GigaVUE Cloud Suite for Third Party Orchestration

GigaVUE Cloud Suite

Product Version: 6.1

Document Version: 1.0

(See Change Notes for document updates.)

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

Change Notes

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

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

Contents

GigaVUE Cloud Suite for Third Party Orchestration

This guide describes how to deploy the GigaVUE Cloud Suite in any of the cloud platforms available in the market.

Topics:

Overview of Third Party Orchestration

The GigaVUE Cloud Suite for third party Orchestration consists of the following components:

- GigaVUE® Fabric Manager (GigaVUE-FM)
- G-vTAP Agents
- G-vTAP Controllers
- GigaVUE V Series Proxy
- GigaVUE V Series Nodes

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

In the third-party orchestration deployment option, you are responsible for the following:

- Installing and launching GigaVUE-FM from the supported cloud or enterprise platform.
- Launching the fabric components in your platform.
- Sharing the IP addresses and subnet CIDR of the fabric components with GigaVUE-FM.

The images of the components are available in the Gigamon Customer Portal.

NOTE: Contact Gigamon Technical Support team if the existing Gigamon images for a specific cloud platform is not compatible.

GigaVUE-FM uses the IP addresses of the fabric components to:

- Identify the traffic
- Monitor the traffic flow
- Forward the traffic to the destination

NOTE: You are responsible for deleting the fabric nodes from the platform when visibility for the platform is no longer required.

For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation and Upgrade Guide*.

Components for Third Party Orchestration

The following table provides a brief description of the components that can be deployed using the third-party orchestration:

Component	Description
GigaVUE® Fabric Manager (GigaVUE-FM)	GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud. You are responsible for launching GigaVUE-FM from your end on the supported cloud or enterprise platforms.
G-vTAP Agent	G-vTAP Agent is an agent that is installed in your Virtual Machine (VM). This agent mirrors the selected traffic from the VMs to the GigaVUE® V Series node. The G-vTAP Agent is offered as a Debian (.deb), Redhat Package Manager (.rpm) or windows package. Refer to Install G-vTAP Agents.
G-vTAP Controller	G-vTAP Controller manages multiple G-vTAP Agents and orchestrates the flow of mirrored traffic to GigaVUE V Series nodes. GigaVUE-FM uses one or more G-vTAP Controllers to communicate with the G-vTAP Agents.
GigaVUE® V Series Proxy	GigaVUE® V Series Proxy manages multiple V Series nodes and orchestrates the flow of traffic from GigaVUE V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.
GigaVUE® V Series 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 using GRE or VXLAN tunnels, provided the cloud platform supports

Get Started with Third Party Orchestration

This chapter describes how to plan and start the third party orchestration deployment.

Refer to the following sections for details:

- License information
- Network Firewall Requirement

License information

GigaVUE Cloud Suite for third-party orchestration supports Volume-Based Licensing model. Refer to the following topics for more detailed information on Volume-Based Licensing and how to activate your license:

- Volume-Based License
- Apply License

Volume-Based License

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

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

Base Bundles

GigaVUE-FM has the following three base bundles:

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

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

Bundle Replacement Policy

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

Add-on Packages

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

Rules for add-on packages:

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

The list of the available add-on SKUs are:

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

How GigaVUE-FM Tracks Volume-Based License Usage

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

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point.

- When a license goes into grace period, you will be notified, along with a list of monitoring sessions that would be affected after the expiry of the grace period.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will be undeployed, but not deleted from the database.
- When a license is renewed or newly imported, the undeployed monitoring sessions will be redeployed.

Manage Volume-Based License

To manage active Volume-Based License:

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

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

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

Use the following buttons to manage your active VBL.

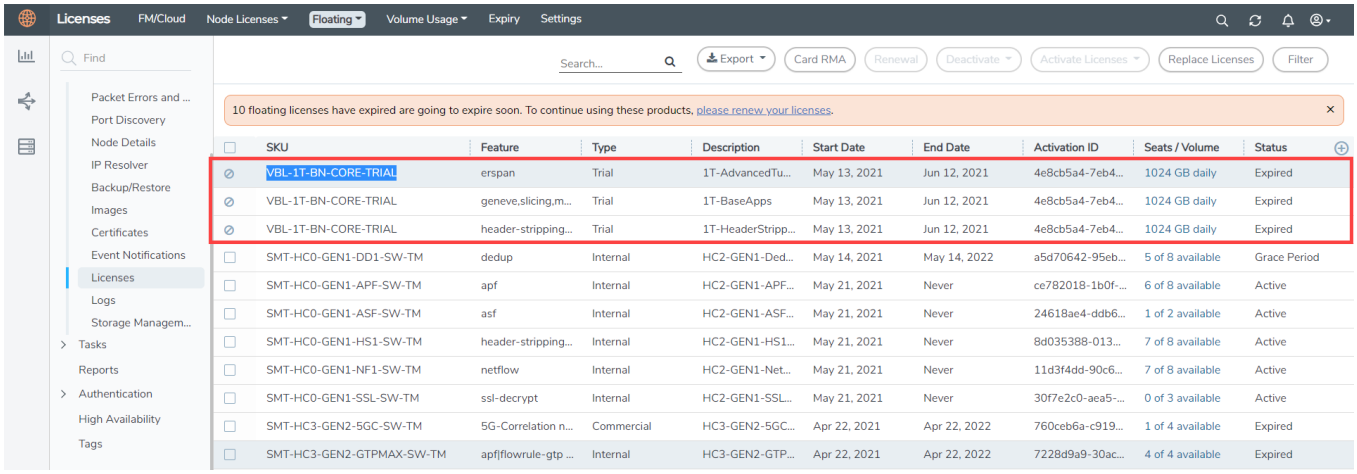
Button	Description
Activate Licenses	Use this button to activate a Volume-Based License. Refer Activate Licenses for more information.
Email Volume Usage	Use this button to send the volume usage details to the email recipients.
Filter	Use this option to narrow down the list of active Volume-Based Licenses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

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

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

Default Trial Licenses

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



This license includes the following applications:

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

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

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

Apply License

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

Network Firewall Requirement

Following is the Network Firewall Requirements for V Series 2 node deployment.

Direction	Type	Protocol	Port	CIDR	Purpose
GigaVUE-FM					
Inbound	• HTTPS • SSH	TCP	• 443 • 22	Administrator Subnet	Management connection to GigaVUE-FM
Inbound	Custom TCP Rule	TCP	5671	V Series 2 Node IP	Allows GigaVUE V Series 2 Nodes to send traffic health updates to GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series node
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP(6)	9900	GigaVUE-FM IP	Allows G-vTAP Controller to communicate with GigaVUE-FM
Outbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Controller to communicate with G-vTAP Agents
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP(6)	9901	G-vTAP Controller IP	Allows G-vTAP Agents to communicate with G-vTAP Controller
Outbound	• UDP • IP	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
V Series Proxy (optional)					

Direction	Type	Protocol	Port	CIDR	Purpose
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	V Series 2 node IP	Allows V Series Proxy to communicate with V Series node
V Series 2 node					
Inbound	Custom TCP Rule	TCP	8889	• GigaVUE-FM IP • V Series Proxy IP	Allows V Series Proxy or GigaVUE-FM to communicate with V Series node
Inbound	• UDP • IP	• UDP (VXLAN) • IP Protocol (L2GRE)	• VXLAN (default 4789) • L2GRE	G-vTAP Agent or Subnet IP	Allows G-vTAP Agents to (VXLAN/L2GRE) tunnel traffic to V Series nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE Tunnel to communicate and tunnel traffic to V Series nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Outbound	Custom UDP Rule	• UDP (VXLAN) • IP Protocol (L2GRE)	VXLAN (default 4789)	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound (optional)	ICMP	ICMP	• echo request • echo reply	Tool IP	Allows V Series node to health check tunnel destination traffic

Deploy GigaVUE Cloud Suite for Third Party Orchestration

You can use your own orchestration system to deploy the GigaVUE fabric components instead of using GigaVUE-FM to deploy your fabric components.

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

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

This chapter describes how to connect, launch, and deploy the fabric components of GigaVUE Cloud Suite using third party orchestration. Refer to the following sections for more detailed information:

- Install GigaVUE-FM
- Prepare G-vTAP Agent to Monitor Traffic
- Create Monitoring Domain
- Modes of Deployments
- Deploy Fabric Components using Generic Mode
- Deploy Fabric Components using Integrated Mode

Install GigaVUE-FM

The GigaVUE-FM software package is available in multiple formats such as OVA, QCOW2, ISO. Use the appropriate media format to deploy GigaVUE-FM.

After you deploy GigaVUE-FM you must perform an initial configuration before you start using GigaVUE-FM. Refer to the *GigaVUE-FM Installation and Upgrade Guide* for details.

To install GigaVUE-FM in your cloud environment refer to *GigaVUE-FM Installation and Upgrade Guide* for details.

Prepare G-vTAP Agent to Monitor Traffic

A G-vTAP Agent is the primary Gigamon monitoring module that is installed in your Virtual Machines (VMs). G-vTAP mirrors the selected traffic from a source interface to a destination mirror interface. The mirrored traffic is encapsulated using GRE or VXLAN tunneling and then sent to the GigaVUE Cloud Suite® V Series node.

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

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

A source interface can be configured with one or more ENIs. While configuring a source interface, you can specify the direction of the traffic to be monitored in the instance. The direction of the traffic can be egress or ingress or both.

NOTE: For environments with both Windows and Linux agents or just windows agents, VXLAN tunnels in the G-vTAP controller specification is required.

Refer to the following sections for more information:

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

Linux G-vTAP Agent Installation

Refer to the following sections for the Linux agent installation:

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

Single ENI Configuration

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

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

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

Dual ENI Configuration

A G-vTAP Agent lets you configure two ENIs. One ENI can be configured as the source interface and another ENI can be configured as the destination interface.

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

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent**`6.1.00`** MSI package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
2. Install the downloaded MSI package as **Administrator** and the G-vTAP Agent service starts automatically.

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

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

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

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

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

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

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

4. Save the file.

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

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

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

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

Windows G-vTAP Agent Installation Using ZIP Package

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

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

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

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

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

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

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

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

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

5. Save the file.

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

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

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

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

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

Install G-vTAP Agents

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

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

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

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

Refer to the following topics for details:

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

Install G-vTAP from Ubuntu/Debian Package

To install from a Debian package:

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

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

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

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

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

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

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

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

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

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

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

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

6. Reboot the instance.

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

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

Install G-vTAP from RPM package

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

1. Run the following command:
   ```
   sudo yum install python3
   sudo pip3 install urllib3
   sudo pip3 install requests
   sudo pip3 install netifaces
   ```
2. Download the G-vTAP Agent **6.1.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
3. Copy this package to your instance. Install the package with root privileges, for example:
   ```
   $ ls gvtap-agent_6.1.00_x86_64.rpm
   $ sudo rpm -i gvtap-agent_6.1.00_x86_64.rpm
   ```

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

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

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

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

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

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

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

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

5. Save the file.

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

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

7. Reboot the instance.

Check the status with the following command:

```
$ sudo service gvtap-agent status

G-vTAP Agent is running
```

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

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

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

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

Install IPSec on G-vTAP Agent

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

- **StrongSwan binary installer TAR file:** The TAR file contains StrongSwan binary installer for different platforms. Each platform has its own TAR file. Refer to https://www.strongswan.org/ for more details.

