>Subnet</strong> and the respective <strong>Security Groups</strong>. Click <strong>Add</strong> to add additional data subnets.</td>
<td><strong>Tag(s)</strong></td>
</tr>
<tr>
<td>(Optional) The key name and value that helps to identify the V Series node instances in your Azure environment. For example, you might have V Series node deployed in many regions. To distinguish these V Series node based on the regions, you can provide a name that is easy to identify. To add a tag:</td>
<td><strong>Min Instances</strong></td>
</tr>
<tr>
<td>a. Click <strong>Add</strong>.</td>
<td>The minimum number of GigaVUE Cloud Suite V Series nodes to be launched in the Azure connection. The minimum number of instances that can be entered is 1.</td>
</tr>
<tr>
<td>b. In the <strong>Key</strong> field, enter the key. For example, enter Name.</td>
<td><strong>Max Instances</strong></td>
</tr>
<tr>
<td>c. In the <strong>Value</strong> field, enter the key value.</td>
<td>The maximum number of GigaVUE Cloud Suite V Series nodes that can be launched in the Azure connection. When the number of instances per V Series node exceeds the max instances specified in this field, increase the number in the Max Instances to Launch. When additional V Series nodes are launched, GigaVUE-FM rebalances the instances assigned to the nodes. This can result in a brief interruption of traffic.</td>
</tr>
</tbody>
</table>

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 in the **Monitoring Domain** page.
Configure and Manage Resources using V Series 2

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

Refer to the following sections for details:

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

Create a Monitoring Session

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

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

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

- In G-vTAP connections, Tool VM instances (Source and Destination IP) must be excluded using Exclusion Map.
- You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:
1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.

2. Click **New** to open the **Create a New Monitoring Session** page.

   **Create A New Monitoring Session**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The name of the monitoring session.</td>
</tr>
<tr>
<td>Monitoring Domain</td>
<td>The name of the monitoring domain that you want to select.</td>
</tr>
<tr>
<td>Connection</td>
<td>The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain.</td>
</tr>
</tbody>
</table>

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

4. Click **Create**. The Monitoring Session details page appears with the new monitoring session.

   If multiple projects had been selected in the connections page, the topology view will show instances in all of the selected projects.

### Create Ingress and Egress Tunnels

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The name of the tunnel endpoint.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the tunnel endpoint.</td>
</tr>
<tr>
<td>Type</td>
<td>VXLAN is the only supported tunnel type for Azure.</td>
</tr>
<tr>
<td>Traffic</td>
<td>The direction of the traffic flowing through the V Series node.</td>
</tr>
</tbody>
</table>
| Direction     | • Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node. Enter values for the Key.  
• Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. Select or enter values for MTU, Time to Live, DSCP, PREC, Flow Label, and Key. |
| Remote Tunnel IP | • For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source.  
• For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint. |

4. Click **Save**.

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

**Create a New Map**

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

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

To create a new map:
1. After creating a new monitoring session, or click **Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.

2. In the canvas, select **New > New Map**, drag and drop a new map template to the workspace. The New Map quick view appears.
3. On the New Map quick view, enter or select the required information as described in the following table.

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

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

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

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

5. Click **Save**.

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

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

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

- Slicing
- Masking
- Dedup
- Load Balancing
- PCAPng

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

- Application Metadata Intelligence
- Application Filtering Intelligence

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

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

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

To add a GigaSMART application:

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

**Slicing**

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

To add a slicing application:
1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.

2. Click the Slicing application and select **Details**. The Application quick view appears.

   ![Application Quick View]

   - **Application**: Slicing
   - **Alias**: slicing
   - **Protocol**: none
   - **Offset**: 
   - **Enhanced Name**: 

   ![Screenshot of Application Quick View]

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

4. Click **Save**.

**Masking**

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

To add a masking application:
1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.

2. Click the Masking application and select **Details**. The Application quick view appears.

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

4. Click **Save**.

**Dedup**

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

To add a de-duplication application:
1. Drag and drop Dedup from APPLICATIONS to the graphical workspace.
2. Click the Dedup application and select Details. The Application quick view appears.

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

Load Balancing

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

To add a load balancing application:
1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.

