GigaVUE Cloud Suite for AnyCloud Guide

GigaVUE Cloud Suite

Product Version: 5.15

Document Version: 1.0

(See Change Notes for document updates.)

Copyright 2022 Gigamon Inc.. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc..

Trademark Attributions

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

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
5.15.00	1.0	03/30/2022	Original release of this document with 5.15.00 GA.

Contents

GigaVUE Cloud Suite for AnyCloud Guide 1
Change Notes 3
Contents 4
GigaVUE Cloud Suite for AnyCloud 6
About GigaVUE Cloud Suite for AnyCloud 6
Components of GigaVUE Cloud Suite for AnyCloud 7
Architecture of GigaVUE Cloud Suite for AnyCloud 8
Get Started with GigaVUE Cloud Suite for AnyCloud 9
License Information 9
Bring Your Own License (BYOL) 9
Deploy GigaVUE Cloud Suite for AnyCloud 11
Obtain Images 11
Launch GigaVUE-FM 11
Launch GigaVUE-FM using ESXi Host 11
Deploy V Series Nodes using VMware ESXi GUI 14
Prepare G-vTAP Agent to Monitor Traffic 17
Linux Agent Installation 17
Windows G-vTAP Agent Installation 21
Install IPSec on G-vTAP Agent 24
Create Monitoring Domain 28
Configure GigaVUE V Series Nodes using VMware ESXi 31
Configure and Manage Resources 35
Create a Monitoring Session 35
Create Tunnel Endpoint 37
Create a New Map 38
Agent Pre-filtering 42
Add Applications (GigaVUE V Series 2) 43
Slicing 43
Masking 44
Dedup 45
Passive SSL Decryption 46
Add Applications (GigaVUE V Series 1) 51
Sampling 52
Slicing 53

Masking 54
NetFlow 55
Dedup 67
Deploy Monitoring Session 67
Add Header Transformations 70
View Monitoring Session Statistics 71
Visualize the Network Topology 72
Administer GigaVUE Cloud Suite for AnyCloud 73
Configure AnyCloud Settings 74
Role Based Access Control 75
GigaVUE-FM Version Compatibility Matrix 76
GigaVUE-FM Version Compatibility for V Series 2 Configuration 76
GigaVUE-FM Version Compatibility for V Series 1 Configuration 76
Additional Sources of Information 77
Documentation 77
How to Download Software and Release Notes from My Gigamon 79
Documentation Feedback 80
Contact Technical Support 81
Contact Sales 81
Premium Support 81
The Gigamon Community 82
Glossary 83

GigaVUE Cloud Suite for AnyCloud

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

Topics:

- About GigaVUE Cloud Suite for AnyCloud
- Get Started with GigaVUE Cloud Suite for AnyCloud
- Deploy GigaVUE Cloud Suite for AnyCloud
- Configure and Manage Resources
- Administer GigaVUE Cloud Suite for AnyCloud
- GigaVUE-FM Version Compatibility Matrix

About GigaVUE Cloud Suite for AnyCloud

The GigaVUE Cloud Suite solution for the following platforms are mature solutions with complete support for configuration and upgrade from GigaVUE-FM:

- GigaVUE Cloud Suite for AWS
- GigaVUE Cloud Suite for Azure
- GigaVUE Cloud Suite for OpenStack

For the other cloud platforms (public or private) available in the market, the GigaVUE Cloud Suite for AnyCloud deployment option provides traffic visibility.

The GigaVUE Cloud Suite for AnyCloud option consists of the following components:

- GigaVUE® Fabric Manager (GigaVUE-FM)
- G-vTAP Agents
- G-vTAP Controllers
- GigaVUE V Series Controllers
- 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 Any Cloud 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.

This section introduces the components of the GigaVUE Cloud Suite for AnyCloud solution and the supported architecture for deploying the cloud solution in any of the available cloud platforms.

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

It provides instructions for connecting GigaVUE-FM in any of the cloud platforms available in the market. For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation and Upgrade Guide* available in the Gigamon Documentation Library.

Components of GigaVUE Cloud Suite for AnyCloud

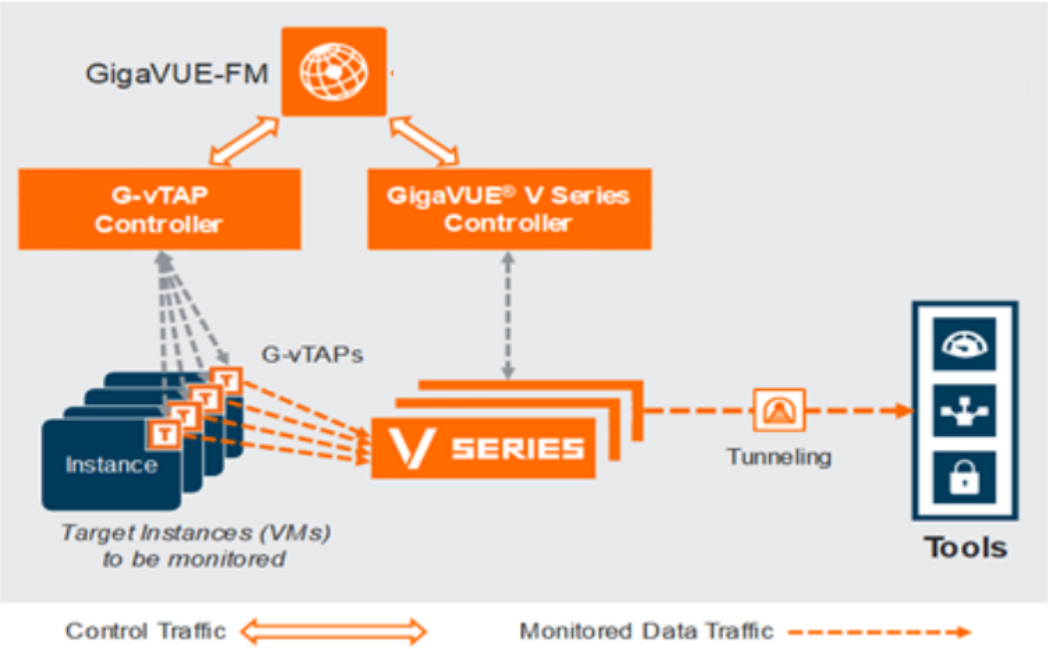
The following table provides a brief description of the components in the AnyCloud deployment option:

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 Controller	GigaVUE® V Series Controller 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 Controllers 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

This guide provides instructions on how to use GigaVUE-FM for configuration in any cloud platform available in the market.

Architecture of GigaVUE Cloud Suite for AnyCloud

The following diagram shows a high-level architecture of the GigaVUE Cloud Suite AnyCloud configuration:



Get Started with GigaVUE Cloud Suite for AnyCloud

This chapter describes how to plan and start the GigaVUE Cloud Suite for AnyCloud deployment.

Refer to the following sections for details:

- License Information

License Information

The GigaVUE Cloud Suite for AnyCloud supports Bring Your Own License (BYOL) model.

Bring Your Own License (BYOL)

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

- Traffic visibility for up to 100 virtual TAP points (VMs)
- Traffic visibility for up to 1000 virtual TAP points (VMs)

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

The minimum term for the license is 3 months. For purchasing licenses with the BYOL option, contact our Gigamon Sales. Refer to Contact Sales. To generate and apply license, refer to the *"Licensing"* section in the *GigaVUE Administration Guide*.

Deploy GigaVUE Cloud Suite for AnyCloud

This chapter describes how to connect to the GigaVUE Cloud Suite for AnyCloud solution.

Refer to the following sections for details:

- Obtain Images
- Launch GigaVUE-FM
- Prepare G-vTAP Agent to Monitor Traffic
- Create Monitoring Domain
- Configure GigaVUE V Series Nodes using VMware ESXi

Obtain Images

You must have obtained the images for the components of the GigaVUE Cloud Suite for AnyCloud.

NOTE: You are responsible for downloading the image and launching it in your environment. The components can be deployed using the compatible disk formats in respective cloud platform.

The number of GigaVUE V Series node required depends on the number of G-vTAP Agents in the environment. The number of G-vTAP Agent instances per GigaVUE V Series nodes is based on the metrics available in the Settings tab.

Launch GigaVUE-FM

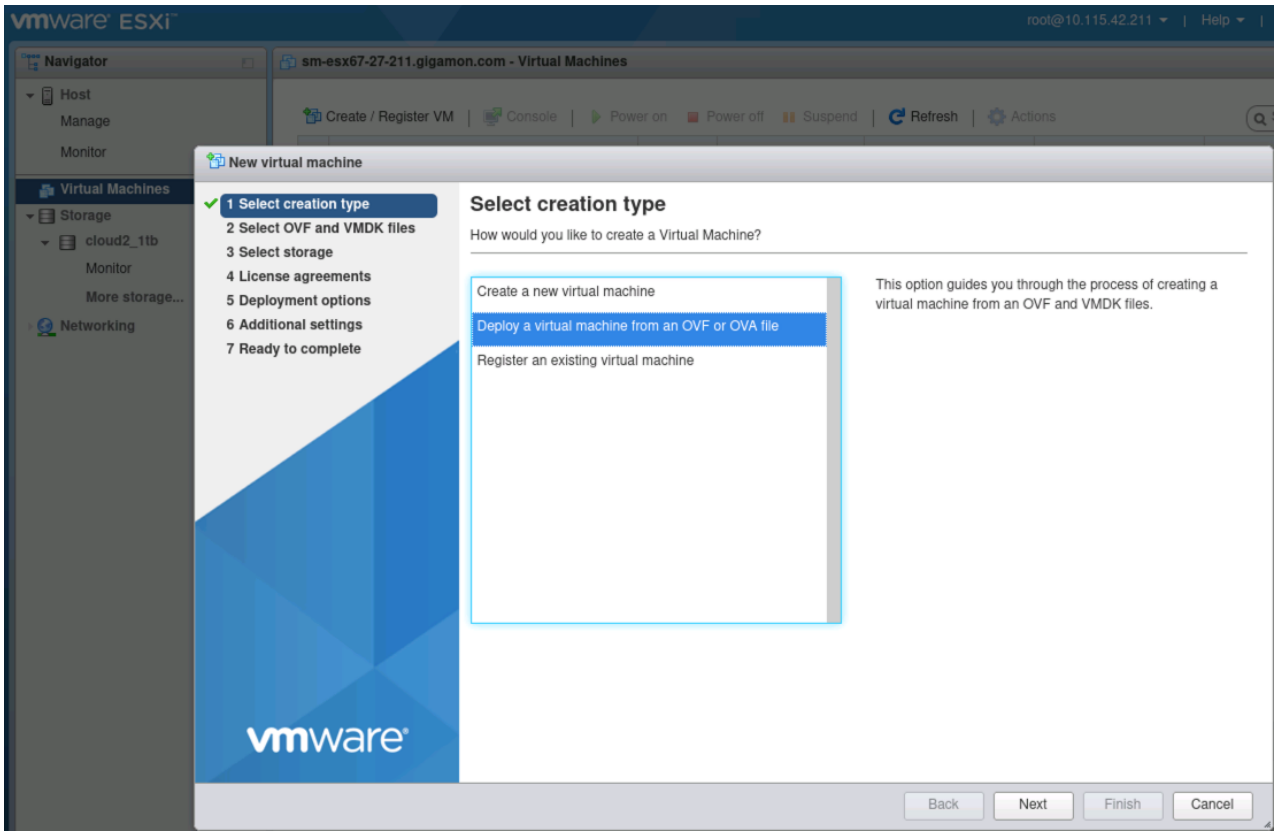
The GigaVUE-FM software package is available in multiple formats such as OVA, QCOW2, ISO. Use the appropriate media format to deploy GigaVUE-FM.