- **IPSec package file:** The package file includes the following:
  - CA Certificate
  - Private Key and Certificate for G-vTAP Agent
  - IPSec configurations

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

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

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

Install G-vTAP from Ubuntu/Debian Package

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

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

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

   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_6.1.00_amd64.deb
```

Install G-vTAP from Red Hat Enterprise Linux and CentOS

1. Launch RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**6.1.00**_x86_64.rpm
   - gvtap-ipsec_**6.1.00**_x86_64.rpm
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.
4. Install G-vTAP Agent package:
```
sudo rpm -ivh gvtap-agent_6.1.00_x86_64.rpm
```
5. Edit gvtap-agent.conf file to configure the required interface as source/destination for mirror:

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

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

NOTE: You must install IPSec package after installing StrongSwan.

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

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

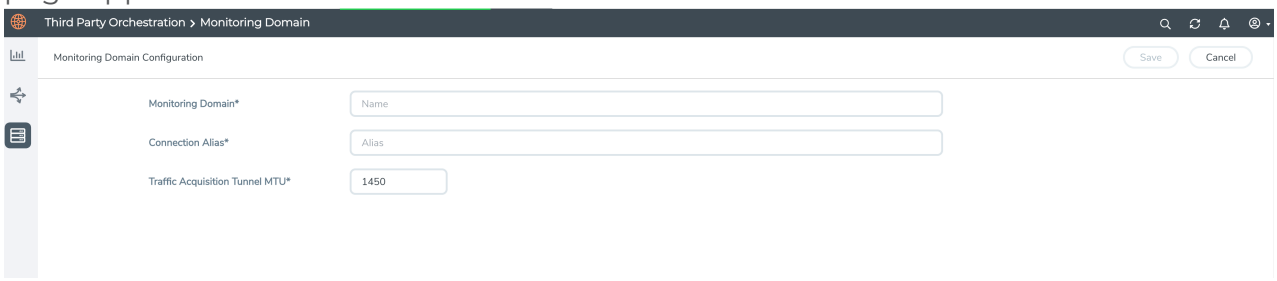
   NOTE: Any changes to the GvTAP agent config file made after the initial setup require an agent restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. When you have an active, successful monitoring session deployed, modifying the GvTAP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

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

Create Monitoring Domain

To create a monitoring domain in Third Party Orchestration:

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



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

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. The available options are: • **G-vTAP**: G-vTAP Agents are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to communicate to the G-vTAP Agents from GigaVUE-FM. The default MTU value is 1450. • **Customer Orchestrated Source**: If you select the Customer Orchestrated Source option, the mirrored, tunneled or the raw traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the G-vTAP Agents and G-vTAP Controllers.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	Enable this option if you wish to use the same monitoring session configuration for the the V Series Node deployed under this monitoring domain. Enable this check box when using packet mirroring configuration for GCP. **NOTE:** Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.
Traffic Acquisition Tunnel MTU (When Traffic Acquisition Method is G-vTAP Agent)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP Agent to the GigaVUE V Series Node.

4. Click **Save**.

Modes of Deployments

There are two ways in which GigaVUE V Series Nodes can be deployed using the third party orchestration. They are:

Generic Mode: In generic mode, when deploying GigaVUE V Series Nodes you can provide the monitoring domain and connection name in your orchestrator. A Monitoring Domain will be created under the **Third Party Orchestration** monitoring domain page in GigaVUE-FM and your GigaVUE fabric components will be deployed in that monitoring domain.

Integrated Mode: In integrated mode, you create a monitoring domain in your respective cloud suite in GigaVUE-FM and then use your own orchestration system to just deploy nodes. The GigaVUE V Series Nodes deployed using your own orchestration system will be displayed under the monitoring domain created in your respective cloud suite. In this case, ensure that the monitoring domain and the connection name given in the GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system.

Configure Role-Based Access for Third Party Orchestration

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

Users

The Users page lets you manage the GigaVUE-FM and GigaVUE-OS FM users. You can also configure user's role and user groups to control the access privileges of the user in GigaVUE-FM. To add users you must be a user with **fm_super_admin** role or a user with either read/write access to the FM security Management category.

To add users, refer to Add Users section in the *GigaVUE Administration Guide* for more detailed information.

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

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

Create Roles

You can associate a rule with user. Refer to Create Roles section in the *GigaVUE Administration Guide* for more detailed information. Under the **Select Permissions** tab select Third Party Orchestration and provide read/write premissions.

Create User Groups

You can use the user group option to associate the users with Roles and Tags. A user group consists of a set of roles and set of tags associated with that group. When a user is created they can be associated with one or more user groups. Refer to Create User GroupsCreate User Groups section in the *GigaVUE Administration Guide* for more detailed information.

Deploy Fabric Components using Generic Mode

In generic mode, when deploying GigaVUE V Series Nodes you can provide the monitoring domain and connection name in your orchestration system. A Monitoring Domain will be automatically created under the **Third Party Orchestration** monitoring domain page in GigaVUE-FM and your GigaVUE fabric components will be deployed in that monitoring domain. In this case, the monitoring domain and connection will be created in GigaVUE-FM after the fabric component deployment in your orchestrator.

Refer to the following section for more detailed information on how to deploy your fabric components in the respective cloud platforms:

- Configure GigaVUE Fabric Components in AWS
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in GCP
- Configure GigaVUE Fabric Components in Nutanix
- Configure GigaVUE Fabric Components in OpenStack
- Configure GigaVUE V Series Nodes using VMware ESXi

Configure GigaVUE Fabric Components in AWS

This section provides step-by-step information on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1500. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.

- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- When deploying the fabric components using generic mode it is not mandatory to add VPC name as the subgroup name.
- You can also create a monitoring domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. Refer to Create Monitoring Domain for more detailed information on how to create monitoring domain under third party orchestration.
- VPC Mirroring cannot be used as a traffic acquisition method when using generic mode.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.

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

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

Configure G-vTAP Controller in AWS

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

To register G-vTAP Controller in AWS EC2, use any one of the following methods:

- Register G-vTAP Controller during Instance Launch
- Register G-vTAP Controller after Instance Launch

Register G-vTAP Controller during Instance Launch

In your AWS EC2 portal, to launch the G-vTAP Controller AMI instance and register G-vTAP Controller using user data, follow the steps given below:

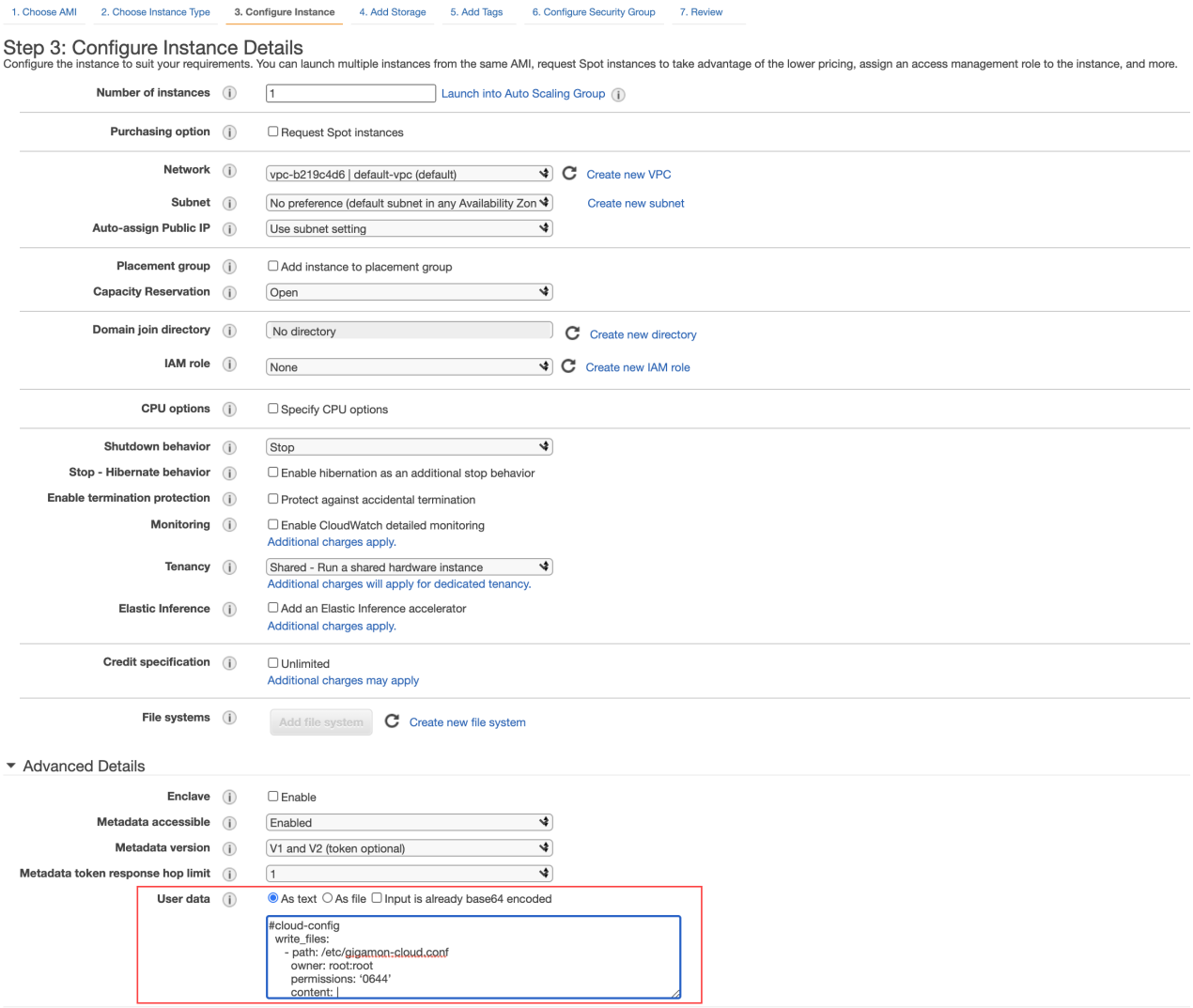
1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.

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

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

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

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



The G-vTAP Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

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

Register G-vTAP Controller after Instance Launch

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

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

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

3. Restart the G-vTAP Controller service.

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

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

Configure G-vTAP Agent in AWS

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

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

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

- Register G-vTAP Agent during Instance Launch
- Register G-vTAP Agent after Instance Launch

Register G-vTAP Agent during Instance Launch

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

In your AWS EC2, to launch the G-vTAP Agent AMI instance and register the G-vTAP Agent using user data, follow the steps given below:

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.

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

```
#cloud-config
write_files:
 - path: /etc/gigamon-cloud.conf
 owner: root:root
 permissions: '0644'
 content:
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the G-vTAP Controller 1>,
                  <IP address of the G-vTAP Controller 2>
        remotePort: 8891
```

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

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

Register G-vTAP Agent after Instance Launch

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

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

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

3. Create a local configuration file and enter the following user data.

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

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

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

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

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

To register GigaVUE V Series Node and GigaVUE V Series Proxy in AWS EC2, use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch
- Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Instances page of AWS EC2, click **Launch instances**. The Launch Instance wizard appears. For detailed information, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab, enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

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

Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

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

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

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

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

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

NOTE: When the GigaVUE V Series Node is stopped or terminated from the AWS, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

Configure GigaVUE Fabric Components in Azure

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

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1500. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.

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

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

Configure G-vTAP Controller in Azure

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

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

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

Register G-vTAP Controller during Virtual Machine Launch

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

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

2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The G-vTAP Controller uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

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

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

Register G-vTAP Controller after Virtual Machine Launch

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

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

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

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

3. Restart the G-vTAP Controller service.

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

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

Configure G-vTAP Agent in Azure

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

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

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

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

Register G-vTAP Agent during Virtual Machine Launch

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

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

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The G-vTAP Agent uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
 - path: /etc/gigamon-cloud.conf
 owner: root:root
 permissions: '0644'
 content:
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the G-vTAP Controller 1>,
                  <IP address of the G-vTAP Controller 2>
        remotePort: 8891
```

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

Register G-vTAP Agent after Virtual Machine Launch

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

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

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

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

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

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

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

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

Configure GigaVUE V Series Node and GigaVUE V Series Proxy in Azure

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

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

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

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

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

1. In the Virtual machines page of the Azure Portal, select **Create** then **Virtual machine**. Then **Create a Virtual Machine** Page appears. For detailed information, refer to Create virtual machine topic in Azure Documentation.
2. On the **Advanced** tab, enter the Custom Data as text in the following format and deploy the virtual machine. The GigaVUE V Series Node and GigaVUE V Series Proxy uses this custom data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register GigaVUE V Series Proxy after Virtual Machine Launch

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

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

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

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

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

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

NOTE: When the GigaVUE V Series Node is stopped or terminated from the Azure, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

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

Configure GigaVUE Fabric Components in GCP

This section provides step-by-step information on how to register GigaVUE fabric components using Google Cloud Platform (GCP) or a configuration file.

Minimum Requirements

The following table lists the minimum requirements for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	• c2-standard-4 for 2 interfaces • c2-standard-8 for 3 interfaces
GigaVUE V Series Proxy	e2-micro
G-vTAP Controller	e2-micro

Keep in mind the following when deploying the fabric components using GCP:

- For successful registration of fabric components, firewall rules must be configured to open ports 443 and 8891. Refer to Use VPC firewall rules topic in GCP documentation for more detailed information on how to configure firewall rules.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.
- When launching an instance, if you wish to access the instance using a private key, you will have add the key to the ssh key. The default password is gigamon.