2. Click the load balancing application and select **Details**. The Application quick view appears.

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

   **NOTE:** Field location is not supported for **gtpuTeid**.

   - In the **load balancing groups**, add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

4. Click **Save**.

**PCAPng**

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

**NOTE:** The PCAPng application is only applicable for the Ericsson 5G Core vTAP architecture. Refer to **Ericsson 5G Core vTAP** for detailed information.

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

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:
1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.

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

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

3. Click **Save**.

4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.

5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

**Create Link Between PCAPng Application and Other Destinations**

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

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

Refer to the following image for a sample configuration.
Deploy Monitoring Session

To deploy the monitoring session:

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

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

3. (Not applicable for Tunnel traffic acquisition method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.

4. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all the V Series nodes. Click on the status link in the Status column on the Monitoring Session page to view the Monitoring Session Deployment Report. When you click on the Status link, the Deployment Report is displayed. If the monitoring session is not deployed properly, then one of the following errors is displayed in the Status column.
   - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.

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

The Monitoring Session page also has the following buttons:

- **Undeploy**—Undeploys the selected monitoring session.
- **Clone**—Duplicates the selected monitoring session.
- **Edit**—Opens the Edit page for the selected monitoring session.
- **Delete**—Deletes the selected monitoring session.

**View Monitoring Session Statistics**

The Monitoring Session Statistics page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. The traffic can be viewed based on kilobits/second, megabits/second or gigabits/second.
On the Monitoring Sessions page, click View in the Statistics column to view the Monitoring Session Statistics page. The Monitoring Session Statistics page appears where you can analyze incoming and outgoing traffic.

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

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

- Directly below the graph, you can click on **IncomingMbps**, **Outgoing Mbps**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.
- At the bottom of the Monitoring Session Statistics page, you can click on **View Monitoring Session Diagram**. The Monitoring Session Diagram quick view appears.
- On the Monitoring Session Diagram page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map Info for this map. You can select Map Rules or Action Sets to view the traffic matching the selected rule on the graph in the quick view.

**Visualize the Network Topology**

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

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

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

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitoring instances.
- Use the arrows at the right-bottom corner to move the topology page up, down, left, or right. Click the **Fit-to-Width** icon to fit the topology diagram according to the width of the page.
- Use + or - icons to zoom in and zoom out the topology view.
Configure and Manage Resources using V Series 1

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

Refer to the following sections for details:

- Create 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The name of the monitoring session.</td>
</tr>
<tr>
<td>Monitoring Domain</td>
<td>The name of the monitoring domain.</td>
</tr>
<tr>
<td>Connection</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. Click Create.

Create Tunnel Endpoints

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

To create 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.

![Add Tunnel Spec](image)

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

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

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>L2, L3, and L4 Filters</strong></td>
<td><strong>EtherType</strong></td>
</tr>
<tr>
<td></td>
<td>The packets are filtered based on the selected ethtype. The following conditions are displayed:</td>
</tr>
<tr>
<td></td>
<td>■ IPv4</td>
</tr>
<tr>
<td></td>
<td>■ IPv6</td>
</tr>
<tr>
<td></td>
<td>■ ARP</td>
</tr>
<tr>
<td></td>
<td>■ RARP</td>
</tr>
<tr>
<td></td>
<td>■ Other</td>
</tr>
<tr>
<td><strong>L3 Filters</strong></td>
<td>If you choose IPv4 or IPv6, the following L3 filter conditions are displayed:</td>
</tr>
<tr>
<td></td>
<td>■ Protocol</td>
</tr>
<tr>
<td></td>
<td>■ IP Fragmentation</td>
</tr>
<tr>
<td></td>
<td>■ IP Time to live (TTL)</td>
</tr>
<tr>
<td></td>
<td>■ IP Type of Service (TOS)</td>
</tr>
<tr>
<td></td>
<td>■ IP Explicit Congestion Notification (ECN)</td>
</tr>
<tr>
<td></td>
<td>■ IP Source</td>
</tr>
<tr>
<td></td>
<td>■ IP Destination</td>
</tr>
<tr>
<td><strong>L4 Filters</strong></td>
<td>If you select TCP or UDP protocol, the following L4 filter conditions are displayed:</td>
</tr>
<tr>
<td></td>
<td>■ Port Source</td>
</tr>
<tr>
<td></td>
<td>■ Port Destination</td>
</tr>
<tr>
<td><strong>MAC Source</strong></td>
<td>The egress traffic from the instances or ENIs matching the specified source MAC address is selected.</td>
</tr>
<tr>
<td><strong>MAC Destination</strong></td>
<td>The ingress traffic from the instances or ENIs matching the specified destination MAC address is selected.</td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td>All the traffic matching the specified IEEE 802.1q Virtual LAN tag is filtered. Specify a number from 0 to 4094.</td>
</tr>
<tr>
<td><strong>VLAN Priority Code Point (PCP)</strong></td>
<td>All the traffic matching the specified IEEE 802.1q Priority Code Point (PCP) is filtered. Specify a value between 0 to 7.</td>
</tr>
<tr>
<td><strong>VLAN Tag Control Information (TCI)</strong></td>
<td>All the traffic matching the specified VLAN TCI value is filtered. Specify the exact TCI value.</td>
</tr>
<tr>
<td><strong>Pass All</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The name of the new map.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The name can contain alphanumeric characters with no spaces.</td>
</tr>
<tr>
<td>Comments</td>
<td>The description of the map.</td>
</tr>
</tbody>
</table>
### Map Rules