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

Launch GigaVUE-FM using ESXi Host

You can use your VMware ESXi host to deploy GigaVUE-FM using OVA or OVF files. To deploy GigaVUE-FM using ESXi host follow the steps given below:

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 page appears.

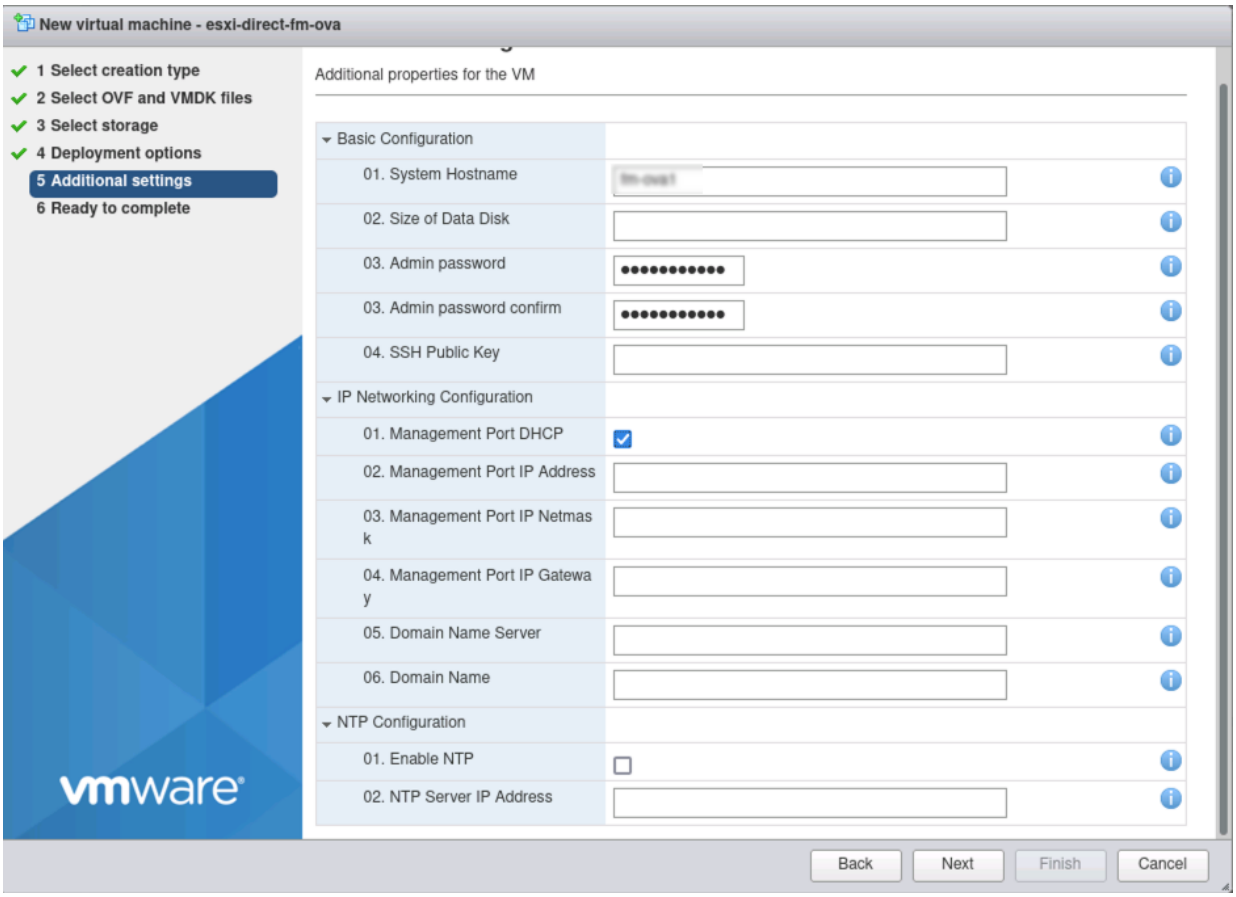


3. On the New Virtual Machine page, click on **Select Creation Type** from the left navigation pane. Then, select **Deploy a Virtual Machine from an OVF or OVA file**.
4. On the left navigation pane, click on **Select OVF and VMDK files**. Provide virtual machine name and upload the ova file. Data is extracted from the OVA or OVF files and based on the data extracted from the image, the ESXi wizard displays the necessary parameters that need to configured.
5. Click on **Select Storage**, to choose the storage type and data store.
6. Under the **Deployment Options**, provide the necessary details given below.
   a. Select the network port group associated with the host from the **Network Mappings** drop-down.
   b. Select Thick/Thin from the **Disk provisioning** field.
   c. (optional) Enable the **Power on automatically** check-box to power on the Virtual Machine automatically.
7. Under the additional settings page, provide Basic Configuration, IP Network Configuration, NTP Configuration details.

- DHCP Configuration:
  a. Under Basic Configuration provide the System Hostname and Admin password.

     NOTE: Use only the default password (admin123A!!) for admin password.

  b. Under IP Network Configuration, enable the **Management Port DHCP** checkbox.
  c. Under NTP Configuration details, provide the NTP server details.



- Static Configuration:
  a. Under Basic Configuration provide the System Hostname and Admin password.

     NOTE: Use only the default password (admin123A!!) for admin password.

  b. Under IP Network Configuration, enter the Management Port IP address, Management Port IP Netmask, Management Port IP Gateway, Domain Name Server and Domain Name details.
  c. Under NTP Configuration details, provide the NTP server details.

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

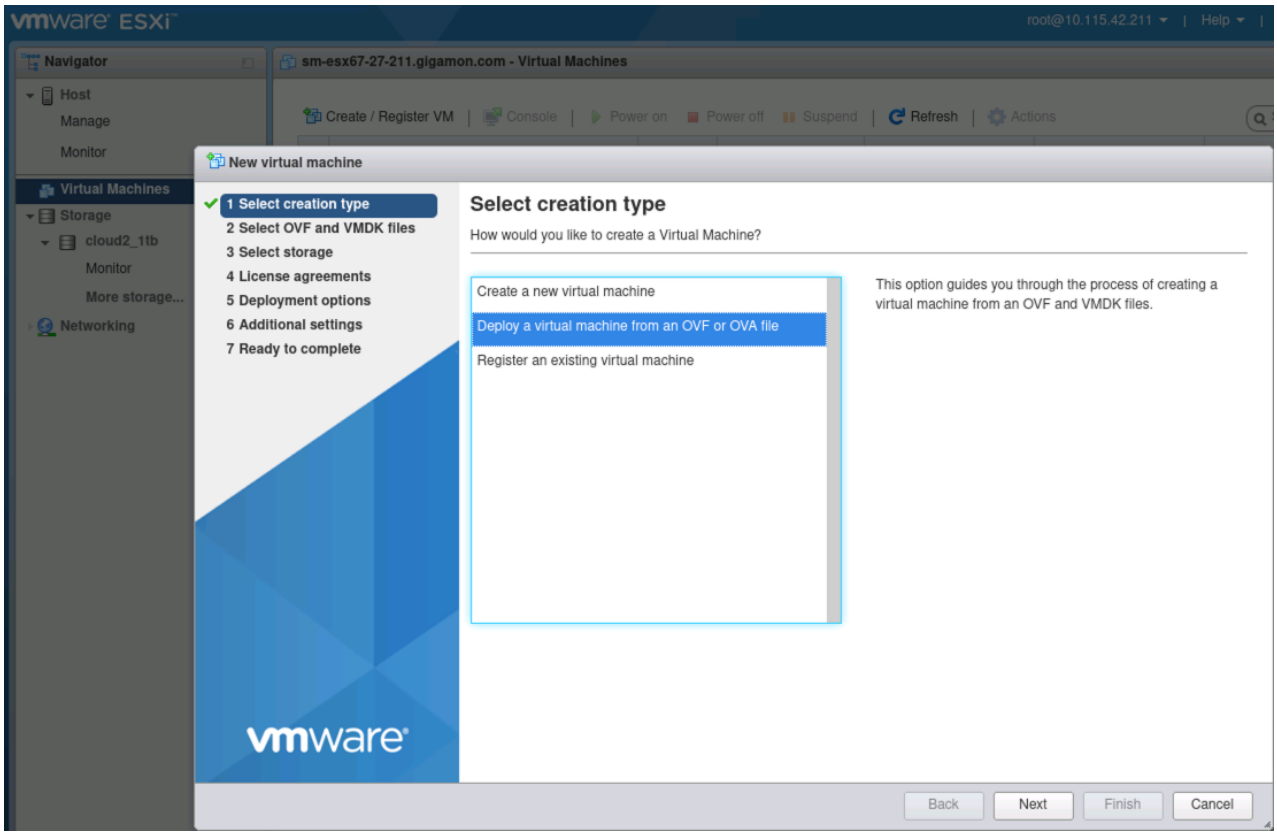
Deploy V Series Nodes using VMware ESXi GUI

You can use your own VMware ESXi host system to deploy V Series nodes and use GigaVUE-FM to configure the advanced features supported by these nodes. These nodes register themselves with GigaVUE-FM using the information provided by the user in the virtual machine creation wizard. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

This section describes how to deploy V Series Nodes under AnyCloud Monitoring Domain using VMware ESXi Host.

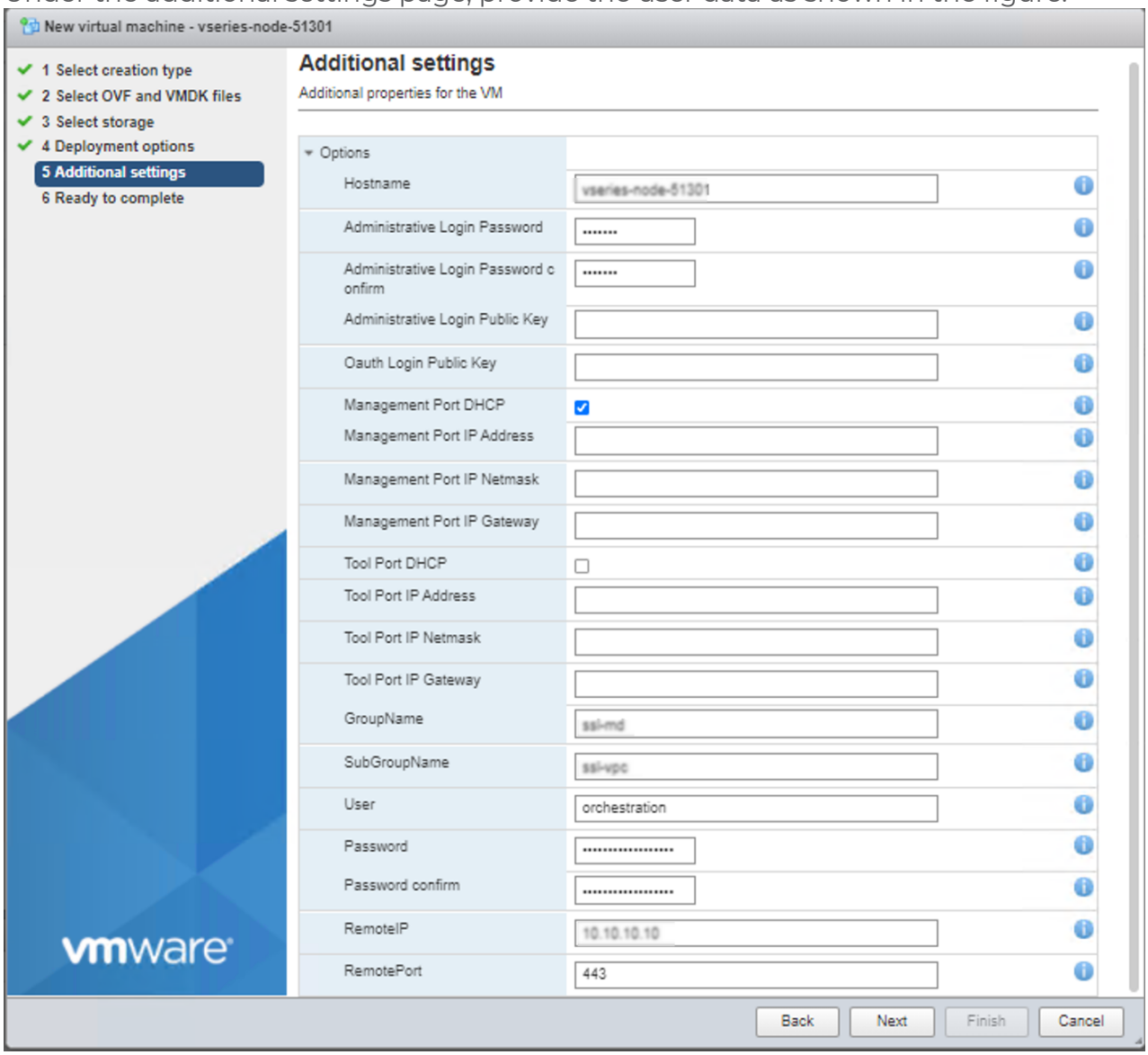
- The nodes will be deployed under the Monitoring Domain created in AnyCloud.
- When registering V Series nodes in GigaVUE-FM, the connection name under each monitoring domain must be unique.