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

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

Configure G-vTAP Controller in GCP

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

To register G-vTAP Controller in GCP, use any one of the following methods:

- Register G-vTAP Controller during Instance Launch
- Register G-vTAP Controller after Instance Launch

Register G-vTAP Controller during Instance Launch

In your GCP, to launch the G-vTAP Controller and to register G-vTAP Controller using custom metadata, follow the steps given below:

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to Create and Start instance topic in GCP Documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The G-vTAP Controller uses this Custom Metadata to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register G-vTAP Controller after Instance Launch

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

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

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

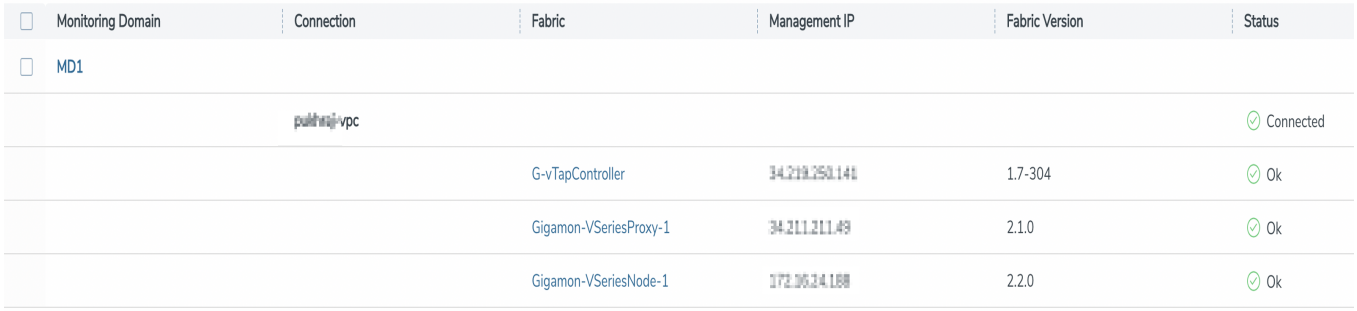
3. Restart the G-vTAP Controller service.

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

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

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

The G-vTAP Controller deployed in GCP appears on the Third Party Orchestration Monitoring Domain page of GigaVUE-FM.



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

Configure G-vTAP Agent in GCP

NOTE: Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms.

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

When using a windows G-vTAP Agent follow the steps given below installing the Windows G-vTAP Agent:

1. Deploy Windows server in GCP. Refer to Create a Windows Server VM instance in Compute Engine topic in Google documentation for step by step instructions.
2. After creating the windows server, follow the instruction in the *Connect to the VM instance by using RDP* section of Set up Chrome Remote Desktop for Windows on Compute Engine topic in the GCP documentation.
3. Download G-vTAP Agent build in your desktop and copy it to RDP session.

4. Turn off the Windows Firewall Defender. Then, install the Windows Agent refer to Windows G-vTAP Agent Installation for step-by-step instructions on how to install Windows Agent.

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

- Register G-vTAP Agent during Instance Launch
- Register G-vTAP Agent after Instance Launch

Register G-vTAP Agent during Instance Launch

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

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

In your GCP, to launch the instance and register the G-vTAP Agent using Custom Metadata, follow the steps given below:

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to Create and Start instance topic in GCP Documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The G-vTAP Agent uses this Custom Metadata to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
 - path: /etc/gigamon-cloud.conf
 owner: root:root
 permissions: '0644'
 content:|
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the G-vTAP Controller 1>,
                  <IP address of the G-vTAP Controller 2>
        remotePort: 8891
```

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

Register G-vTAP Agent after Instance Launch

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

1. Install the G-vTAP Agent in the Linux or Windows platform. For detailed instructions, refer to Linux G-vTAP Agent Installation and Windows G-vTAP Agent Installation.
2. Log in to the G-vTAP Agent.
3. Create a local configuration file and enter the following user data.

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

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

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

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in GCP

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

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

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch
- Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the VM instances page of Google Cloud Platform, click **Create instances** . For detailed information, refer to Create and Start instance topic in GCP Documentation.
2. Under the **Metadata** tab, enter the **key** as **user-data** and in the **value** field enter the below mentioned text in the following format and deploy the instance. The G-vTAP Agent uses this Custom Metadata to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

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

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

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

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

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

NOTE: When the GigaVUE V Series Node is stopped or terminated from the GCP, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

Configure Packet Mirroring for GCP

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers. The capture can be configured for both egress and ingress traffic, only ingress traffic, or only egress traffic.

Refer to the following topics for detailed information.

- Configure Packet Mirroring in GCP
- Deploy GigaVUE V Series Solution with Packet Mirroring

Prerequisites:

- When using packet mirroring, a minimum of 3 NICs must be configured and the Machine Type must be c2-standard-8 (8 vCPU, 32 GB memory).
- Create an instance template in GCP, refer to Create instance templates topic in Google Cloud Platform for more details.
- Create Instance Group in GCP with autoscaling in Managed Instance Group. Refer Create a MIG with autoscaling enabled topic in Google Cloud Documentation for more details.
- Configure TCP or UDP internal Load balancer with packet forwarding enabled and ensure that the GigaVUE V Series Nodes data NICs are used to receive traffic.
- Load Balancer forwards raw traffic. Therefore when configuring the monitoring session the Raw End Point must be used as the first component which receives traffic.
- Three NICs must be configured because REP and TEP cannot share the same interface.

A typical GCP deployment to support the internal load balancer and packet mirroring requires the following components:

- GigaVUE-FM (Fabric Manager
- GigaVUE V Series 2 Node
- GCP Internal Load Balancer (uniformly distributes traffic from GCP target VMs to GigaVUE V Series nodes)

Configure Packet Mirroring in GCP

To configure packet mirroring in GCP, refer to Use Packet Mirroring topic in Google Cloud Documentation for step-by-step instructions. After configuring the packet mirroring in GCP you must deploy the GigaVUE V Series solution in GigaVUE-FM.

Deploy GigaVUE V Series Solution with Packet Mirroring

To deploy GigaVUE V Series solution with packet mirroring in GigaVUE-FM:

Edit the monitoring domain and update the following details:

1. In the **Monitoring Domain Configuration** page, select **Customer Orchestrated Source** as the Traffic Acquisition method.
2. Enable the **Uniform Traffic Policy** check box. When enabling this option, same monitoring session configuration will be applied to all V Series Nodes.
3. Click **Save** to save the configuration.

Create a monitoring session with the following instructions:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select **Third Party Orchestratio**n. The **Monitoring Sessions** page appears.
2. Click **New** to open the **Create a New Monitoring Session** page. Refer to Create a Monitoring Session for more detailed information on how to create a monitoring session.
3. In the **Edit Monitoring Session** page. Add Raw End point as the first component and Tunnel End Point as the final component.
4. Then add your application to the monitoring session. Connect your components.
5. To deploy the monitoring session after adding the Raw End Point click the **Deploy** button in the edit monitoring session page.
6. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the interface for REP and TEP from the drop-down menu.

Configure GigaVUE Fabric Components in Nutanix

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

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1300. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.
- When you deploy the fabric components using third party orchestration, you cannot delete the monitoring domain without unregistering the registered fabric components.

In Nutanix Prism Central, you can configure the following GigaVUE fabric components:

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

Configure G-vTAP Controller in Nutanix

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

To register the G-vTAP Controller in Nutanix, you can use any one of the following methods:

- Register G-vTAP Controller during Instance Launch
- Register G-vTAP Controller after Instance Launch

Register G-vTAP Controller during Instance Launch

In the Nutanix Prism Central, to launch the G-vTAP Controller instance and register the G-vTAP Controller using user data, perform the following steps:

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For more information, refer to Creating a VM through Prism Central (AHV) topic in the Nutanix Documentation.
2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. Enter the registration data in the text box and deploy the instance. The G-vTAP Controller uses the user data to generate the config file (**/etc/gigamon-cloud.conf**) that is used to register with GigaVUE-FM.

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

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

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

Register G-vTAP Controller after Instance Launch

To register G-vTAP Controller after launching a Virtual Machine using a configuration file, perform the following steps:

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

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

3. Restart the G-vTAP Controller service.

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

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

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

Configure G-vTAP Agent in Nutanix

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

G-vTAP Agent should be registered using the registered G-vTAP Controller. It uses PORT 8891.

To register G-vTAP Agent in Nutanix, you can use any one of the following methods.

- Register G-vTAP Agent during Instance Launch
- Register G-vTAP Agent after Instance Launch

Register G-vTAP Agent during Instance Launch

NOTE: Registering G-vTAP Agent during Virtual Machine Launch is not applicable for Windows Agents. You can register the Windows Agent after launching the Virtual machine using a configuration file. The configuration file is located in **C:\ProgramData\gvtap-agent\gigamon-cloud.conf**

In Nutanix Prism Central, to launch the G-vTAP Agent instance and register the G-vTAP Agent using user data, perform the following steps:

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For detailed information, refer to Creating a VM through Prism Central (AHV) topic in Nutanix Documentation.
2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. Enter the registration data in the text box and deploy the instance. The G-vTAP Agent uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
write_files:
 - path: /etc/gigamon-cloud.conf
 owner: root:root
 permissions: '0644'
 content:|
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC Name>
        user: <Username>
        password: <Password>
        remoteIP: <IP address of the G-vTAP Controller 1>,
                  <IP address of the G-vTAP Controller 2>
        remotePort: 8891
```

Register G-vTAP Agent after Instance Launch

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

To register G-vTAP Agent after launching a Virtual Machine using a configuration file, perform the following steps:

1. Install the G-vTAP Agent in the Linux or Windows platform. For detailed instructions, refer to Linux G-vTAP Agent Installation and Windows G-vTAP Agent Installation.
2. Log in to the G-vTAP Agent.
3. Create a local configuration file and enter the following user data.

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

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

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

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

Configure GigaVUE V Series Nodes and V Series Proxy in Nutanix

NOTE: It is not mandatory to register GigaVUE V Series Nodes using the V Series proxy. However, if there are large number of nodes connected to GigaVUE-FM or if you want to hide the IP addresses of the nodes, then you can register the nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

NOTE: Before deploying V Series Node, enable the Multi Queue. For more information on enabling the multi-queue, refer to the Nutanix KB article How to change number of vNIC queues and enable RSS virtio-net Multi-Queue for AHV VMs. You can enable the Multi Queue using the Nutanix REST APIs. For more infomation on Nutanix APIs, refer to Nutanix support site.

To register GigaVUE V Series Node and GigaVUE V Series Proxy in Nutanix, you can use any one of the following methods.

- Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch
- Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

NOTE: When using VPC mirroring as the traffic acquistion method, add a tag with key **GigamonNode** and value **VSeriesNode** to the V Series Node or Proxy created on the platform.

1. On the Prism Central, go to the **List** tab and click **Create VM**. The Create VM dialogue box appears. For detailed information, refer to Creating a VM through Prism Central (AHV) topic in Nutanix Documentation.

2. On the **Step 3:Management** tab, in the Guest Customization field, select **Cloud-init (Linux)**. enter the registration data in the text box and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

- You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

Register GigaVUE V Series Node and GigaVUE V SeriesProxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, perform the following steps:

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

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

- You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes directly, enter the `remotePort` value as 443 and the `remoteIP` as <IP address of the GigaVUE-FM> or if you wish to deploy GigaVUE V Series Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

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

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

Limitations

IPv6 is not supported by Nutanix for the current release of GigaVUE Cloud Suite.

Configure GigaVUE Fabric Components in OpenStack

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

Keep in mind the following when deploying the fabric components using generic mode:

- Ensure that the Traffic Acquisition Tunnel MTU is set to the default value of 1500. To edit the Traffic Acquisition Tunnel MTU, select the monitoring domain and click on the **Edit Monitoring Domain** option. Enter the **Traffic Acquisition Tunnel MTU** value and click Save.
- Before deploying the monitoring session ensure that the appropriate Traffic Acquisition Tunnel MTU value is set. Otherwise, the monitoring session must be un-deployed and deployed again.
- User and Password provided in the registration data must be configured in the **User Management** page. Refer to Configure Role-Based Access for Third Party Orchestration for more detailed information. Enter the UserName and Password created in the **Add Users** Section.