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map Rules</td>
<td>The rules for filtering the traffic in the map.</td>
</tr>
<tr>
<td></td>
<td>To add a map rule:</td>
</tr>
<tr>
<td></td>
<td>a. Click <a href="#">Add a Rule</a>.</td>
</tr>
<tr>
<td></td>
<td>b. Select a condition from the <a href="#">Search L2 Conditions</a> drop-down list</td>
</tr>
<tr>
<td></td>
<td>and specify a value. Based on this selection, the Search L3 Conditions</td>
</tr>
<tr>
<td></td>
<td>drop-down list is automatically updated.</td>
</tr>
<tr>
<td></td>
<td>c. Select a condition from the <a href="#">Search L3 Conditions</a> drop-down list</td>
</tr>
<tr>
<td></td>
<td>and specify a value.</td>
</tr>
<tr>
<td></td>
<td>d. (Optional) If you have selected TCP or UDP as the protocol in the L3</td>
</tr>
<tr>
<td></td>
<td>conditions, then select Port Source or Port Destination from the Search</td>
</tr>
<tr>
<td></td>
<td>L4 Conditions drop-down list and specify a value. If you have selected</td>
</tr>
<tr>
<td></td>
<td>conditions other than TCP or UDP, then the Search L4 Conditions drop-down</td>
</tr>
<tr>
<td></td>
<td>list is disabled.</td>
</tr>
<tr>
<td></td>
<td>e. (Optional) In the Priority and Action Set box, assign a priority and</td>
</tr>
<tr>
<td></td>
<td>action set.</td>
</tr>
<tr>
<td></td>
<td>f. (Optional) In the Rule Comment box, enter a comment for the rule.</td>
</tr>
</tbody>
</table>

**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 V Series Nodes.

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

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

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

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

Agent Pre-filtering 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 V Series Nodes. Consequently, traffic flow to the V Series Nodes is reduced, which reduces the load/cost on the Cloud networks.
- Only rules from first-level maps are pushed to the agents.
- Pass rules are supported 100%.
- Drop rules are supported for only simple cases or single-drop rules with a pass all case.
- Rules that span all monitoring sessions will be merged for an G-vTAP agent, if applicable.
- If the max-rule limit of 16 is reached, then all the traffic is passed to the V Series node; no filtering will be performed.

Enable/Disable G-vTAP Agent Pre-filtering

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

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

1. 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 the On check box to determine that the application is slicing packets. Select the Off check box to determine that the application is not currently slicing the packets. The state can be changed at a later time whenever required.
5. In the Slice Length field, specify the length of the packet that must be sliced.
6. From the Protocol drop-down list, specify an optional parameter for slicing the specified length of the protocol. The options are as follows:
   - None
   - IPv4
   - IPv6
   - UDP
   - TCP
7. Click Save.
Masking

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

To add a masking application:

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

2. Click the Mask application and select Details.

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

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

5. In the Mask offset field, enter the offset from which the application should start masking data following the pattern specified in the Pattern field. The value can be specified in terms of either a static offset, that is, from the start of the packet or a relative offset, that is, from a particular protocol layer as specified in the Protocol field.