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 page appears.



3. On the New Virtual Machine page, click on **Select Creation Type** from the left navigation pane. Then, select **Deploy a Virtual Machine from an OVF or OVA file**.
4. On the left navigation pane, click on **Select OVF and VMDK files**. Provide virtual machine name and upload the ova file.
5. Click on **Select Storage**, to choose the storage type and data store.
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: Description: orchestration
- Password: orchestration123A!
- remoteIP: <IP address of the GigaVUE-FM>
- remotePort: 443

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

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

Prepare G-vTAP Agent to Monitor Traffic

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

> **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 or VXLAN tunnel interface to the GigaVUE Cloud Suite V Series node.

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

> **NOTE:** AnyCloud deployment supports monitoring for only one vNIC per guest VM, although it is still possible to have a dedicated tunnel vNIC on a guest VM in addition to monitored vNIC.

Refer to the following sections for more information:

- Linux Agent Installation
- Windows G-vTAP Agent Installation
- Install IPSec on G-vTAP Agent

Linux Agent Installation

Refer to the following sections for the Linux agent installation:

- Single vNIC Configuration
- Install G-vTAP Agents

Single vNIC Configuration

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

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

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

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

Example—Grant permission to monitor ingress and egress traffic at iface

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

NOTE: The GigaVUE Cloud Suite for AnyCloud supports only single NIC G-vTAP Agent configuration.

Install G-vTAP Agents

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

You can install the G-vTAP Agents either from Debian or RPM packages as follows:

- Install G-vTAP from Debian Package
- Install G-vTAP from RPM package

Install G-vTAP from Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support. For more detailed information refer GigaVUE-FM Version Compatibility Matrix.
2. Copy this package to your VM. Install the package with root privileges, for example:

```
$ ls gvtap-agent_1.8-5_amd64.deb

$ sudo dpkg -i gvtap-agent_1.8-5_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.

   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
   ```

4. Save the file.
5. Reboot the VM.

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

```
$ sudo /etc/init.d/gvtap-agent status

G-vTAP Agent is running
```

Install G-vTAP from RPM package

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

1. Download the G-vTAP Agent Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Contact Technical Support. For more detailed information refer GigaVUE-FM Version Compatibility Matrix.
2. Copy this package to your VM. Install the package with root privileges, for example:

   ```
   $ ls gvtap-agent_1.8-5_x86_64.rpm

   $ sudo rpm -i gvtap-agent_1.8-5_x86_64.rpm
   ```

3. 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.

   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
   ```

4. Save the file.
5. Reboot the VM.

Check the status with the following command:

```
$ sudo /etc/init.d/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_**1.8-5**_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_1.8-5_x86_64.rpm
   ```

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

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

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

7. Install strongSwan:

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

8. Reboot the instance.

Windows G-vTAP Agent Installation

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

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

Windows G-vTAP Agent Installation Using MSI Package

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

1. Download the Windows G-vTAP Agent **1.8-5** 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 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 **`1.8-5`** 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 restart the Windows G-vTAP Agent, perform one of the following actions:
   - Restart the VM.
   - Run 'sc stop gvtap' and 'sc start gvtap' from the command prompt.
   - Restart the G-vTAP Agent from the Windows Task Manager.

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

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

Install IPSec on G-vTAP Agent

If IPSec is used to establish secure connection between G-vTAP Agents andGigaVUE V 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_**1.8-5**_amd64.deb
   - gvtap-ipsec_**1.8-5**_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_1.8-5_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_1.8-5_amd64.deb
   ```

Install G-vTAP from Red Hat Enterprise Linux and CentOS

1. Launch RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**1.8-5**_x86_64.rpm
   - gvtap-ipsec_**1.8-5**_x86_64.rpm