In your OpenStack Dashboard, you can configure the following GigaVUE fabric components:

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

Configure G-vTAP Controller in OpenStack

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

To register G-vTAP Controller in OpenStack, use any one of the following methods:

- Register G-vTAP Controller during Instance Launch
- Register G-vTAP Controller after Instance Launch

Register G-vTAP Controller during Instance Launch

In your OpenStack dashboard, to launch the G-vTAP Controller and register G-vTAP Controller using Customization Script, follow the steps given below:

1. a. On the Instance page of OpenStack dashboard, click **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.

   b. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The G-vTAP Controller uses this registration data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register G-vTAP Controller after Instance Launch

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

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

a. Log in to the G-vTAP Controller.

b. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following Customization Script.

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

c. Restart the G-vTAP Controller service.

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

The deployed G-vTAP Controller registers with the GigaVUE-FM. After successful registration the G-vTAP Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing ,the fabric node status appears as 'Unhealthy'. If

more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the G-vTAP Controller and if that fails as well then GigaVUE-FM unregisters the G-vTAP Controller and it will be removed from GigaVUE-FM.

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

Configure G-vTAP Agent in OpenStack

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

To register G-vTAP Agent using a configuration file:

1. Install the G-vTAP Agent in the Linux or Windows platform. For detailed instructions, refer to Linux G-vTAP Agent Installation and Windows G-vTAP Agent Installation.
2. Log in to the G-vTAP Agent.
3. Edit the local configuration file and enter the following Customization Script.

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

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

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

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

The deployed G-vTAP Agent registers with the GigaVUE-FM through the G-vTAP Controller. After successful registration the G-vTAP Agent sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, G-vTAP Agent status appears as 'Unhealthy'. If

more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the G-vTAP Agent and if that fails as well then GigaVUE-FM unregisters the G-vTAP Agent and it will be removed from GigaVUE-FM.

Configure GigaVUE V Series Nodes and V Series Proxy in OpenStack

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

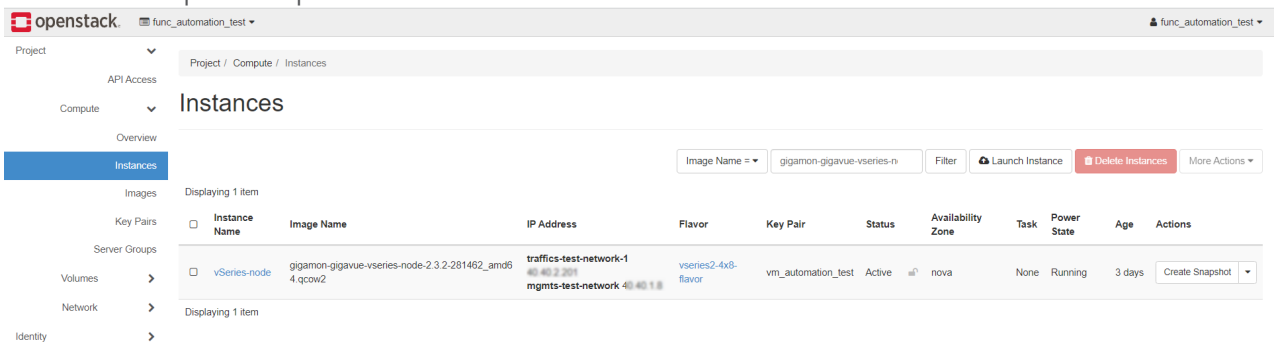
To register GigaVUE V Series Node and GigaVUE V Series Proxy in OpenStack, use any one of the following methods:

- Register V Series Nodes or V Series Proxy during Instance Launch
- Register V Series Node or V Series Proxy after Instance Launch

Register V Series Nodes or V Series Proxy during Instance Launch

To register V Series nodes or proxy using the Customization Script in OpenStack GUI:

1. On the Instance page of OpenStack dashboard, click **Launch instance**. The Launch Instance wizard appears. For detailed information, refer to Launch and Manage Instances topic in OpenStack Documentation.



2. On the **Configuration** tab, enter the Customization Script as text in the following format and deploy the instance. The V Series nodes or V Series proxy uses this customization script to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

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

Register V Series Node or V Series Proxy after Instance Launch

To register V Series node or proxy using a configuration file:

1. Log in to the V Series node or proxy.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following customization script.

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

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

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

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

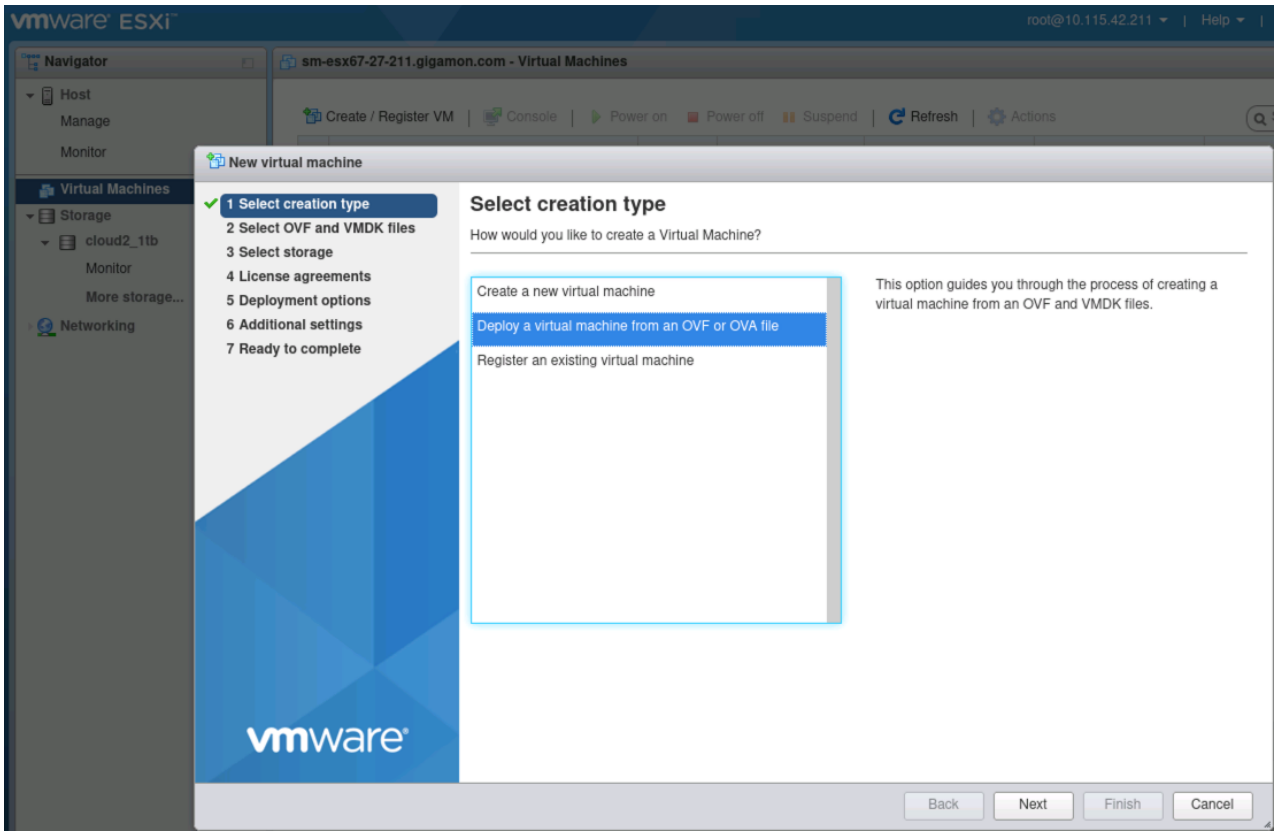
   NOTE: When the GigaVUE V Series Node is stopped or terminated from the OpenStack, it does not send any unregistration request and GigaVUE-FM will unregister the V Series Node soon after.

Configure GigaVUE V Series Nodes using VMware ESXi

This section describes how to deploy GigaVUE V Series Nodes under Third Party Orchestration Monitoring Domain using VMware ESXi Host.

- The nodes will be deployed under the Monitoring Domain in the **Third Party Orchestration**.
- When registering GigaVUE V Series nodes in GigaVUE-FM, the connection name under each monitoring domain must be unique.

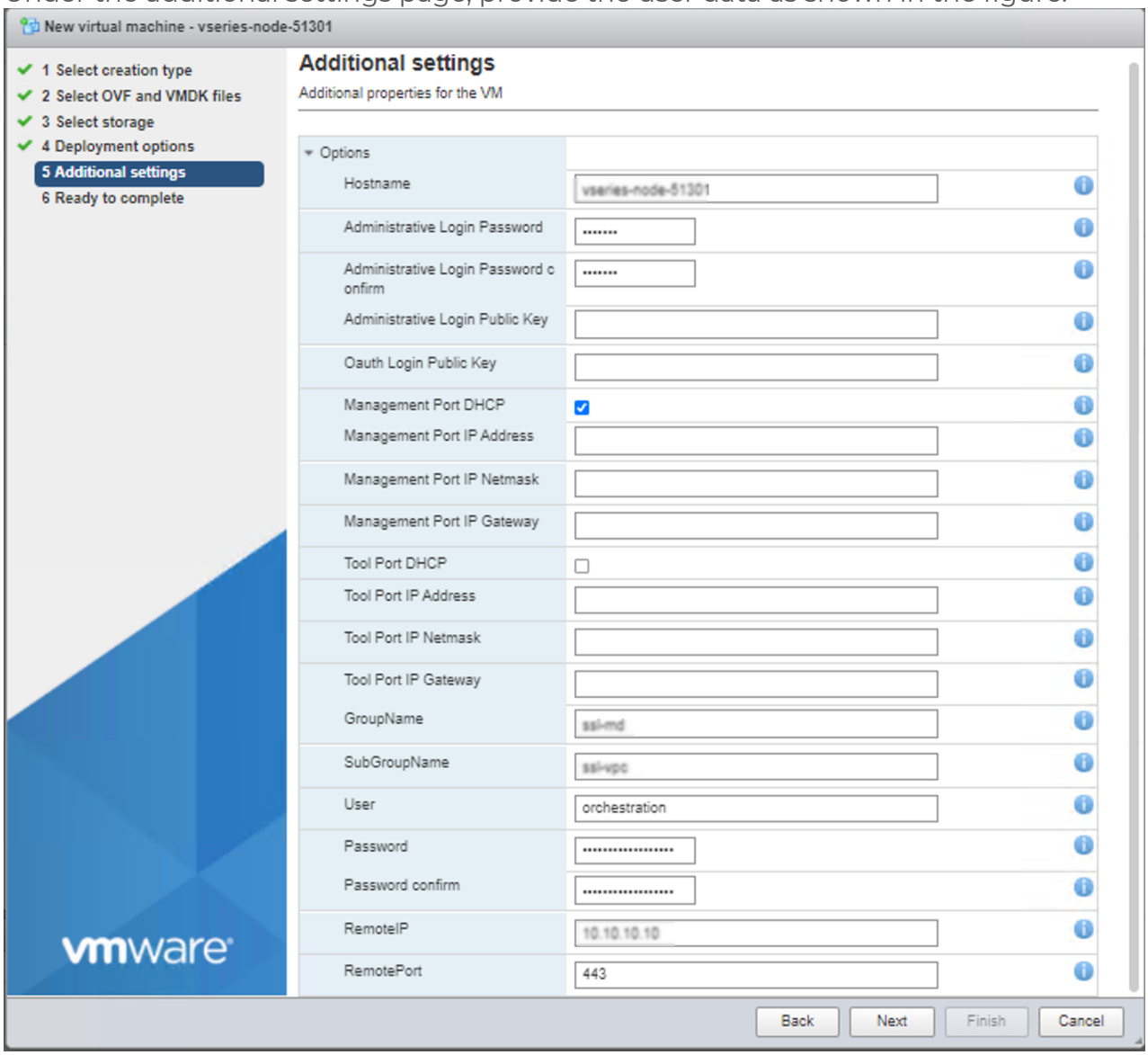
1. Login to VMware ESXi host using your web browser.
2. On the left navigation pane, select Virtual Machines and click **Create/Register VM**. The New Virtual Machine dialog box appears.



3. On the **Select Creation Type** page, select **Deploy a Virtual Machine from an OVF or OVA file**.
4. The **Select OVF and VMDK files** page appears. Provide a name for the Virtual machine. Upload either OVF and VMDK files or OVA files. Click Next.
5. Then, the **Select Storage** page appears, select the storage type and data store. Click Next.