6. In the Mask length field, enter the length of the packet that must be masked.

7. In the Mask pattern field, enter the pattern for masking the packet. The value of the pattern is from 0 to 255.

8. From the Protocol drop-down list, specifies an optional parameter for masking packets on the data coming from the selected protocol.

9. Click Save.
NetFlow

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

The following are the key benefits of NetFlow application:

- Compresses network information into a single flow record.
- Facilitates up to 99% reduction in data transferred.
- Accelerates the migration of mission-critical workloads to 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 Cloud Suite V Series node in the monitoring session.
The NetFlow record generation is performed on GigaVUE Cloud Suite V Series node running the NetFlow application. In Add Applications to Monitoring Session, incoming packets from G-vTAP agents are sent to the GigaVUE Cloud Suite V Series node. In the GigaVUE V Series node, one map sends the TCP packet to the version 5 NetFlow application. Another map sends the UDP packet to a sampling application. The map rules and applications such as slice, mask, and sample can only be applied prior to sending the data to NetFlow.

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

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

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

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

**Match/Key Fields**

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

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Supported NetFlow Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Link</strong></td>
<td></td>
</tr>
<tr>
<td>Destination MAC</td>
<td>Configures the destination MAC address as a key field.</td>
</tr>
<tr>
<td>Egress Dest MAC</td>
<td>Configures the post Source MAC address as a key field.</td>
</tr>
<tr>
<td>Ingress Dest MAC</td>
<td>Configures the IEEE 802 destination MAC address as a key field.</td>
</tr>
<tr>
<td>Source MAC</td>
<td>Configures the IEEE 802 source MAC address as a key field.</td>
</tr>
<tr>
<td><strong>IPv4</strong></td>
<td></td>
</tr>
<tr>
<td>ICMP Type Code</td>
<td>Configures the type and code of the IPv4 ICMP</td>
</tr>
<tr>
<td>Description</td>
<td>Supported NetFlow Versions</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>IPv4 Dest IP</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IPv4 ICMP Code</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv4 ICMP Type</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv4 Options</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv4 Src IP</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IPv4 Total Length</td>
<td>IPFIX</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
</tr>
<tr>
<td>IP CoS</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IP DSCP</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IP Header Length</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IP Precedence</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IP Protocol</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IP Total Length</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IP TTL</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IP Version</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td></td>
</tr>
<tr>
<td>IPv6 Dest IP</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IPv6 Flow Label</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IPv6 ICMP Code</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv6 ICMP Type</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 ICMP Type Code</td>
<td>Configures the type and code of the IPv6 ICMP message as a key field.</td>
</tr>
<tr>
<td>IPv6 Payload Length</td>
<td>Configures the value of the payload length field in the IPv6 header as a key field.</td>
</tr>
<tr>
<td>IPv6 Src IP</td>
<td>Configures the IPv6 source address in the IP packet header as a key field.</td>
</tr>
<tr>
<td>Transport</td>
<td></td>
</tr>
<tr>
<td>L4 Dest Port</td>
<td>Configures the destination port identifier in the transport header as a key field.</td>
</tr>
<tr>
<td>L4 Src Port</td>
<td>Configures the source port identifier in the transport header as a key field.</td>
</tr>
<tr>
<td>TCP AcK Number</td>
<td>Configures the acknowledgment number in the TCP header as a key field.</td>
</tr>
<tr>
<td>TCP Dest Port</td>
<td>Configures the destination port identifier in the TCP header as a key field.</td>
</tr>
<tr>
<td>TCP Flags</td>
<td>Configures the TCP control bits observed for the packets of this flow as a key field.</td>
</tr>
<tr>
<td>TCP Header Length</td>
<td>Configures the length of the TCP header as a key field.</td>
</tr>
<tr>
<td>TCP Seq Number</td>
<td>Configures the sequence number in the TCP header as a key field.</td>
</tr>
<tr>
<td>TCP Src Port</td>
<td>Configures the source port identifier in the TCP header as a key field.</td>
</tr>
<tr>
<td>TCP Urgent</td>
<td>Configures the urgent pointer in the TCP header as a key field.</td>
</tr>
<tr>
<td>TCP Window Size</td>
<td>Configures the window field in the TCP header as a key field.</td>
</tr>
<tr>
<td>UDP Dest Port</td>
<td>Configures the destination port identifier in the UDP header as a key field.</td>
</tr>
<tr>
<td>UDP Src Port</td>
<td>Configures the source port identifier in the TCP header as a key field.</td>
</tr>
</tbody>
</table>