3. Copy the downloaded G-vTAP package files and strongSwan TAR file to the G-vTAP Agent.
4. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_1.8-5_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_1.8-5_x86_64.rpm
   ```

NOTE: You must install IPSec package after installing StrongSwan.

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

1. Launch the RHEL/CentOS agent image.
2. Download the following packages from the Gigamon Customer Portal. For assistance contact Contact Technical Support.
   - strongSwan TAR files
   - gvtap-agent_**1.8-5**_x86_64.rpm
   - gvtap-ipsec_**1.8-5**_x86_64.rpm
   - gvtap.te and gvtap_ipsec.te files (type enforcement files)
3. Copy the downloaded G-vTAP package files and strongSwan TAR file to G-vTAP Agent.
4. Checkmodule -M -m -o gvtap.mod gvtap.te
   ```
   semodule_package -o gvtap.pp -m gvtap.mod
   sudo semodule -i gvtap.pp
   ```
5. Checkmodule -M -m -o gvtap_ipsec.mod gvtap_ipsec.te
   ```
   semodule_package -o gvtap_ipsec.pp -m gvtap_ipsec.mod
   sudo semodule -i gvtap_ipsec.pp
   ```
6. Install G-vTAP Agent package:
   ```
   sudo rpm -ivh gvtap-agent_1.8-5_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_1.8-5_x86_64.rpm
   ```
10. Reboot the instance.

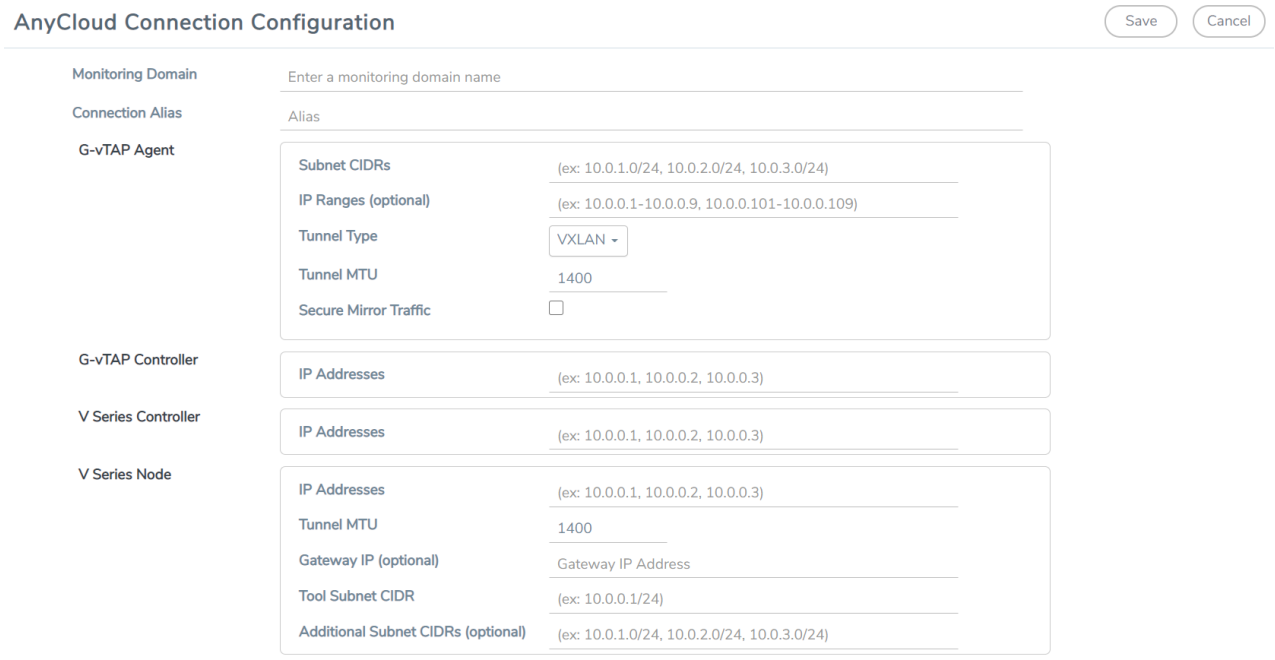
Create Monitoring Domain

Before connecting to your cloud platform, you must ensure the following:

- GigaVUE-FM must be launched in your cloud platform.
- G-vTAP Agent, G-vTAP Controller, GigaVUE V Series Node and GigaVUE V Series Controller must be installed in your cloud platform.

To configure a AnyCloud connection from GigaVUE-FM:

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


AnyCloud Connection Configuration
Save
Cancel
Monitoring Domain
Enter a monitoring domain name
Connection Alias
Alias
G-vTAP Agent
Subnet CIDRs
(ex: 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24)
IP Ranges (optional)
(ex: 10.0.0.1-10.0.0.9, 10.0.0.101-10.0.0.109)
Tunnel Type
VXLAN
Tunnel MTU
1400
Secure Mirror Traffic
G-vTAP Controller
IP Addresses
(ex: 10.0.0.1, 10.0.0.2, 10.0.0.3)
V Series Controller
IP Addresses
(ex: 10.0.0.1, 10.0.0.2, 10.0.0.3)
V Series Node
IP Addresses
(ex: 10.0.0.1, 10.0.0.2, 10.0.0.3)
Tunnel MTU
1400
Gateway IP (optional)
Gateway IP Address
Tool Subnet CIDR
(ex: 10.0.0.1/24)
Additional Subnet CIDRs (optional)
(ex: 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24)

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.
G-vTAP Agent	
Subnet CIDRs	The CIDR of the G-vTAP Agent.
IP Ranges (optional)	IP range of the G-vTAP Agent. This is optional.
Tunnel Type	Tunnel type for carrying the mirrored traffic from the G-vTAP Agents to the GigaVUE V Series nodes. The tunnel type can be: • L2GRE • VXLAN
Tunnel MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP Agent to the GigaVUE V Series node. For GRE, the default value is 9001. For VXLAN, the default value is 8951. NOTE: The G-vTAP Agent tunnel MTU should be 50 bytes less than the agent's destination interface MTU size. If Secure Mirror Traffic option is enabled, then to minimize fragmentation you must configure MTU value for G-vTAP Agent.
Secure Mirror Traffic	Check box to establish secure tunnel between G-vTAP Agents and GigaVUE V Series nodes.
G-vTAP Controller	
IP Addresses	IP address of the G-vTAP controller
V Series Controller	
IP Addresses	IP address of the GigaVUE Cloud Suite V Series controller
V Series Node	
IP Addresses	IP address of the GigaVUE Cloud Suite V Series node
Tunnel MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the GigaVUE V Series node to the destination.
Gateway IP (optional)	IP address of the Gateway. This field is optional.
Tool Subnet CIDR	CIDR of the tool subnet
Additional Subnet CIDRs (optional)	Additional subnet CIDR

4. Click **Save**.

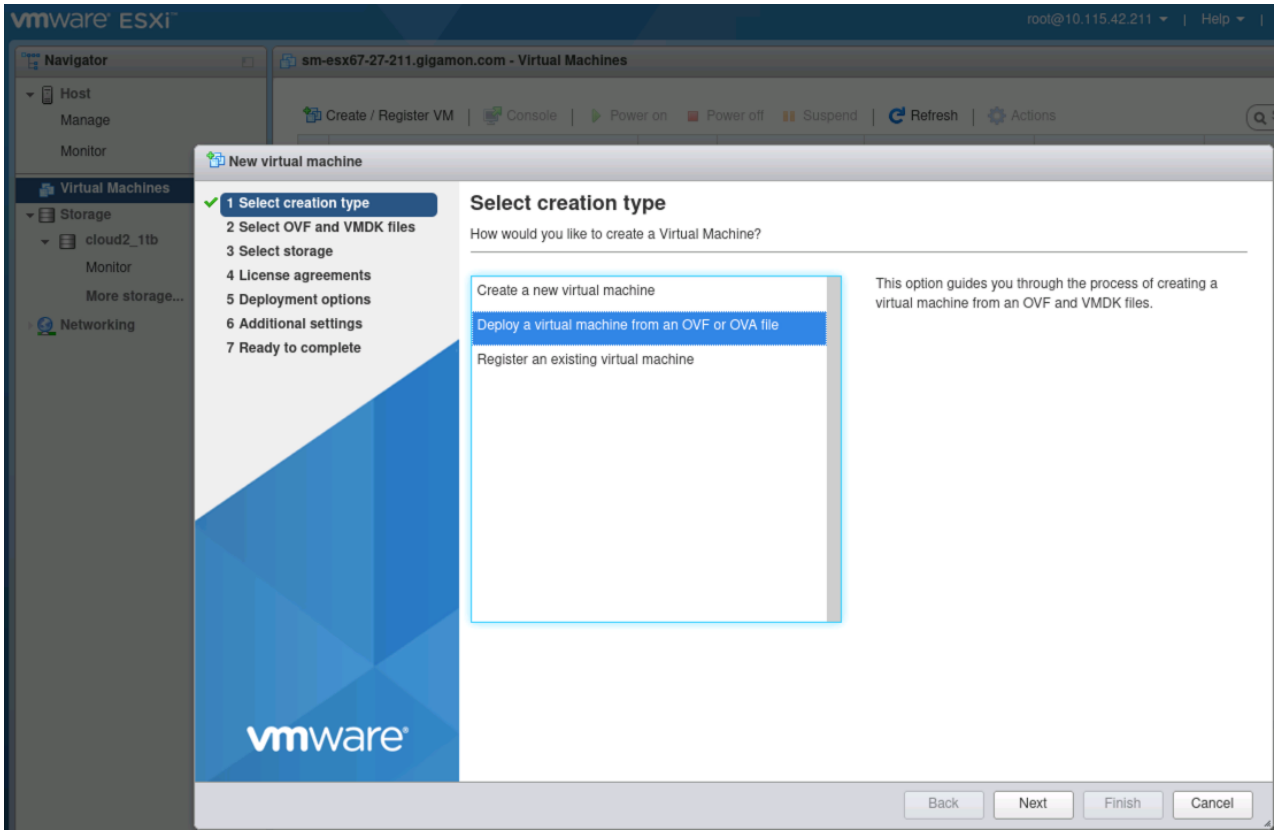
Configure GigaVUE V Series Nodes using VMware ESXi

You can use your own VMware ESXi host system to deploy GigaVUE V Series nodes and use GigaVUE-FM to configure the advanced features supported by these nodes. These nodes register themselves with GigaVUE-FM using the information provided by the user in the virtual machine creation wizard. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

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

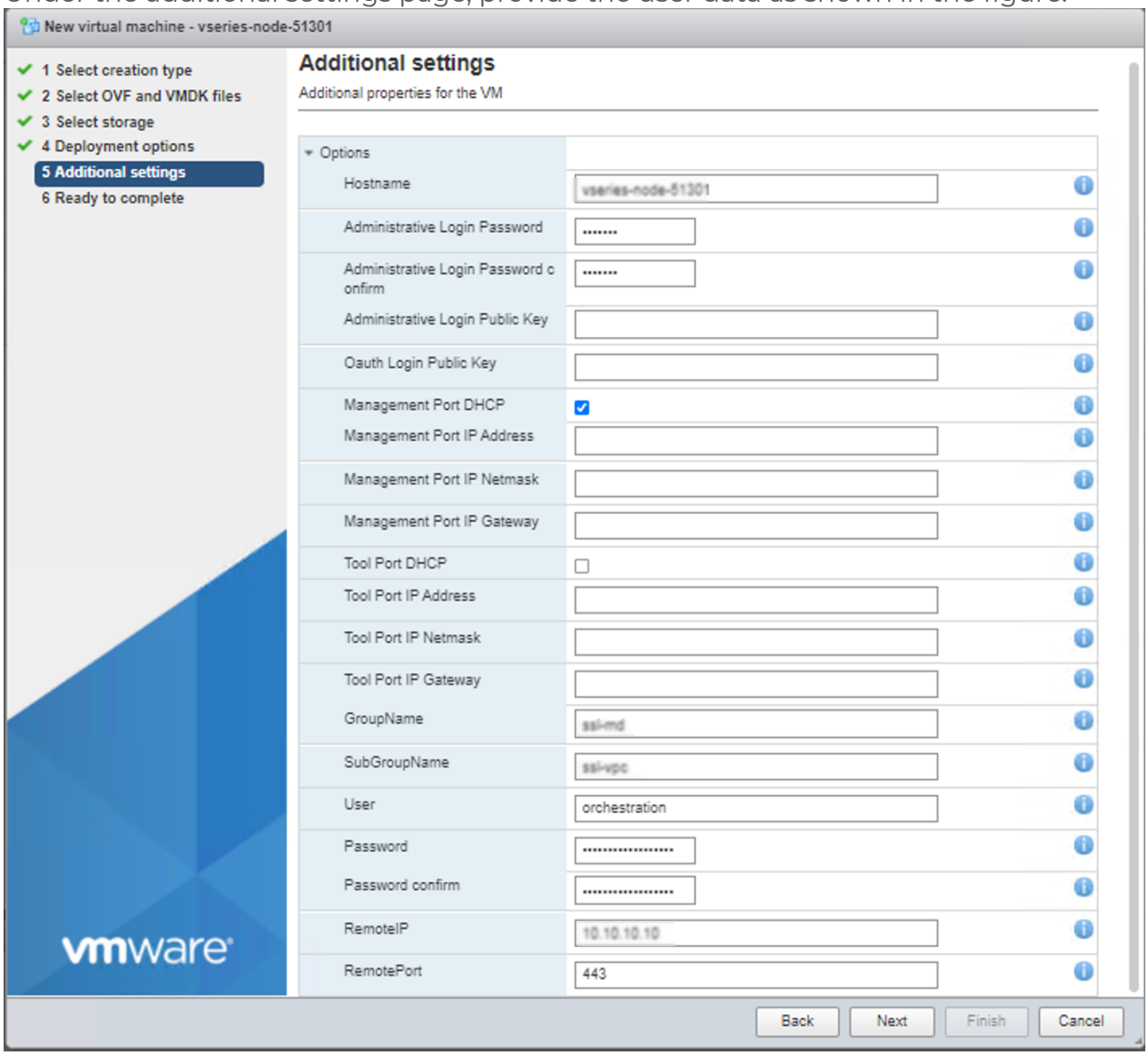
- The nodes will be deployed under the Monitoring Domain created in AnyCloud.
- When registering GigaVUE V Series nodes in GigaVUE-FM, the connection name under each monitoring domain must be unique.

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 page appears.



3. On the New Virtual Machine page, click on **Select Creation Type** from the left navigation pane. Then, select **Deploy a Virtual Machine from an OVF or OVA file**.
4. On the left navigation pane, click on **Select OVF and VMDK files**. Provide virtual machine name and upload the ova file.
5. Click on **Select Storage**, to choose the storage type and data store.
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: Description: orchestration
- Password: orchestration123A!
- remoteIP: <IP address of the GigaVUE-FM>
- remotePort: 443

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

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

Configure and Manage Resources

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.

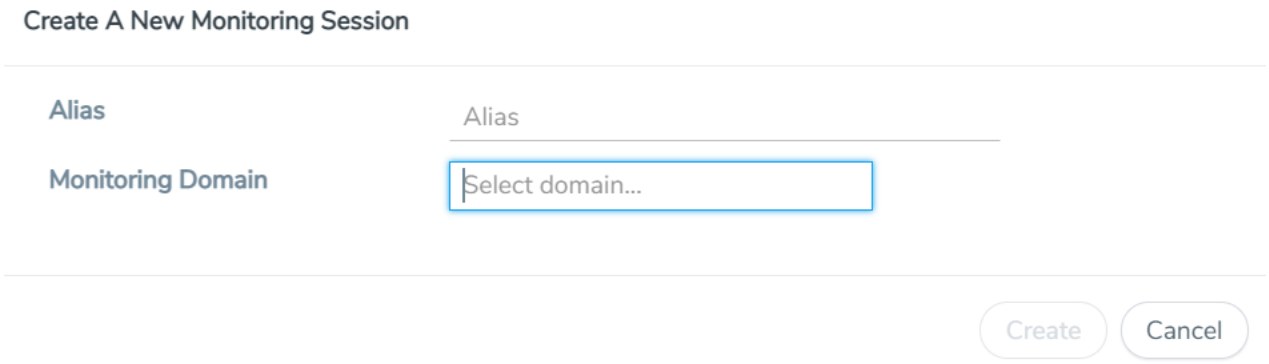
To design your monitoring session, refer to the following sections:

- Create a Monitoring Session
- Create Tunnel Endpoint
- Create a New Map
- Add Applications (GigaVUE V Series 2)
- Add Applications (GigaVUE V Series 1)
- Deploy Monitoring Session
- Add Header Transformations
- View Monitoring Session Statistics
- Visualize the Network Topology

Create a Monitoring Session

To create a new session:

1. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > AnyCloud**. The Monitoring Session page appears.
2. In the Monitoring Session page, click **New**. The **Create a New Monitoring Session** window appears.



3. Enter the appropriate information in the Monitoring Session Info as described in the following table.