6. Under the **Deployment Options**, provide the necessary details given below.
    a. Select the network port group associated with the host, network ports and tunneling port details from the **Network Mappings** drop-down.
    b. Select Thick/Thin from the **Disk provisioning** field.
    c. Select **Management Port DHCP** from the **Deployment type** drop-down.
    d. (optional) Enable the **Power on automatically** check-box to power on the Virtual Machine automatically.

7. Under the additional settings page, provide the user data as shown in the figure.



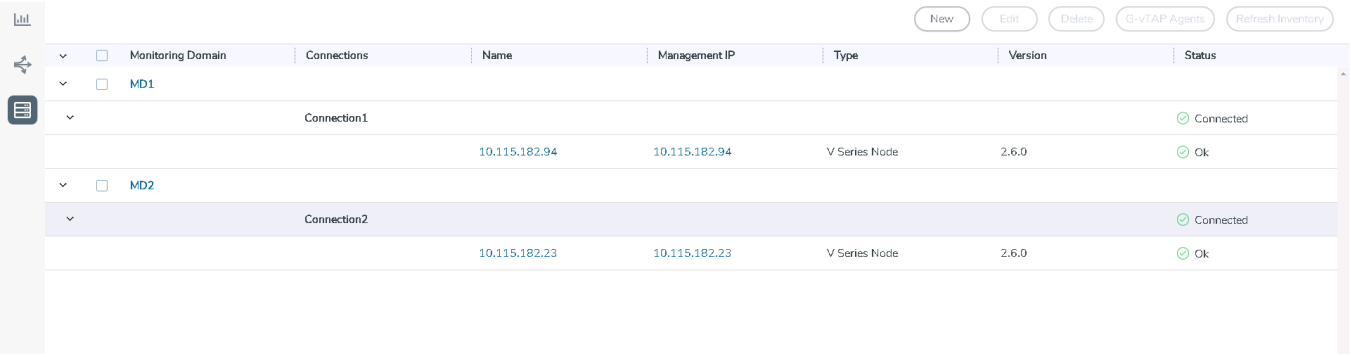
Enter the following values in the additional settings:

- Hostname: <Host Name>
- Administration Password: <Your Password>
- GroupName: <Monitoring domain name>
- SubGroupName: < Connection name>
- User: <Username>
- Password: <Password>
- remoteIP: <IP address of the GigaVUE-FM>
- remotePort: 443

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

8. Review the setting selection in the **Ready to Complete page**, then click Finish.

The GigaVUE V Series Node deployed in VMware ESXi host appears in Third-party Orchestration Monitoring Domain page of GigaVUE-FM.



Deploy Fabric Components using Integrated Mode

In integrated mode, you create a monitoring domain in your respective cloud suite in GigaVUE-FM and then use your own orchestration system to just deploy nodes. The GigaVUE V Series Nodes deployed using your own orchestration system will be displayed under the monitoring domain created in your respective cloud suite. In this case, ensure that the monitoring domain and the connection name given in the GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system.

Refer to the following topics on more detailed information on how to deploy your fabric components in the respective cloud platforms:

- Configure GigaVUE Fabric Components in AWS
- Configure GigaVUE Fabric Components in Azure
- Configure GigaVUE Fabric Components in OpenStack

Configure Monitoring Session

GigaVUE-FM automatically collects inventory data on all target instances available in your 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 design your monitoring session, refer to the following sections:

- Create a Monitoring Session
- Create Tunnel Endpoint
- Create Raw Endpoint
- Create Map
- GigaVUE Cloud Suite with GigaVUE V Series 2 node supports the following GigaSMART applications in the GigaVUE-FM canvas:
- 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.

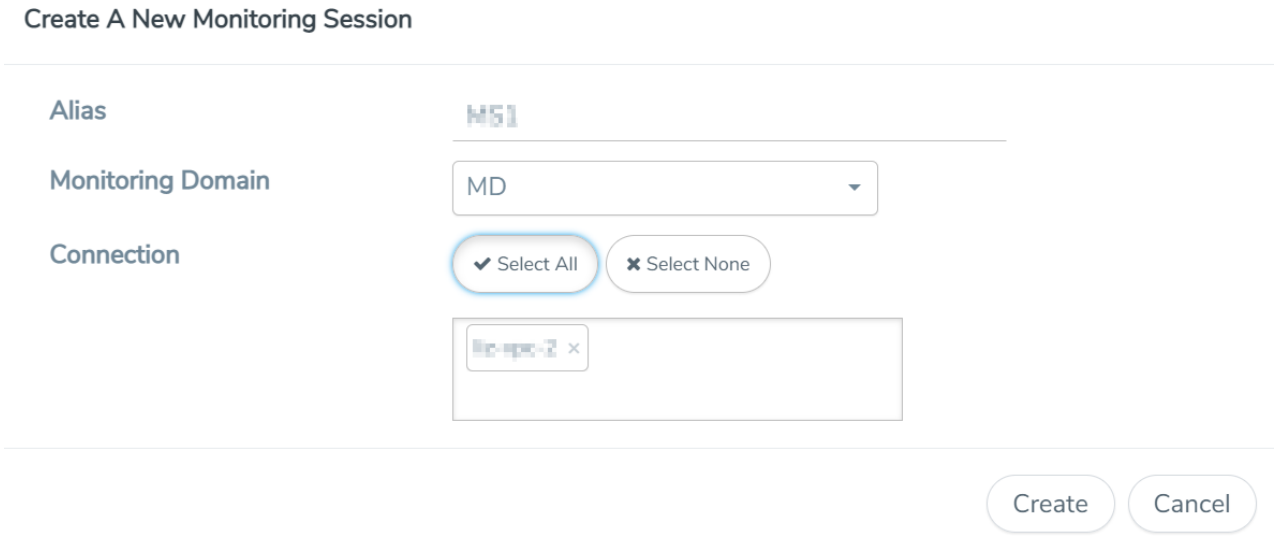
For the connections without G-vTAPs there is no targets that are automatically selected. You can use Tunnel as a Source in the monitoring session to accept a tunnel from anywhere.

You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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



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

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

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

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

Create Tunnel Endpoint

The customized traffic from the GigaVUE V Series node is distributed to the tunnel endpoints.

To create a new tunnel endpoint:

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

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

4. Click **Save**.

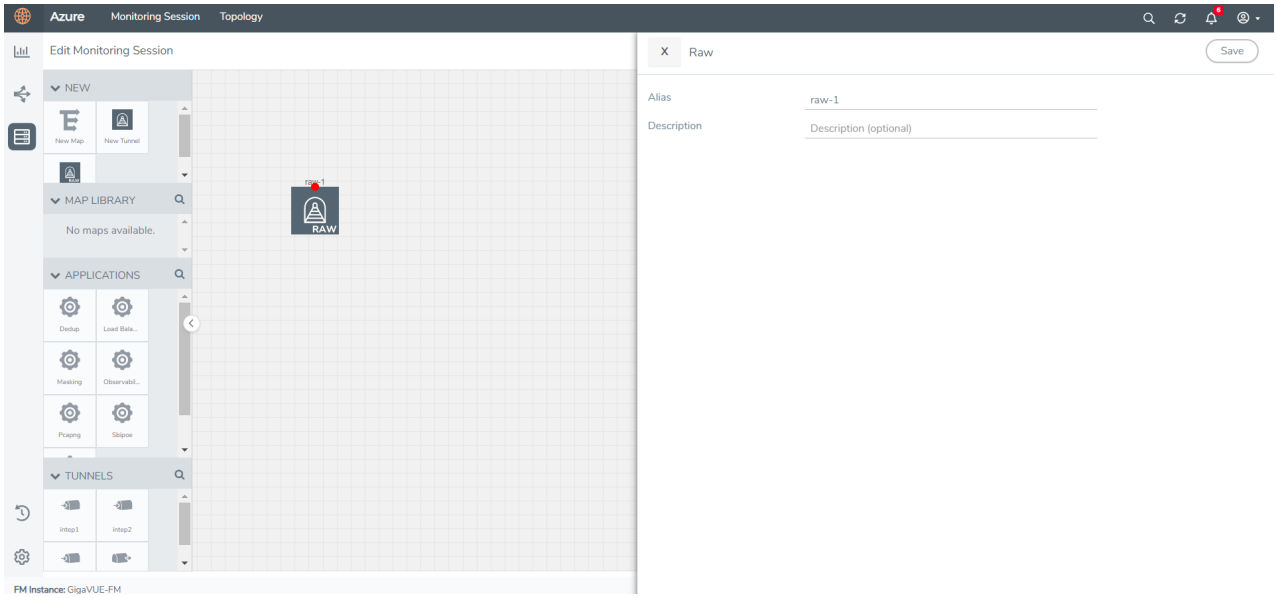
To delete a tunnel, select the required tunnel and click **Delete**.

Create Raw Endpoint

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

To add Raw Endpoint to the monitoring session:

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



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

Create Map

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

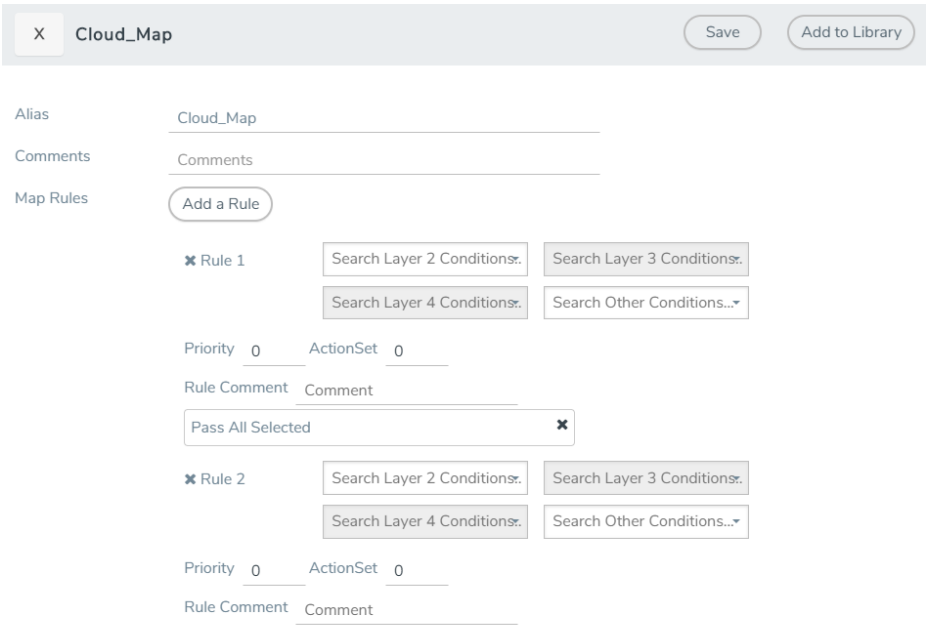
Conditions	Description
L2, L3, and L4 Filters	
EtherType	The packets are filtered based on the selected ethertype. The following conditions are displayed: ▪ IPv4 ▪ IPv6 ▪ ARP ▪ RARP ▪ Other

Conditions	Description
	L3 Filters If you choose IPv4 or IPv6, the following L3 filter conditions are displayed: ▪ Protocol ▪ IP Fragmentation ▪ IP Time to live (TTL) ▪ IP Type of Service (TOS) ▪ IP Explicit Congestion Notification (ECN) ▪ IP Source ▪ IP Destination **L4 Filters** If you select TCP or UDP protocol, the following L4 filter conditions are displayed: ▪ Port Source ▪ Port Destination
MAC Source	The egress traffic from the instances or ENIs matching the specified source MAC address is selected.
MAC Destination	The ingress traffic from the instances or ENIs matching the specified destination MAC address is selected.
VLAN	All the traffic matching the specified IEEE 802.1q Virtual LAN tag is filtered. Specify a number from 0 to 4094.
VLAN Priority Code Point (PCP)	All the traffic matching the specified IEEE 802.1q Priority Code Point (PCP) is filtered. Specify a value between 0 to 7.
VLAN Tag Control Information (TCI)	All the traffic matching the specified VLAN TCI value is filtered. Specify the exact TCI value.
Pass All	All the packets coming from the monitored instances are passed through the filter. When Pass All is selected, the L3 and L4 filters are disabled.