**Collect/Non-Key Fields**

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

The supported Collect/Non-Key elements are outlined in the following table:
<table>
<thead>
<tr>
<th>Description</th>
<th>Supported NetFlow Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Counter</strong></td>
<td></td>
</tr>
<tr>
<td>Byte Count</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>Packet Count</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td><strong>Data Link</strong></td>
<td></td>
</tr>
<tr>
<td>Destination MAC</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>Egress Des MAC</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Ingress Des MAC</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Source MAC</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td><strong>Timestamp</strong></td>
<td></td>
</tr>
<tr>
<td>Flow End Millisec</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Flow End Sec</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Flow End Time</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>Flow Start Millisec</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Flow Start Sec</td>
<td>IPFIX</td>
</tr>
<tr>
<td>Flow Startup Time</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td><strong>Flow</strong></td>
<td></td>
</tr>
<tr>
<td>Flow End Reason</td>
<td>IPFIX</td>
</tr>
<tr>
<td><strong>IPv4</strong></td>
<td></td>
</tr>
<tr>
<td>ICMP Type Code</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IPv4 Dest IP</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td>IPv4 ICMP Code</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv4 ICMP Type</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv4 Options</td>
<td>IPFIX</td>
</tr>
<tr>
<td>IPv4 Src IP</td>
<td>v9 and IPFIX</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv4 Total Length</td>
<td>Configures the total length of the IPv4 packet as a non-key field.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
</tr>
<tr>
<td>IP CoS</td>
<td>Configures the IP Class Of Service (CoS) as a key field.</td>
</tr>
<tr>
<td>IP Protocol</td>
<td>Configures the value of the protocol number in the IP packet header as a key field.</td>
</tr>
<tr>
<td>IP Version</td>
<td>Configures the IP version field in the IP packet header as a key field.</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td></td>
</tr>
<tr>
<td>IPv6 Dest IP</td>
<td>Configures the IPv6 destination address in the IP packet header as a key field.</td>
</tr>
<tr>
<td>IPv6 Flow Label</td>
<td>Configures the value of the IPv6 flow label field in the IP packet header as a key field.</td>
</tr>
<tr>
<td>IPv6 Src IP</td>
<td>Configures the IPv6 source address in the IP packet header as a key field.</td>
</tr>
<tr>
<td><strong>Transport</strong></td>
<td></td>
</tr>
<tr>
<td>L4 Dest Port</td>
<td>Configures the destination port identifier in the transport header as a non-key field.</td>
</tr>
<tr>
<td>L4 Src Port</td>
<td>Configures the source port identifier in the transport header as a non-key field.</td>
</tr>
<tr>
<td>TCP AcK Number</td>
<td>Configures the acknowledgment number in the TCP header as a non-key field.</td>
</tr>
<tr>
<td>TCP Dest Port</td>
<td>Configures the destination port identifier in the TCP header as a non-key field.</td>
</tr>
<tr>
<td>TCP Flags</td>
<td>Configures the TCP control bits observed for the packets of this flow as a non-key field.</td>
</tr>
<tr>
<td>TCP Header Length</td>
<td>Configures the length of the TCP header as a non-key field.</td>
</tr>
<tr>
<td>TCP Seq Number</td>
<td>Configures the sequence number in the TCP header as a non-key field.</td>
</tr>
<tr>
<td>TCP Src Port</td>
<td>Configures the source port identifier in the TCP header as a non-key field.</td>
</tr>
<tr>
<td>TCP Urgent</td>
<td>Configures the urgent pointer in the TCP header as a non-key field.</td>
</tr>
<tr>
<td>TCP Window Size</td>
<td>Configures the window field in the TCP header as a non-key field.</td>
</tr>
<tr>
<td>UDP Dest Port</td>
<td>Configures the destination port identifier in the UDP header as a non-key field.</td>
</tr>
<tr>
<td>UDP Src Port</td>
<td>Configures the source port identifier in the UDP header as a non-key field.</td>
</tr>
</tbody>
</table>
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.