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

4. Click **Create**.

Create Tunnel Endpoint

The customized traffic from the GigaVUE Cloud Suite 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 Cloud Suite V Series node. Choose **Out** for creating a tunnel from the GigaVUE Cloud Suite V Series node to the destination endpoint. NOTE: Traffic Direction **In** is not supported in the current release.
Remote Tunnel IP	The IP address of the tool. NOTE: You cannot create two tunnels from a GigaVUE Cloud Suite 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**.

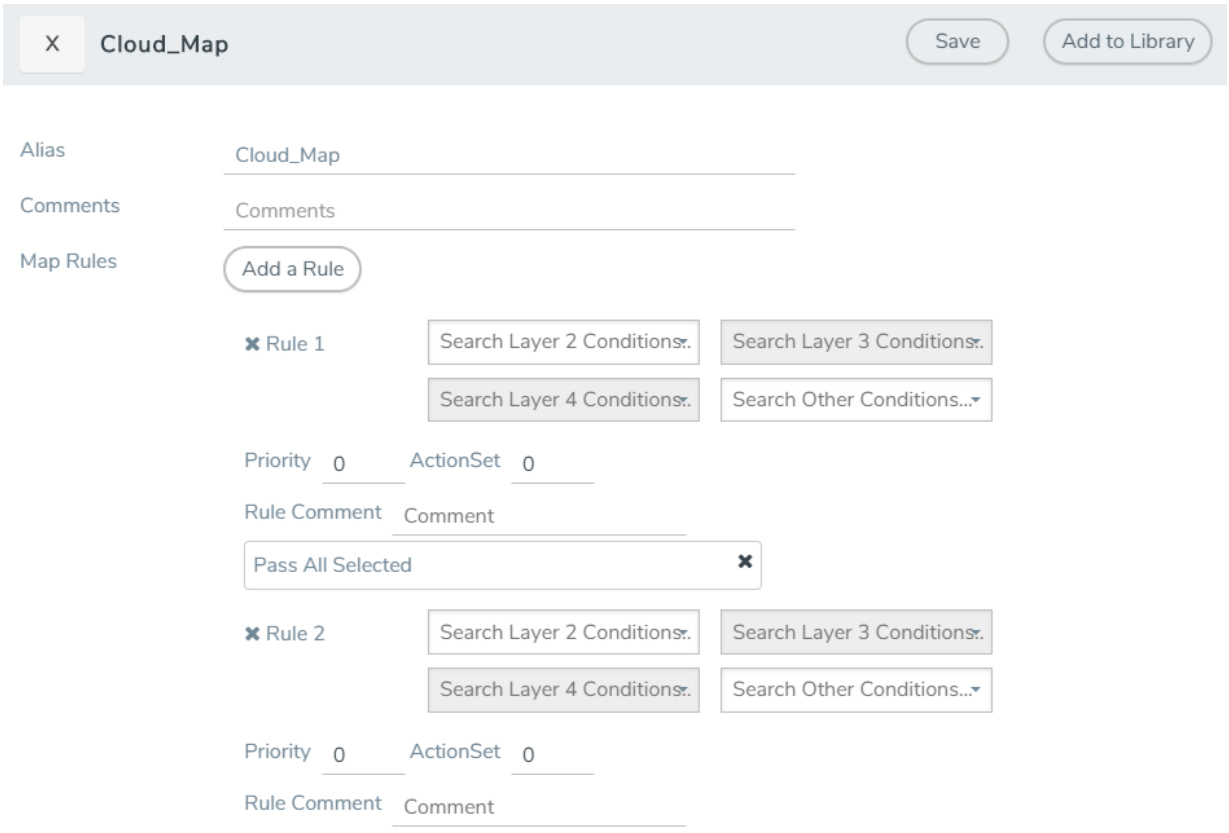
Create a New Map

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

Conditions	Description
L2, L3, and L4 Filters	
EtherType	The packets are filtered based on the selected ethertype. The following conditions are displayed: ▪ IPv4 ▪ IPv6 ▪ ARP ▪ RARP ▪ Other **L3 Filters** If you choose IPv4 or IPv6, the following L3 filter conditions are displayed: ▪ Protocol ▪ 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 VMs matching the specified source MAC address is selected.
MAC Destination	The ingress traffic from the VMs 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.



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

To create a new map:

1. In the Monitoring Session canvas, from **Maps** section, drag and drop a new map template to the workspace. If you are creating an exclusion or inclusion map, drag and drop a new map template to their respective section at the bottom of the workspace. The new map page is displayed.

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

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

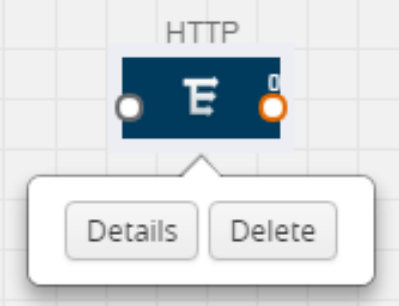
NOTE: Do not create duplicate map rules with the same priority.

3. To reuse the map, click **Add to Library**. Save the map using one of the following options:
   - Select an existing group from the **Select Group** list and click **Save**.
   - Enter a name for the new group in the **New Group** field and click **Save.**

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

4. Click **Save**.

To edit or delete a map, click a map and select **Details** to edit the map or **Delete** to delete the map as shown in the following figure.



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

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

Agent Pre-filtering

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

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

Agent Pre-filtering Guidelines

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

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

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

Agent Pre-filtering Capabilities and Benefits

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

- The agent pre-filtering option can be enabled or disabled at the monitoring-session level and is enabled by default.
- When enabled, traffic is filtered at the G-vTAP Agent-level, before mirroring to the V Series Nodes. Consequently, traffic flow to the V Series Nodes is reduced, which reduces the load/cost on the Cloud networks.
- Only rules from first-level maps are pushed to the agents.
- Pass rules are supported 100%.
- Drop rules are only supported for simple cases.
- Rules that span all monitoring sessions will be merged for an G-vTAP Agent, if applicable.
- If the max-rule limit of 16 is reached, then all the traffic is passed to the V Series node; no filtering will be performed.

Enable/Disable G-vTAP Agent Pre-filtering

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

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

1. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > AnyCloud**. The Monitoring Session page appears.
2. Click the check box of a monitoring session and then click **Edit** to edit an existing session.
3. Select or deselect the **Agent Pre-filtering** check box in the Monitoring Session info box to change the setting. It is enabled by default.
4. Click **OK**.
5. The Monitoring Session view displays the setting in the Agent Pre-filtering column.

Add Applications (GigaVUE V Series 2)

GigaVUE Cloud Suite with V Series 2 node supports the following GigaSMART applications:

- Slicing
- Masking
- Dedup
- Passive SSL Decryption

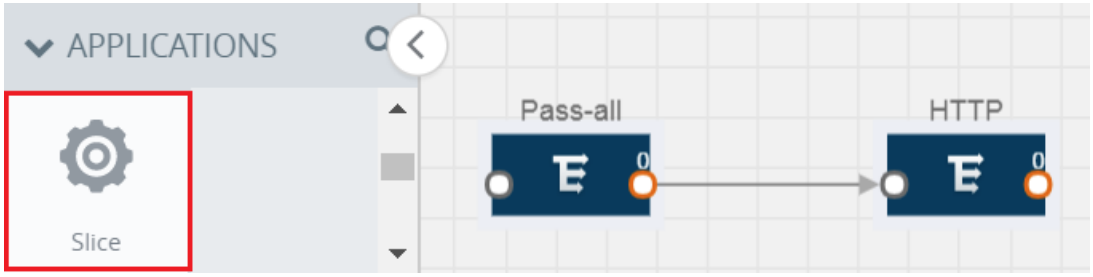
You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools.

Slicing

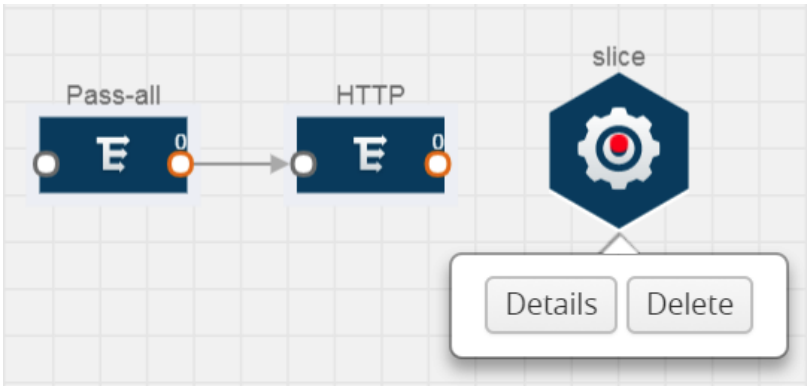
Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes.

To add a slicing application:

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



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



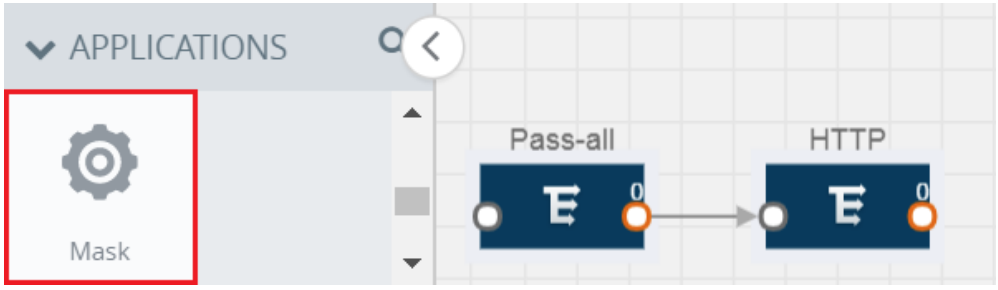
3. In the **Alias** field, enter a name for the slice.
4. For State, select **On** or **Off** check box to enable or disable slicing. The state can be changed at a later time whenever required.
5. In the Slice Length field, specify the length of the packet that must be sliced.
6. From the Protocol drop-down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

Masking

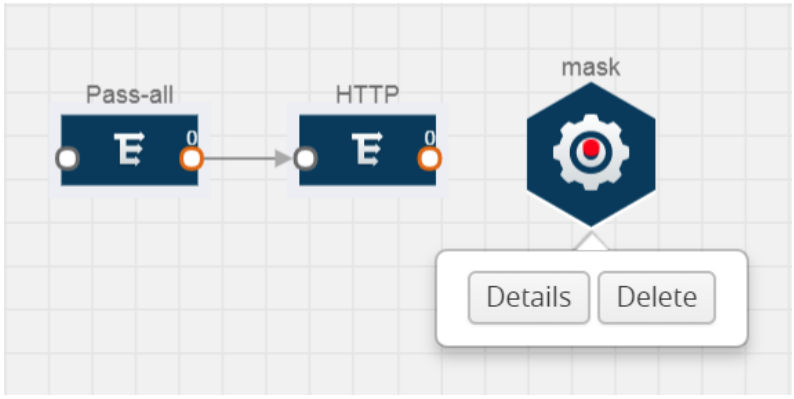
Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.

To add a masking application:

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



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



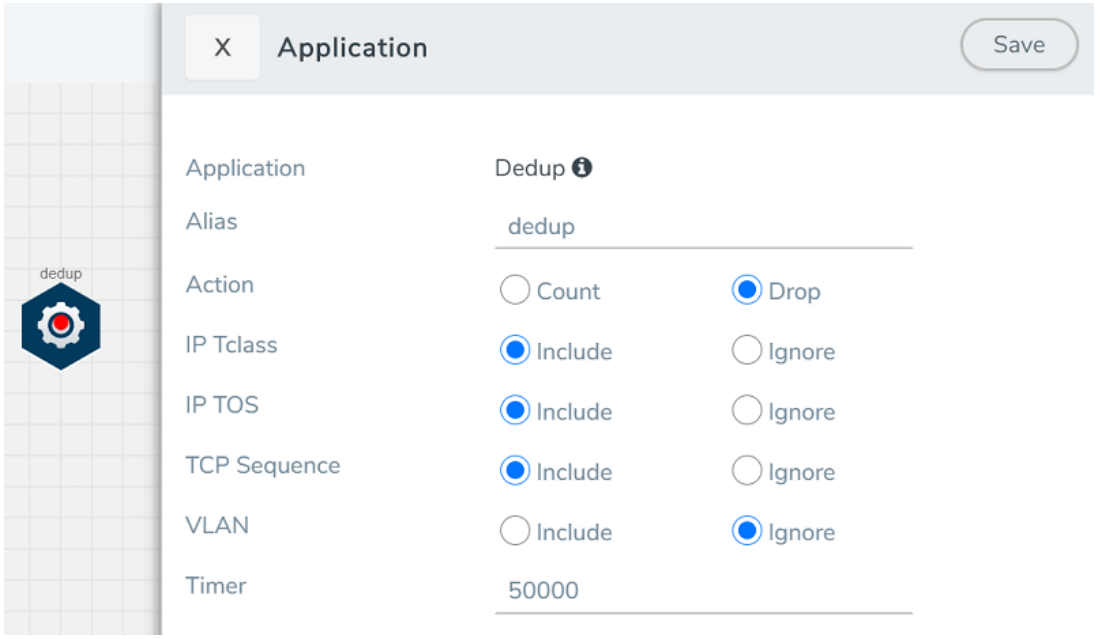
3. In the **Alias** field, enter a name for the mask.
4. For State, select **On** or **Off** check box to enable or disable masking. The state can be changed at anytime whenever required.
5. In the Mask offset field, enter the offset from which the application should start masking data following the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

Dedup

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

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.



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

Passive SSL Decryption