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

When you select a condition with either source or destination specified, it determines the direction based on the selection. For example, if only IP source is selected as shown in the

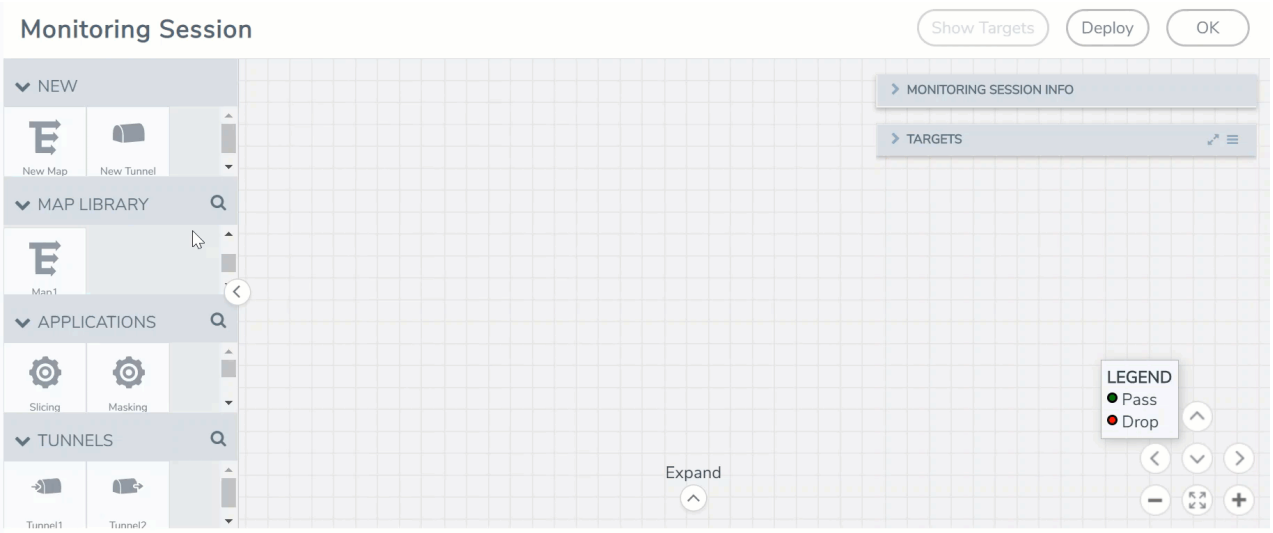
following figure, the egress traffic from the instances in the subnet 10.0.1.0/24 is selected for monitoring the traffic.



NOTE: You can create Inclusion and Exclusion Maps using all default conditions except EtherType and Pass All.

To create a new map:

1. 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. Enter the appropriate information for creating a new map as shown in the following table.

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

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

4. To reuse the map, click **Add to Library**. Save the map using one of the following ways:
   - 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 VPC.
5. Click **OK**.

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

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

- Slicing
- Masking

- De-duplication
- Load Balancing
- PCAPng Application
- Application Metadata Exporter
- Passive SSL Decryption

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

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

- Application Metadata Intelligence
- Application Filtering Intelligence

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

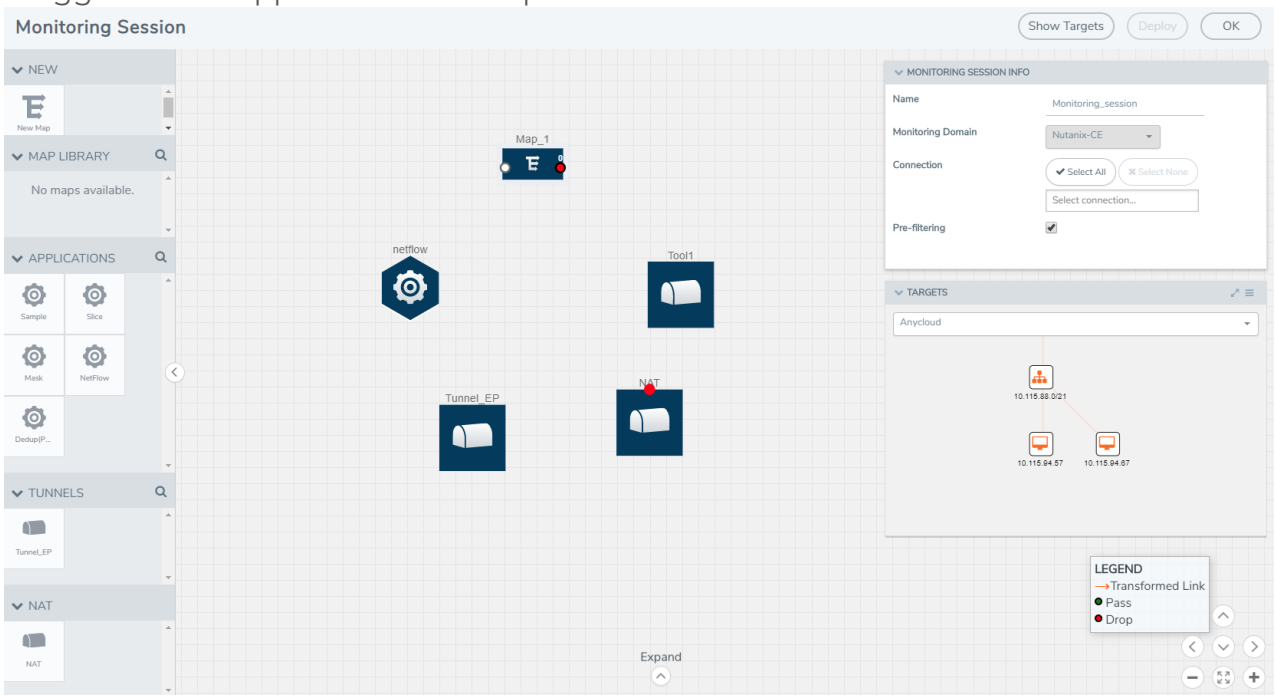
Deploy Monitoring Session

To deploy the monitoring session:

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

   NOTE: For information about adding applications to the workspace, refer to Add Applications (GigaVUE V Series 2) and Add Applications (GigaVUE V Series 1).

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



You can add up to 8 links from a action set to different maps, applications, or monitoring tools.

5. Hover your mouse on the map, click the red dot, and drag the link over to another map, application, or tunnel. You can drag more than one link from a map to the destination. On these links, you can apply link transformation to alter the packets. For information about adding link transformation, refer to Add Header Transformations.
6. Hover your mouse on the application, click the red dot, and drag the link (arrow) over to the tunnel endpoints. The traffic matching the rules in each action set is routed to maps, applications, or monitoring tools.
7. Click **Show Targets** to view details about the subnets and monitoring instances.The instances and the subnets that are being monitored are highlighted in orange.
8. Click **Deploy** to deploy the monitoring session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on all GigaVUE V Series nodes and G-vTAP Agents. If the monitoring session is not deployed properly, then one of the following errors is displayed:
   - Partial Success—The session is not deployed on one or more instances due to G-vTAP or GigaVUE V Series node failure.
   - Failure—The session is not deployed on any of the GigaVUE V Series nodes and G-vTAP Agents.

   Click on the status link to view the reason for the partial success or failure.
9. Click **View** under Statistics to view and analyze the incoming and outgoing traffic.

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

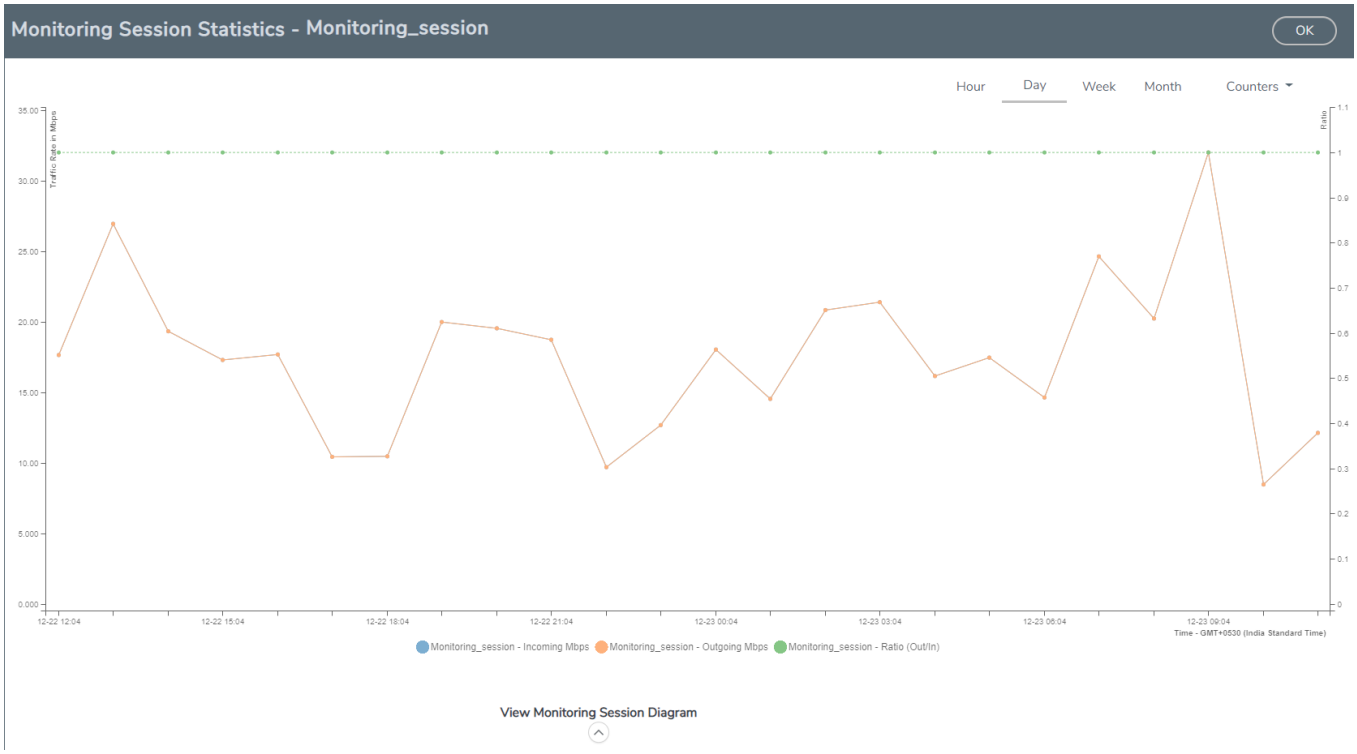
- Use the **Clone** button to duplicate the selected monitoring session.
- Use the **Edit** button to edit the selected monitoring session.
- Use the **Delete** button to delete the selected monitoring session.

View Monitoring Session Statistics

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

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

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



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

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

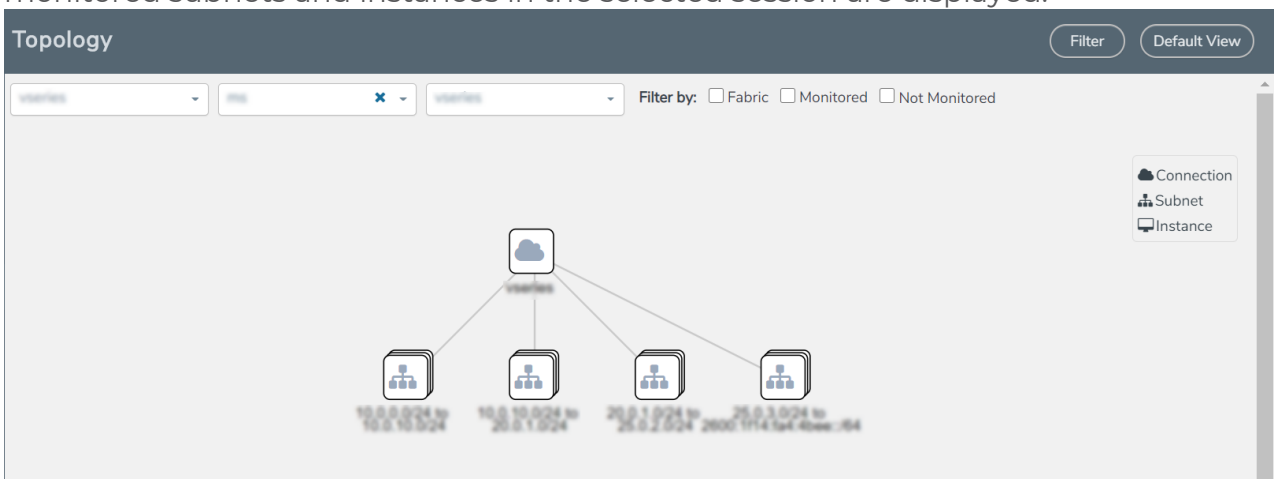
- On the **Monitoring Session Diagram** page, you can expand any map, or tunnel to open a **Details** quick view of that item to see more details about the incoming and outgoing traffic for that item.
- You can also scroll down the Map **Details** quick view to view the Map Rules, Action Sets, and Map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

Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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



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

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

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

Configure Application Intelligence Solutions on GigaVUE V Series Nodes using Third Party Orchestration

You can use your own orchestration system to deploy GigaVUE V Series Nodes and then use GigaVUE-FM to configure advanced features like Application Intelligence, Application Metadata Intelligence, and Application Filtering Intelligence.