![Diagram showing NetFlow drag and drop](image)

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

![Diagram showing NetFlow details](image)

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 Cloud Suite V Series nodes. Refer **Example 1** below.

**Example 1**

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

1. Create a monitoring session.

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

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

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

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

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

8. Click Deploy to deploy the monitoring session.

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

If the monitoring session is not deployed properly, then one of the following errors is displayed:

- Partial Success—The session is not deployed on one or more instances due to G-vTAP or GigaVUE Cloud Suite V Series node failure.
- Failure—The session is not deployed on any of the GigaVUE Cloud Suite V Series nodes and G-vTAP agents.

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

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

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Source</td>
<td>Modify the Ethernet source address.</td>
</tr>
<tr>
<td>MAC Destination</td>
<td>Modify the Ethernet destination address.</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>Specify the VLAN ID.</td>
</tr>
<tr>
<td>VLAN PCP</td>
<td>Specify the VLAN priority.</td>
</tr>
<tr>
<td>Strip VLAN</td>
<td>Strip the VLAN tag.</td>
</tr>
<tr>
<td>IPv4 Source</td>
<td>Specify the IPv4 source address.</td>
</tr>
<tr>
<td>IPv4 Destination</td>
<td>Specify the IPv4 destination address.</td>
</tr>
<tr>
<td>ToS</td>
<td>Specify the DSCP bits in IPv4 traffic class.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Specify the UDP, TCP, or SCTP source port.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specify the UDP, TCP, or SCTP destination port.</td>
</tr>
<tr>
<td>Tunnel ID</td>
<td>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.</td>
</tr>
</tbody>
</table>

To add a header transformation:
1. On the Monitoring Session, click the link and select **Details**. The Link quick view is displayed.

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

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

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

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

### View Monitoring Session Statistics

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

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 **Incoming Mbps**, **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.
Administer GigaVUE Cloud Suite for Azure

You can perform the following administrative tasks:

- Set Up Email Notifications
- Configure Proxy Server
- Configure Azure Settings
- Manager User Roles and Permissions
- 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*.

![Configure Email Server](image)

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The name of the proxy server.</td>
</tr>
<tr>
<td>Host</td>
<td>The host name or the IP address of the proxy server.</td>
</tr>
<tr>
<td>Host IP Address Type</td>
<td>The type of the Host IP address that indicate whether the proxy server IP address is private or public to the VNet.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the proxy server for connecting to the Internet.</td>
</tr>
<tr>
<td>Username</td>
<td>(Optional) The username of the proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password of the proxy server.</td>
</tr>
<tr>
<td>NTLM</td>
<td>(Optional) The type of the proxy server used to connect to the VNet.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain name of the client accessing the proxy server.</td>
</tr>
<tr>
<td>Workstation</td>
<td>(Optional) The name of the workstation or the computer accessing the proxy server.</td>
</tr>
</tbody>
</table>

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. Refer to **Create Monitoring Domain**.

## 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:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of connections allowed</td>
<td>Specifies the maximum number of VNet connections you can establish in GigaVUE-FM.</td>
</tr>
<tr>
<td>Refresh interval for VM target selection inventory (secs)</td>
<td>Specifies the frequency for updating the state of Virtual Machines target selection in Azure.</td>
</tr>
<tr>
<td>Refresh interval for fabric deployment inventory (secs)</td>
<td>Specifies the frequency for updating the state of fabric deployment information such as subnets, security groups, images, and VNets.</td>
</tr>
</tbody>
</table>
## 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.

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

<table>
<thead>
<tr>
<th>Controls/Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

### All Audit Logs

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

**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.

### GigaVUE-FM Version Compatibility for V Series 2 Configuration

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.13.00</td>
<td>v1.8-2</td>
<td>v1.8-2</td>
<td>v2.3.0</td>
<td>v2.3.0</td>
</tr>
</tbody>
</table>