GigaVUE V Series 2 nodes support Secure Sockets Layer (SSL) decryption. SSL is a cryptographic protocol that adds security to TCP/IP communications such as Web browsing and email. The protocol allows the transmission of secure data between a server and client who both have the keys to decode the transmission and the certificates to verify trust between them. Passive SSL decryption delivers decrypted traffic to out-of-band tools that can then detect threats entering the network.

NOTE: Passive SSL Decryption is called as SSL Decrypt on GigaVUE V Series 2.

Licensing

GigaSMART Passive SSL Decryption on V Series 2 follows Volume Based License. (VBL).

Volume Based License (VBL)

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

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

Configure Passive SSL Decryption on V Series 2

To configure passive SSL Decryption on V Series 2, follow the steps given below:

Prerequisite: Register the nodes on the Monitoring Domain. Refer Configure GigaVUE V Series Nodes using VMware ESXi for more detailed information.

Upload SSL Keys

To upload an SSL private key, do the following:

1. On the left navigation pane, select **Inventory >Resources > Security** to open the Security page. Select SSL Keys on the top navigation bar.
2. Click **Add**. The **Create SSL Key** page appears.
3. In the **Create SSL Key** page, enter the following details:
   - For **Alias**, enter an alias for the SSL key.
   - For **Description**, enter any additional information for the SSL key.
   - For **Key Upload Type**, select **PEM** or **PKCS12**.
   - (optional) For **Passphrase**, enter a passphrase for the key.
   - Select a **Private Key** by pasting the copied key in PEM format or installing from URL or installing from local directory.
   - Select a **Certificate** by pasting the copied key in PEM format or installing from URL or installing from local directory.

     NOTE: Install from URL option only supports scp protocol.
4. Click **Save**.

NOTE: Passive SSL Decryption on V Series 2 does not support HSM.

Delete SSL Keys

To delete a particular SSL key select the key on the SSL Keys page, and then select Delete. To delete all SSL Keys, select the **Delete All** button.

Create SSL Service

After you have uploaded a private key, you can add a service. A service maps to a physical server, such as an HTTP server. One server can run multiple services. A service is a combination of an IP address and a server port number. Also, the key and the service must be tied together. Refer to *Configuring SSL Decryption Examples* for examples.

Prerequisites

Before creating a service, you must do the following:

- Upload a private key as described in Upload SSL Keys

To create a service, do the following:

1. On the left navigation pane, select **Inventory >Resources > Security** to open the Security page. Select SSL Service on the top navigation bar.The SSL Services page appears.
2. Click **Add**.
3. On the SSL Service configuration page, do the following:
   - Enter an alias.
   - Enter the information for the service: Server IP Address, Server Port.
4. Click **Save**.

Delete SSL Service

To delete a particular SSL service select the service on the SSL Services page, and then select Delete. To delete all SSL services, select the **Delete All** button.

Notes about Private Keys and Passwords

Consider the following notes about private keys and passwords:

- Encrypted private keys are stored on the node. When a private key is uploaded, it is encrypted with a password before it is stored, therefore keys are password-protected. Keychain passwords are not stored on the node.
- Because only encrypted private keys are stored on the node and because the keychain password is not stored on the node, after any node reboot you will be prompted to enter the password. Until the password is entered, Passive SSL decryption is not working.
- Key content cannot be displayed.
- Keys that are synchronized across a cluster are encrypted.

Key Mapping

After adding the SSL Service, now you map the private key with the service using Key Mapping.

To map a key with the service, follow the steps given below,

1. On the left navigation pane, select **Inventory >Resources > Security** to open the Security page. Select **SSL Key Mapping** on the top navigation bar.
2. Click **Add**.
3. Enter the Key Mapping Alias.
4. Select the SSL Service and Key Alias from the drop-down.
5. Click **Save**.

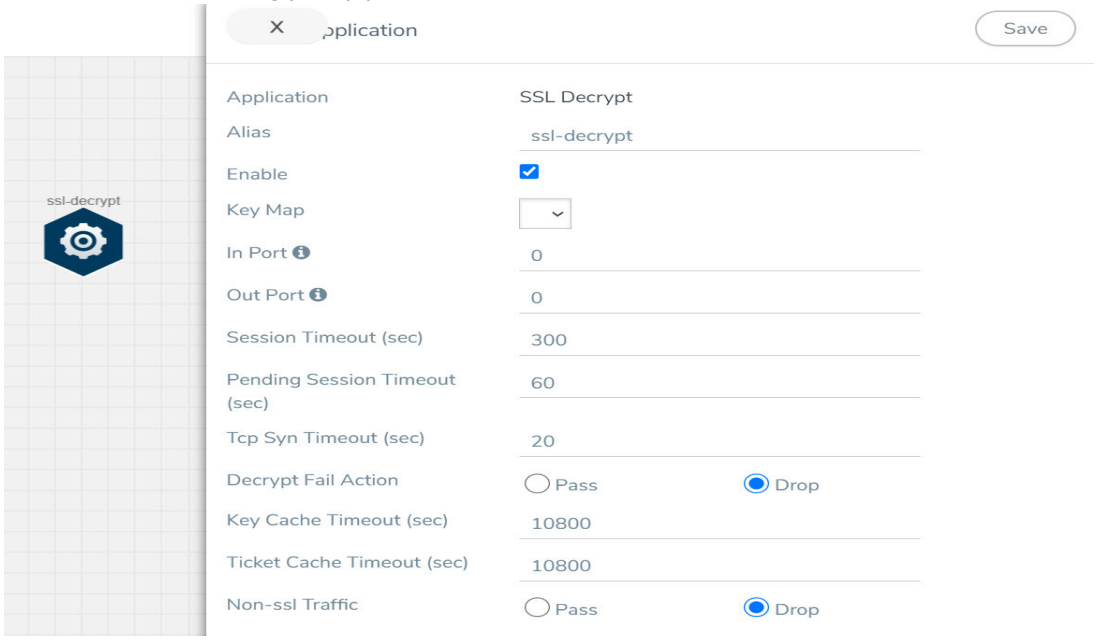
Delete SSL Key Mappings

To delete a particular SSL key map select the key mapping on the SSL Key Mapping page, and then select Delete. To delete all SSL Key Mapping, select the **Delete All** button.

Add SSL Decrypt to Monitoring Session

After mapping your keys with service, to add GigaSMART applications to V series 2, follow the steps given below,

1. Create a new monitoring session. Refer to Create a Monitoring Session for more detailed instructions.
2. Drag and drop **SSL Decrypt** from APPLICATIONS to the graphical workspace.
3. Click the SSL Decrypt application and select **Details**.



4. Select the **Enable** checkbox to enable the application.
5. Select the **Key Map** (created in the previous step) from the drop-down.
6. Click **Save**.
7. Click **Deploy**. The Select nodes to deploy the monitoring session page appears.
8. Select the nodes you want to deploy and select an interface for each node. Then, click **Deploy**.

View Application Statistics

After adding SSL Decrypt to the monitoring session, to view the application statistics, open the **Monitoring Session Statistics** page. Refer to View Monitoring Session Statistics for more detailed information.

1. Click **View Monitoring Session Diagram**. The monitoring session diagram appears, click the SSL Decrypt application.
2. The ssl-decrypt application statistics page appears.
3. You can view the following in the SSL application statistics page:
   - **Application**: The application statistics are displayed here.
   - **Sessions**: To view the session summary and session details of the SSL Decryption application, select the V Series Node IP and enter the Server Name and Client/ Server IP address. Then click Apply.