Deploying the fabric components to configure Application Intelligence session using third party Orchestration can be done in two ways:

- Generic Mode
- Integrated Mode

Generic Mode

When using generic mode, GigaVUE-FM automatically creates an environment and connection when you deploy your fabric components in your orchestration system. In this case, the environment and the connections are created after the fabric components registeration. The fabric components deployed will listed in both the monitoring page and the connections page. They can only be used in either one of these places. For example: If the GigaVUE V Series Nodes in the Connection page is used to configure Application Intelligence session, then it cannot be used for monitoring purposes in the monitoring domain. The default traffic acquisition method is G-vTAP Agents. You can edit the connection and change the traffic acquisition method you wish to use.

NOTE: When using generic mode you cannot configure multiple connections under a single connection group.

Integrated Mode

When deploying your fabric components using integrated mode, you must create environments and connections before registering your fabric components. And provide the environment and connection name as groupname and subgroupname in the registration data that will be used in your orchestration system.

To configure the Application Intelligence solution on the GigaVUE V Series Nodes, create a virtual environment with the required connections. After creating the connections, configure the sources and the required destinations for the traffic flow.

Important Notes for Application Intelligence Session:

- You can configure multiple connections under a single connection group (only in integrated mode).
- You can deploy multiple GigaVUE V Series Nodes in a connection.
- You can use **V Series Node API Proxy Server** (VPS) to scale and manage multiple V Series Nodes. Refer to the GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide for detailed information.
- You can use tool templates while creating an Application Metadata Intelligence session. To create a custom tool template for GigaVUE V Series Node, signature is required from the node. Refer to the Tool Templates section in the *GigaVUE Fabric Management Guide* for more detailed information.
- When using generic mode the default traffic acquisition method is G-vTAP Agent, you can edit the connection and change the traffic acquisition method. This is applicable only when using third party orchestration method. You cannot edit connection when using GigaVUE-FM as your orchestrator.

Configure Environment

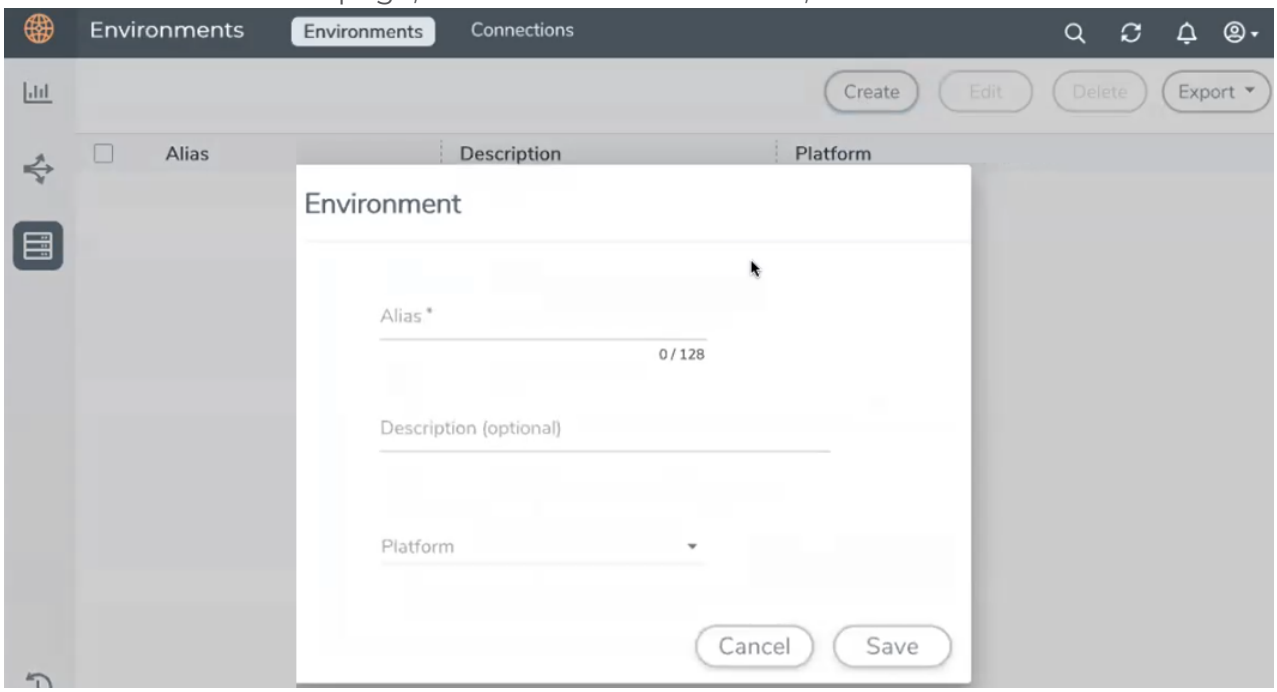
The Environments page allows you to create the following:

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

Create Environment

To configure the Environment:

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



3. Select or enter the following details:

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

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

Use the following buttons to manage your environment:

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

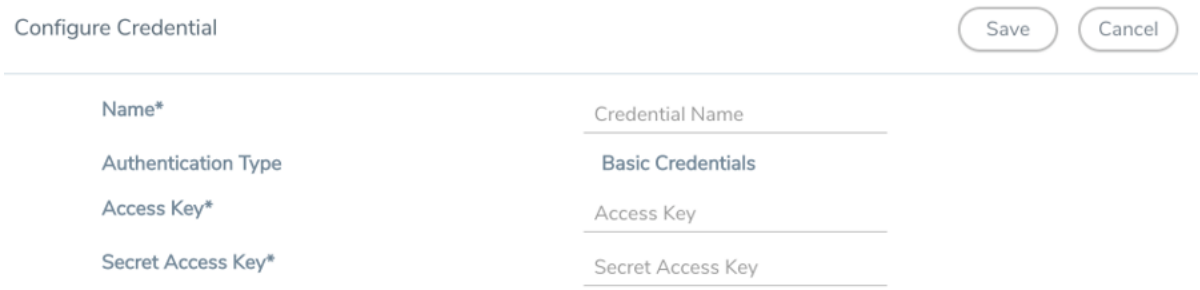
Create Credentials

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

Create AWS Credentials

To create AWS credentials:

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



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

Field	Action
Name	An alias used to identify the AWS credential.
Authentication Type	**Basic Credentials** For more information, refer to AWS Security Credentials.
Access Key	Enter your AWS access key. It is the credential of an IAM user or the AWS account root user.
Secret Access Key	Enter your secret access key. It is the AWS security password or key.

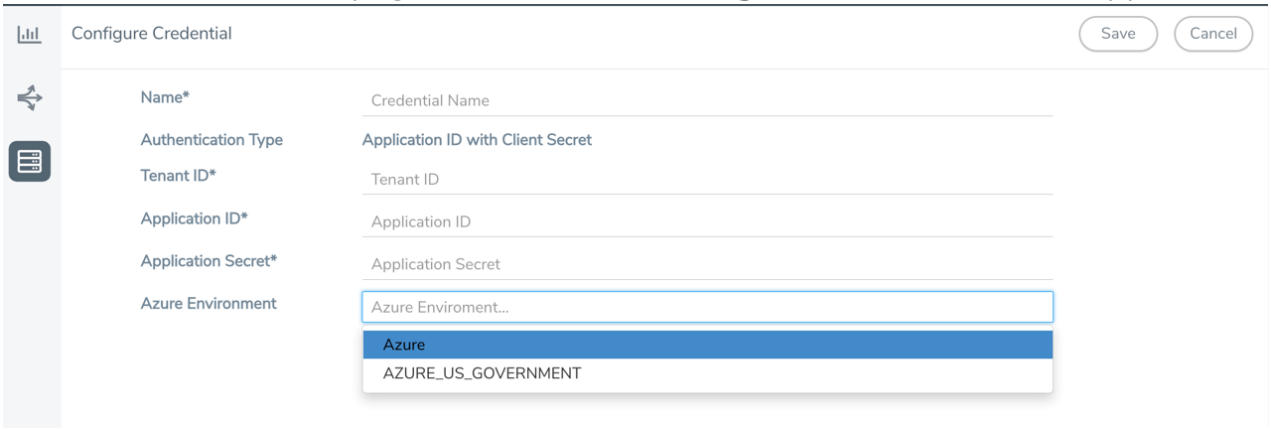
5. Click **Save**.

Create Azure Credentials

To create Azure credentials:

1. From the left navigation pane, click**Inventory** > **Resources** > **Environment**.
2. On the **Environments** page, on the **Credentials** tab, select **Azure** from the drop-down menu.

3. In the Azure Credential page, click **Add**. The **Configure Credential** wizard appears.



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

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

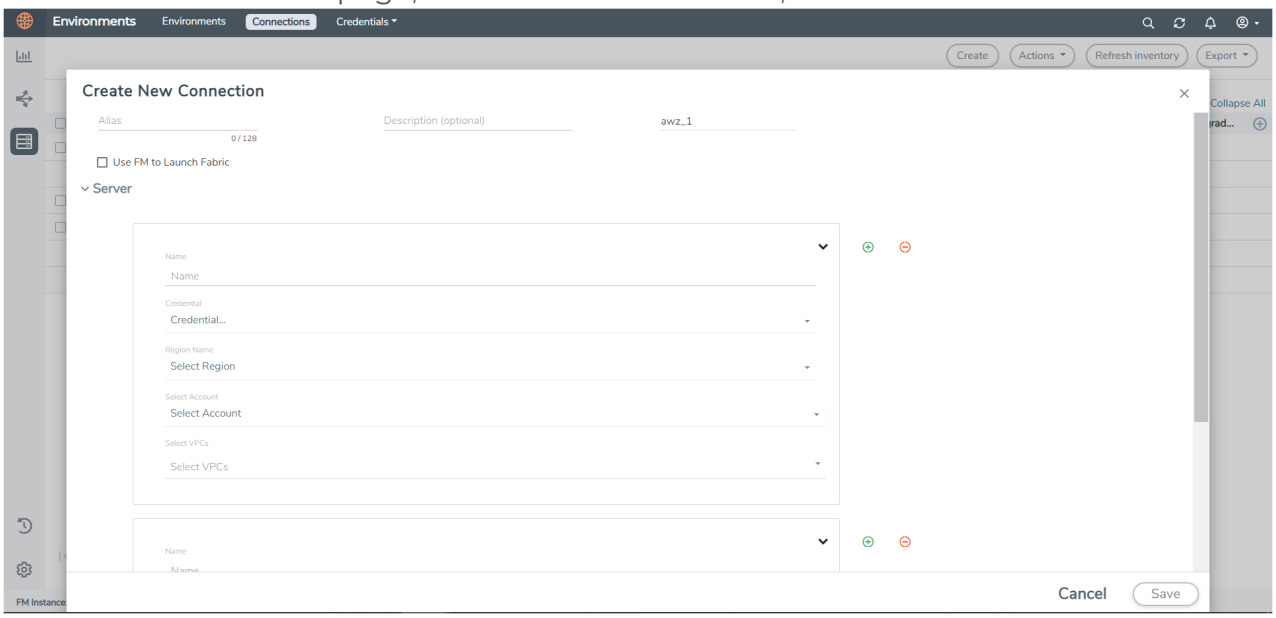
5. Click **Save**.

You can view the list of available AWS and Azure credentials in the Credentials page.

Create Connection

To create a new Connection:

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



3. The **Create New Connection** dialog box opens.

Field	Description
Alias	Alias name used to identify the connection.
Description	Brief description about the connection.
Environment	Select the environment. Refer to the Configure Environment section Create Connection
Use FM to Launch Fabric	Disable this check box, if you wish to deploy GigaVUE fabric components using third party orchestration.