### GigaVUE-FM Version Compatibility for V Series 1 Configuration

<table>
<thead>
<tr>
<th>GigaVUE-FM</th>
<th>G-vTAP Agent Version</th>
<th>G-vTAP Controller Version</th>
<th>GigaVUE V Series Controller</th>
<th>GigaVUE V Series 1 Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.10.01, 5.11.00, 5.11.01, 5.12.00, 5.13.00</td>
<td>v1.7-1</td>
<td>v1.7-1</td>
<td>v1.7-1</td>
<td>v1.7-1</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>GigaVUE Cloud Suite 5.13 Hardware and Software Guides</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DID YOU KNOW?</strong> 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 &gt; Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</td>
</tr>
<tr>
<td>Hardware</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>*G-TAP A Series 2 Installation Guide</td>
</tr>
<tr>
<td>GigaVUE-HC1 Hardware Installation Guide</td>
</tr>
<tr>
<td>GigaVUE-HC2 Hardware Installation Guide</td>
</tr>
<tr>
<td>GigaVUE-HC3 Hardware Installation Guide</td>
</tr>
<tr>
<td>GigaVUE M Series Hardware Installation Guide</td>
</tr>
<tr>
<td>GigaVUE TA Series Hardware Installation Guide</td>
</tr>
<tr>
<td>*GigaVUE-OS Installation Guide for DELL S4112F-ON</td>
</tr>
<tr>
<td>Software Installation and Upgrade Guides</td>
</tr>
<tr>
<td>GigaVUE-FM Installation, Migration, and Upgrade Guide</td>
</tr>
<tr>
<td>GigaVUE-OS Upgrade Guide</td>
</tr>
</tbody>
</table>
## GigaVUE Cloud Suite 5.13 Hardware and Software Guides

### Administration

**GigaVUE Administration Guide**
- covers both GigaVUE-OS and GigaVUE-FM

### Fabric Management

**GigaVUE Fabric Management Guide**
- how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features

### Cloud Configuration and Monitoring

how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms

**GigaVUE Cloud Suite for AnyCloud Guide**
- how to deploy the GigaVUE Cloud Suite solution in any cloud platform

**GigaVUE Cloud Suite for AWS Guide**

**GigaVUE Cloud Suite for AWS Quick Start Guide**
- quick view of AWS deployment

**GigaVUE Cloud Suite for AWS SecretRegions Guide**

**GigaVUE Cloud Suite for Azure Guide**

**GigaVUE Cloud Suite for Kubernetes Guide**

**GigaVUE Cloud Suite for Nutanix Guide**

**GigaVUE Cloud Suite for OpenStack Guide**

**GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide**

**GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide**

**GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide**

### Reference

**GigaVUE-OS CLI Reference Guide**
- library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices

**GigaVUE-OS Cabling Quick Reference Guide**
- guidelines for the different types of cables used to connect Gigamon devices

**GigaVUE-OS Compatibility and Interoperability Matrix**
- compatibility information and interoperability requirements for Gigamon devices

- samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
GigaVUE Cloud Suite 5.13 Hardware and Software Guides

Release Notes

new features, resolved issues, and known issues in this release;
important notes regarding installing and upgrading to this release

**NOTE:** Release Notes are not included in the online documentation.

**NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.

In-Product Help

GigaVUE-FM Online Help
how to install, deploy, and operate GigaVUE-FM.

GigaVUE-OS H-VUE Online Help
provides links the online documentation.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Additional Sources of Information
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.

<table>
<thead>
<tr>
<th>Documentation Feedback Form</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>About You</strong></td>
</tr>
<tr>
<td>Your Name</td>
</tr>
<tr>
<td>Your Role</td>
</tr>
<tr>
<td>Your Company</td>
</tr>
<tr>
<td><strong>For Online Topics</strong></td>
</tr>
<tr>
<td>Online doc link</td>
</tr>
<tr>
<td>Topic Heading</td>
</tr>
<tr>
<td><strong>For PDF Topics</strong></td>
</tr>
<tr>
<td>Document Title</td>
</tr>
<tr>
<td>Product Version</td>
</tr>
<tr>
<td>Document Version</td>
</tr>
<tr>
<td>Chapter Heading</td>
</tr>
<tr>
<td>PDF page #</td>
</tr>
<tr>
<td><strong>How can we improve?</strong></td>
</tr>
<tr>
<td>Describe the issue</td>
</tr>
<tr>
<td>How can we improve the content?</td>
</tr>
<tr>
<td>Be as specific as possible.</td>
</tr>
<tr>
<td>Any other comments?</td>
</tr>
</tbody>
</table>
Contact Technical Support

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

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

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

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