   - **Server Certificates**: To view the server certificate statistics, select the V Series Node IP from the drop-down and enter the Key Alias. Then, click Apply.
   - **Services**: All the service related statistics are displayed here. To view the statistics, select the V Series Node IP and the Service Alias from the drop-down and click Apply.
   - **Error Codes**: The error messages are displayed here.

Server Certificates, Services and Error Codes pages has **Refresh** and **Reset** button, which helps you to refresh and reset the statistics.

Add Applications (GigaVUE V Series 1)

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

- Sampling
- Slicing
- Masking
- NetFlow
- Dedup

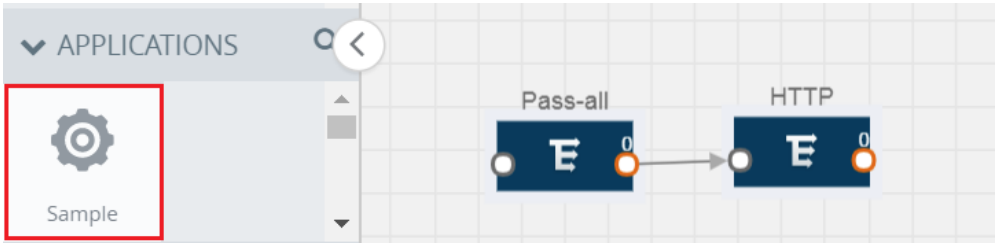
You can optionally use these applications to optimize the traffic sent from your instances to the monitoring tools.

Sampling

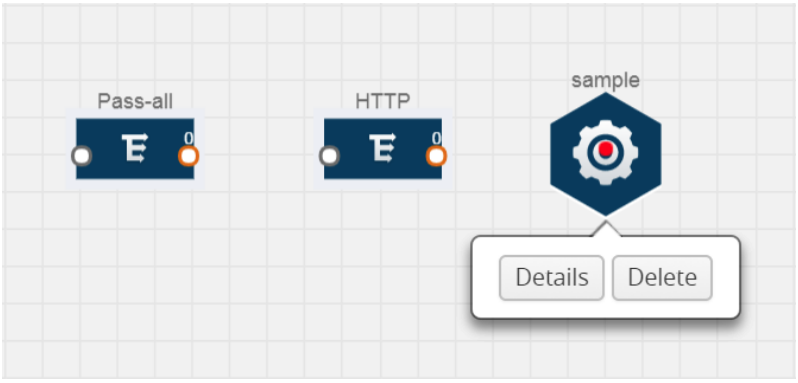
Sampling lets you sample the packets randomly based on the configured sampling rate and then forwards the sampled packets to the monitoring tools.

To add a sampling application:

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



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



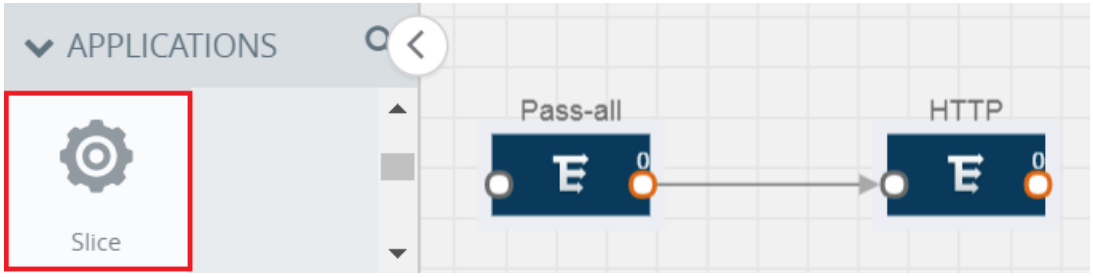
3. In the **Alias** field, enter a name for the sample.
4. For State, select the **On** check box to determine that the application is sampling packets randomly. Select the **Off** check box to determine that the application is not currently sampling the packets. The state can be changed at anytime whenever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

Slicing

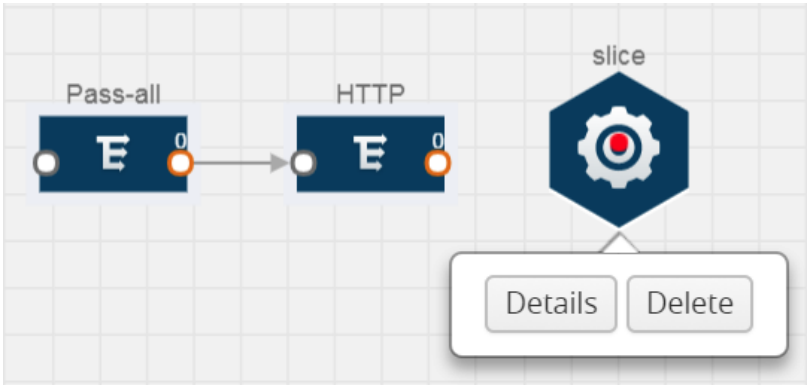
Packet slicing lets you truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes.

To add a slicing application:

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



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



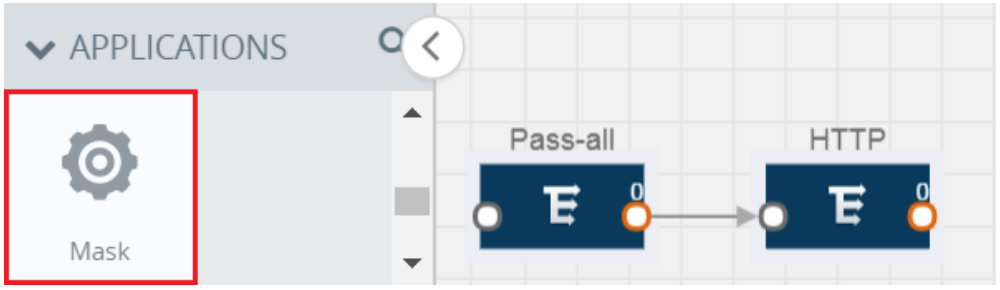
3. In the **Alias** field, enter a name for the slice.
4. For State, select **On** or **Off** check box to enable or disable slicing. The state can be changed at a later time whenever required.
5. In the Slice Length field, specify the length of the packet that must be sliced.
6. From the Protocol drop-down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

Masking

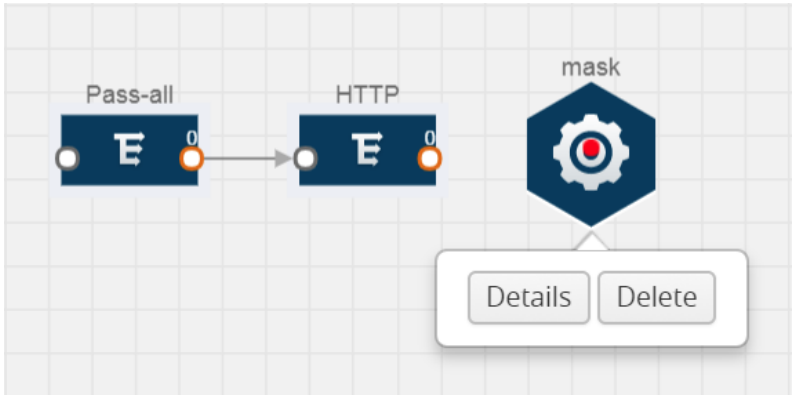
Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis.

To add a masking application:

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



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



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

NetFlow

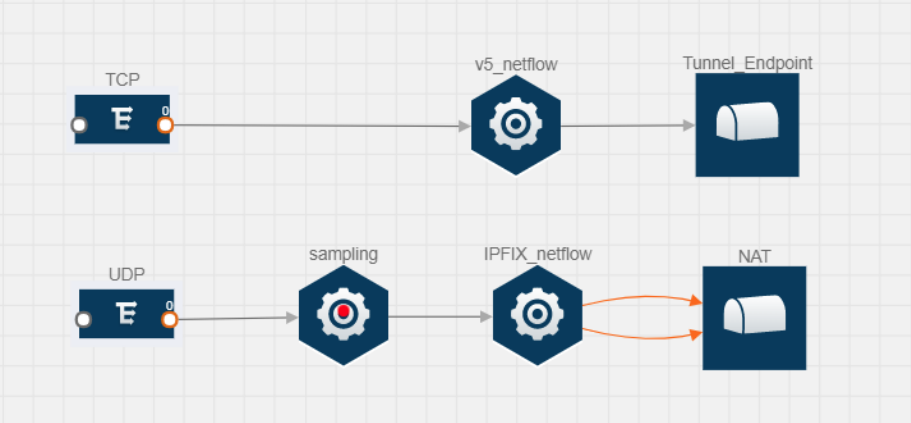
NetFlow collects IP network traffic on all interfaces where NetFlow monitoring is enabled. It gathers information about the traffic flows and exports the NetFlow records, which includes data and templates, to at least one NetFlow collector. The application that serves as a NetFlow collector receives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

The following are the key benefits of NetFlow application:

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

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

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



The NetFlow record generation is performed on GigaVUE Cloud Suite V Series node running the NetFlow application. In Add Applications (GigaVUE V Series 1), incoming packets from G-vTAP Agents are sent to the GigaVUE Cloud Suite V Series node. In the GigaVUE V Series node, one map sends the TCP packet to the version 5 NetFlow application. Another map sends the UDP packet to a sampling application. The map rules and applications such as slice, mask, and sample can only be applied prior to sending the data to NetFlow.

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

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

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

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

Match/Key Fields

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

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

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

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

Collect/Non-Key Fields

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

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

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

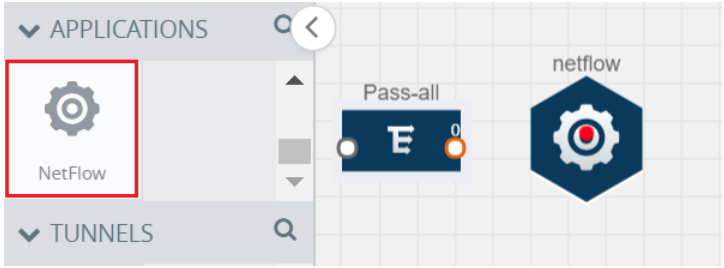
	Description	Supported NetFlow Versions
	message as a non-key field.	
IPv4 Dest IP	Configures the IPv4 destination address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 ICMP Code	Configures the code of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 ICMP Type	Configures the type of the IPv4 ICMP message as a non-key field.	IPFIX
IPv4 Options	Configures the IPv4 options in the packets of the current flow as a non-key field.	IPFIX
IPv4 Src IP	Configures the IPv6 source address in the IP packet header as a non-key field.	v9 and IPFIX
IPv4 Total Length	Configures the total length of the IPv4 packet as a non-key field.	IPFIX
Network		
IP CoS	Configures the IP Class Of Service (CoS) as a key field.	v9
IP Protocol	Configures the value of the protocol number in the IP packet header as a key field.	v9
IP Version	Configures the IP version field in the IP packet header as a key field.	v9
IPv6		
IPv6 Dest IP	Configures the IPv6 destination address in the IP packet header as a key field.	v9
IPv6 Flow Label	Configures the value of the IPv6 flow label field in the IP packet header as a key field.	v9
IPv6 Src IP	Configures the IPv6 source address in the IP packet header as a key field.	v9
Transport		
L4 Dest Port	Configures the destination port identifier in the transport header as a non-key field.	v9 and IPFIX
L4 Src Port	Configures the source port identifier in the transport header as a non-key field.	v9 and IPFIX
TCP AcK Number	Configures the acknowledgment number in the TCP header as a non-key field.	IPFIX
TCP Dest Port	Configures the destination port identifier in the TCP header as a non-key field.	IPFIX