Connect to AWS

To connect to AWS, select or enter the following details under the server details:

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials for detailed information on how to create credentials.
Secret Region	The AWS region for the connection. For example, EU (London). **NOTE:** If the region you want to choose is not available in the Region Name list, you

Field	Description
	can add a custom region. **Adding a Custom Region** To add a custom region: **a.** In the Region Name drop-down list, select **Custom Region**. **b.** In the Custom Region Name field, enter the name of the region that is not available in the list.
Select Account	Select the AWS account name/id.
Select VPCs	Select the VPC
Traffic Acquisition Method	Select a Tapping method. The available options are: ▪ **G-vTAP**: If you select G-vTAP as the tapping method, you must configure the G-vTAP Controller to monitor the G-vTAP Agents. You can also configure the G-vTAP Controller and G-vTAP Agents using your own orchestor. Refer to Configure GigaVUE Fabric Components using AWS Orchestrator for detailed information. ▪ **VPC Traffic Mirroring**: If you select VPC Traffic Mirroring option as tapping method, only nitro-based agent is support. If you wish to use an external load balancer (optional). Select **Yes** to use a load balancer. Refer to Configure an External Load Balancer for detailed information. G-vTAP Controller configuration is not required for VPC Traffic Mirroring. **NOTE:** VPC Traffic Mirroring is not applicable when generic mode. ▪ **Tunnel**: If you use select Tunnel as the tapping method, you can select the tunnel as a source where the traffic is directly tunneled to GigaVUE V Series Nodes without deploying G-vTAP Agents or G-vTAP controllers.. **NOTE:** For VPC Traffic Mirroring option, additional permissions are required. Refer to the Permissions for details.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. **NOTE:** The default MTU is 1450. You can edit the MTU value according to your requirements. The valid range is between 1450 to 9000.

Connect to Azure

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

Field	Description
Name	Name used to identify the connection.
Credential	Select your credentials from the drop-down menu. Refer Create Credentials

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

Connect to VMware ESXi

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

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

Field	Description
vCenter IP Address/ Hostname	The IP address of the virtual server.
vCenterUserName	Valid user name
vCenterPassword	Password for the user

Connect to VMware NSX-T

Rules and Notes

- NSXT- manager version must be 3.1.3. Otherwise after editing the solution, the packets will not reach the GigaVUE V Series Node.
- NSX-T manager cannot be registered for more than one GigaVUE-FM.

- For GigaVUE-FM software version 5.13.00, you cannot deploy more than one GigaVUE V Series Node.
- **For GigaVUE-FM software version 5.13.00**: If you configure a GigaVUE V Series Node with the Application intelligence solution, then you must not configure other basic GigaSMART applications, such as slicing, masking, and vice-e-versa. These GigaSMART applications cannot work in parallel.

To connect to VMware NSX-T, select or enter the following details:

Field	Description
Alias	Alias name used to identify the connection.
Description	Brief description about the connection.
Environment	Select the environment configured in the Create Connection
Server	The IP address or the DNS name of the virtual server.
vCenterUserName	Valid user name
vCenterPassword	Password for the user
NSX-T Manager IP Address	IP address or Hostname of your VMware NSX-T.
NSX-T User Name	Username of your NSX-T account.
NSX-T Password	Password of your NSX-T account.
Image URL	Web Server URL of the directory where V Series node OVA, VMDK, and OVF files are available. The Web Server URL must be in the follwoing format: *http://<server-IP:port>/<path to where the OVF files are saved>* and the port can be any valid number.
GigaVUE-FM User Name	GigaVUE-FM username.
GigaVUE-FM Password	GigaVUE-FM password

After creating a connection, deploy your fabric components. Refer toDeploy Fabric Components using Generic Mode for more detailed information on how to deploy fabric components like G-vTAP Agents, G-vTAP Controllers, and GigaVUE V Series Node and Proxy using your own orchestrator for the above mentioned platforms.

NOTE: When a G-vTAP Controller is unregistered, the solution goes to a failed state, to resolve this ensure either deploy a new G-vTAP Controller or redeploy the existing G-vTAP Controller.

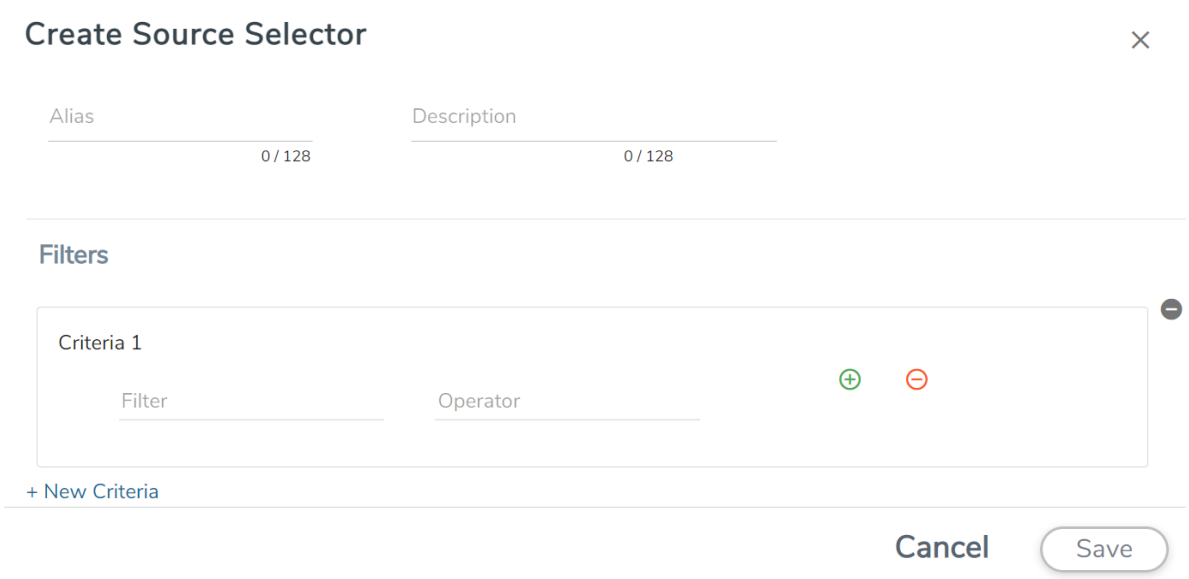
Create Source Selectors

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

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

To configure the Source Selectors:

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



3. Enter or select the required information:

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

4. Click Save to save the source selector.

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

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

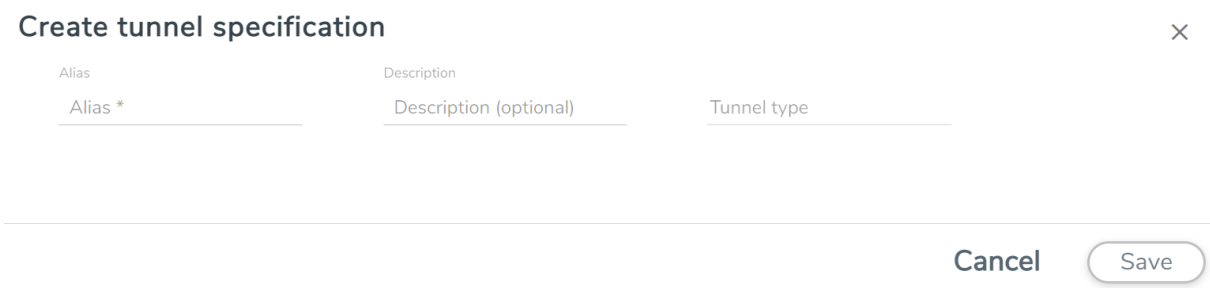
Create Tunnel Specifications

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

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

To configure the tunnels:

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



3. Enter or select the following information:

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

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

Configure Application Intelligence Session

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

Prerequisites

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

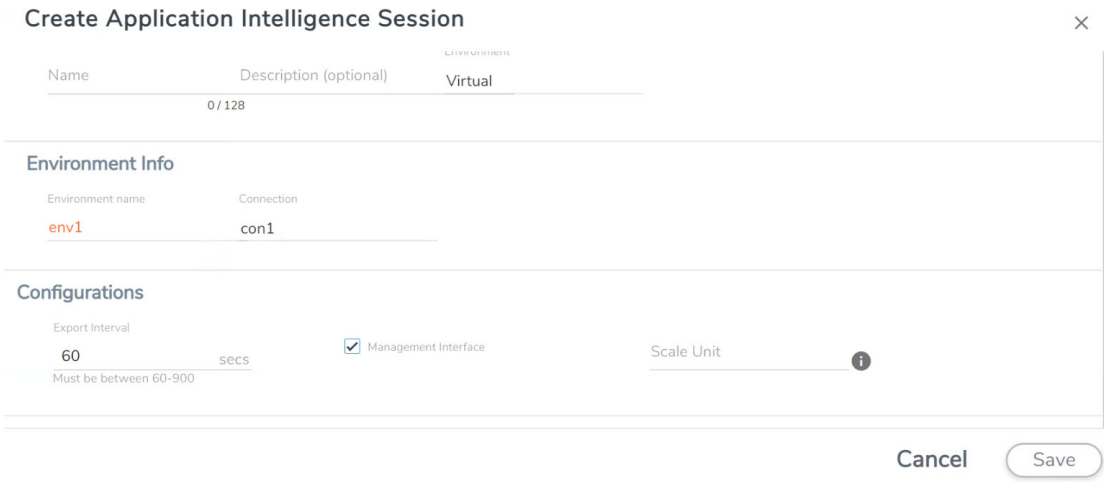
> **NOTE:** For Application Visualization and Application Metadata Intelligence, the destination(s) are defined internally by the solution.

Create an Application Intelligence Session in Virtual Environment

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

To create an Application Intelligence Session:

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



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

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

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

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

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

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

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

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

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

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

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

7. Click **Save**. The session created is added in the list view.

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

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

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

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

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

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

Administer GigaVUE Cloud Suite for Third Party Orchestration

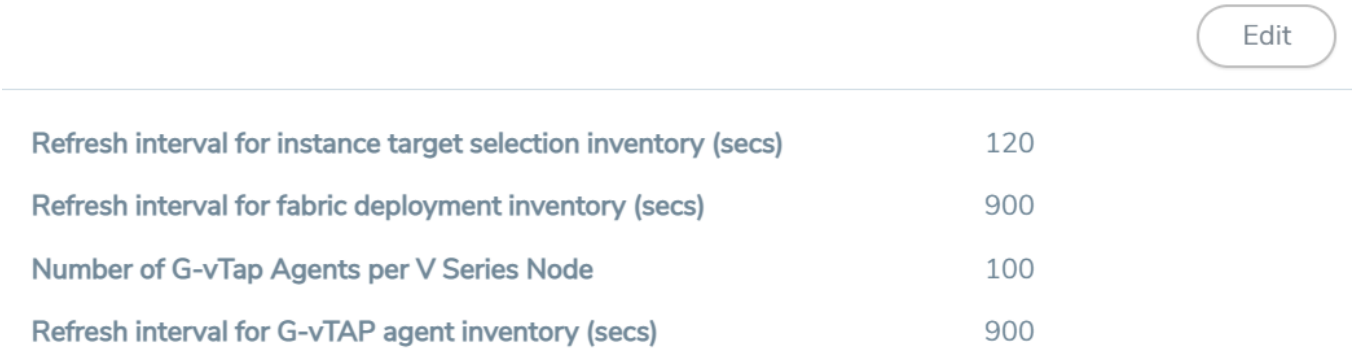
You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

- Configure Third Party Orchestration Settings
- Role Based Access Control

Configure Third Party Orchestration 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 > Third Party Orchestration> Settings**.



In the Settings page, select **Advanced** tab to edit these Third Party Orchestration settings.

Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of the instances.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric nodes
Number of G-vTAP Agents per V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE V Series node.
Refresh interval for G-vTAP Agent inventory (secs)	Specifies the frequency for discovering the G-vTAP Agents available.

Role Based Access Control

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

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

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

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

NOTE: Cloud APIs are also RBAC enabled.

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

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

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series 2 Nodes
6.1.00	v6.1.00	v6.1.00	v6.1.00	v6.1.00
6.0.00	v1.8-7	v1.8-7	v2.7.0	v2.7.0
5.16.00	v1.8-5	v1.8-5	v2.6.0	v2.6.0
5.15.00	v1.8-5	v1.8-5	v2.5.0	v2.5.0
5.14.00	v1.8-4	v1.8-4	v2.4.0	v2.4.0
5.13.01	v1.8-3	v1.8-3	v2.3.3	v2.3.3

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

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

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

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

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

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

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

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

Visit the Gigamon Community site to:

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

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

Register today at community.gigamon.com

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

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

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

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)