TCP Flags	Configures the TCP control bits observed for the packets of this flow as a non-key field.	v9 and IPFIX
TCP Header Length	Configures the length of the TCP header as a non-key field.	IPFIX
TCP Seq Number	Configures the sequence number in the TCP	IPFIX

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

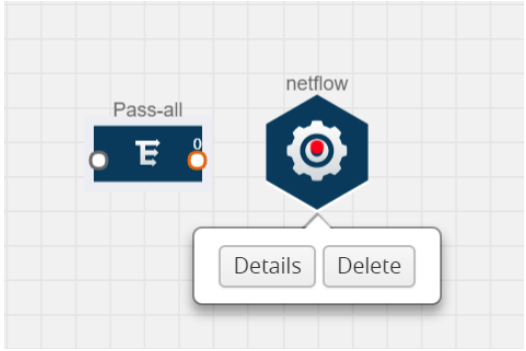
Add Version 5 NetFlow Application

To add a version 5 NetFlow application:

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



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



3. In the **Alias** field, enter a name for the v5 NetFlow application.
4. For State, select the **On** check box to determine that the application is currently running. Select the **Off** check box to determine that the application is currently not running. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select v5.

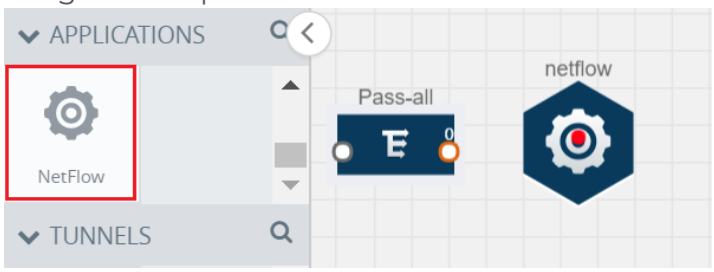
6. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.
7. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.
8. Click **Save**.

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

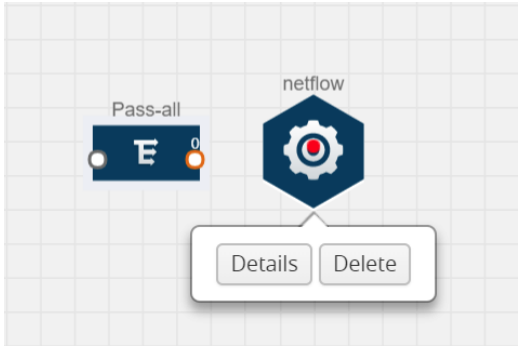
Add Version 9 and IPFIX NetFlow Application

To add a v9 and IPFIX NetFlow application:

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



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



3. In the **Alias** field, enter a name for the NetFlow application.
4. For State, select the **On** check box to determine that the application is generating NetFlow records from the packets coming from the G-vTAP Agents. Select the **Off** check box to determine that the application is not currently generating NetFlow records. The state can be changed at anytime whenever required.
5. From the **NetFlow version** drop-down list, select the version you want to use to generate the NetFlow records. The default version selected is v5.

6. In the **Source ID** field, enter the observation domain to isolate the traffic. The NetFlow application uses source ID to segregate the records into categories. For example, you can assign source ID 1 for traffic coming over TCP. This results in generating a separate NetFlow record for TCP data. Similarly, you can assign Source ID 2 for traffic coming over UDP. This results in generating a separate NetFlow record for UDP data.
7. From the **Match fields** drop-down list, select the parameters that identify what you want to collect from the incoming packets. The Match fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to Match/Key Fields.
8. From the **Collect fields** drop-down list, select the parameters that identify what you want to collect from the NetFlow records. The Collect fields displayed in the drop-down list are based on the NetFlow version selected in step 5. Refer to Collect/Non-Key Fields.
9. In **Active cache timeout**, enter the number of seconds that an active flow record must remain in the cache before it is exported and removed. The default value is 1800 seconds.
10. In **Inactive cache timeout**, enter the number of seconds an inactive flow record must remain in the cache before it times out. The default value is 15 seconds.
11. In **Template refresh interval**, enter the frequency at which the template must be sent to the tool. The default value is 1800 seconds.
12. Click **Save**.

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

Network Address Translation (NAT)

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

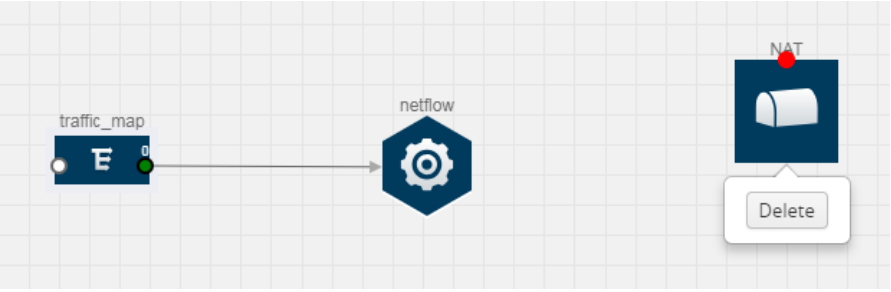
The NetFlow records are exported to the collector over UDP protocol with the configurable source IP and destination IP.

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

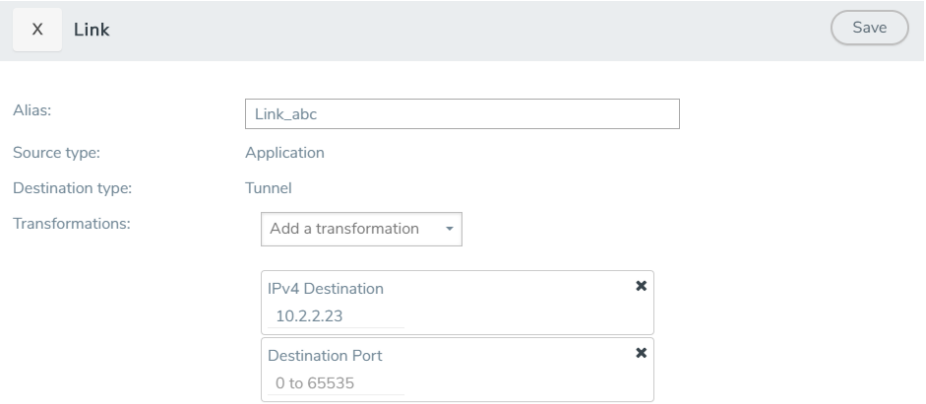
Add NAT and Link NetFlow Application to NAT

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

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



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



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

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

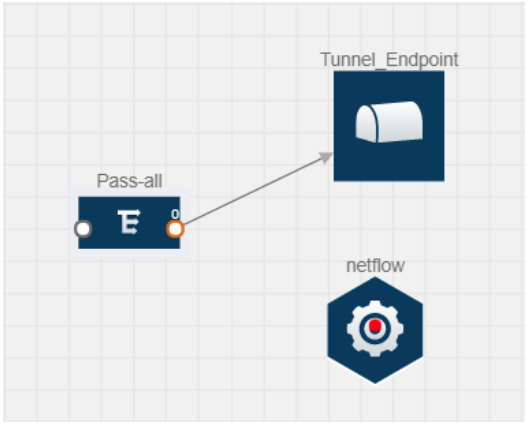
NetFlow Examples

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

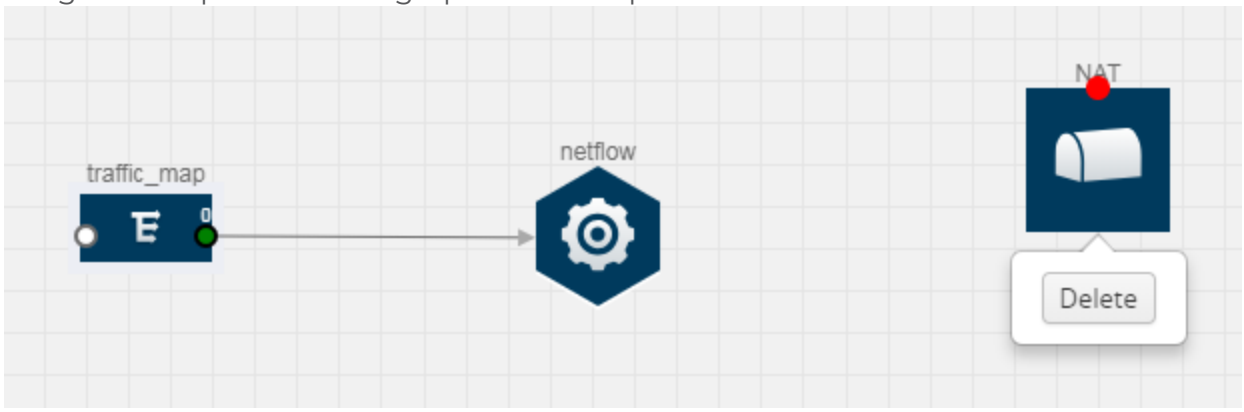
Example 1

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

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



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



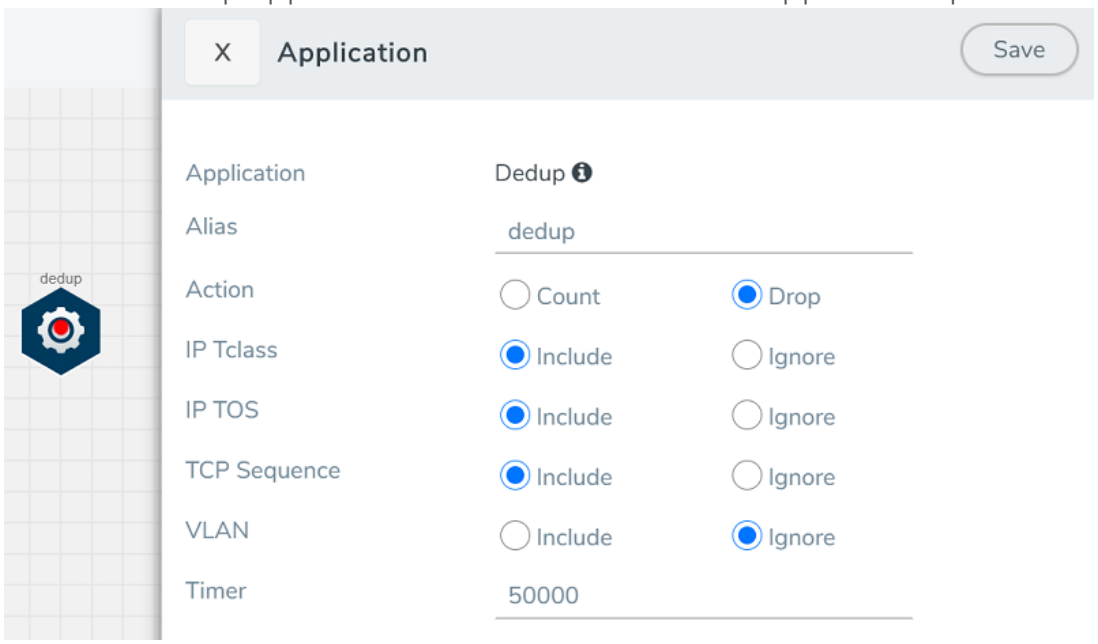
9. Create a link from the v5 NetFlow application to NAT. The link must be configured with the destination IP address of the NetFlow collector and the GigaVUE Cloud Suite V Series node interface. For steps to configure the link, refer to Add Applications (GigaVUE V Series 1).
10. Click on the link created from the v5 NetFlow application to NAT. The information about the NetFlow collector destination IP and port is displayed.

Dedup

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

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.



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

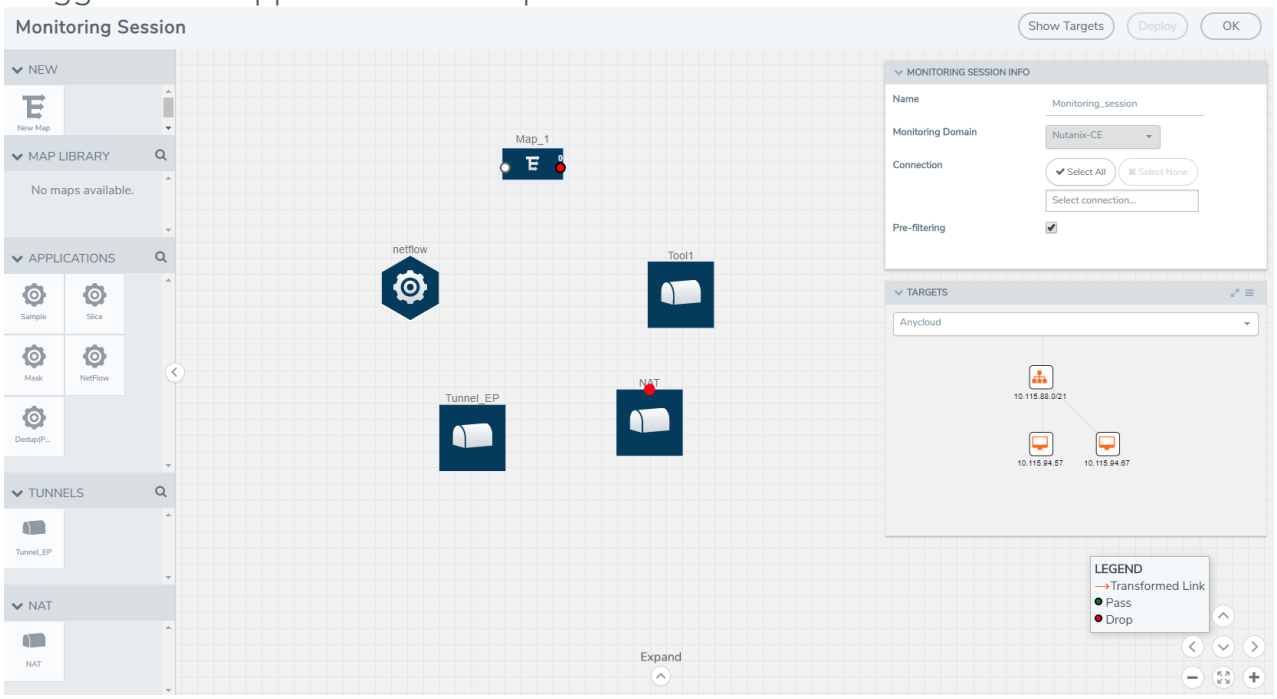
Deploy Monitoring Session

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

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

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

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

Add Header Transformations

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

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

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

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

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

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

Option	Description
MAC Source	Modify the Ethernet source address.
MAC Destination	Modify the Ethernet destination address.
VLAN Id	Specify the VLAN ID.
VLAN PCP	Specify the VLAN priority.
Strip VLAN	Strip the VLAN tag.
IPv4 Source	Specify the IPv4 source address.
IPv4 Destination	Specify the IPv4 destination address.

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

To add a header transformation:

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

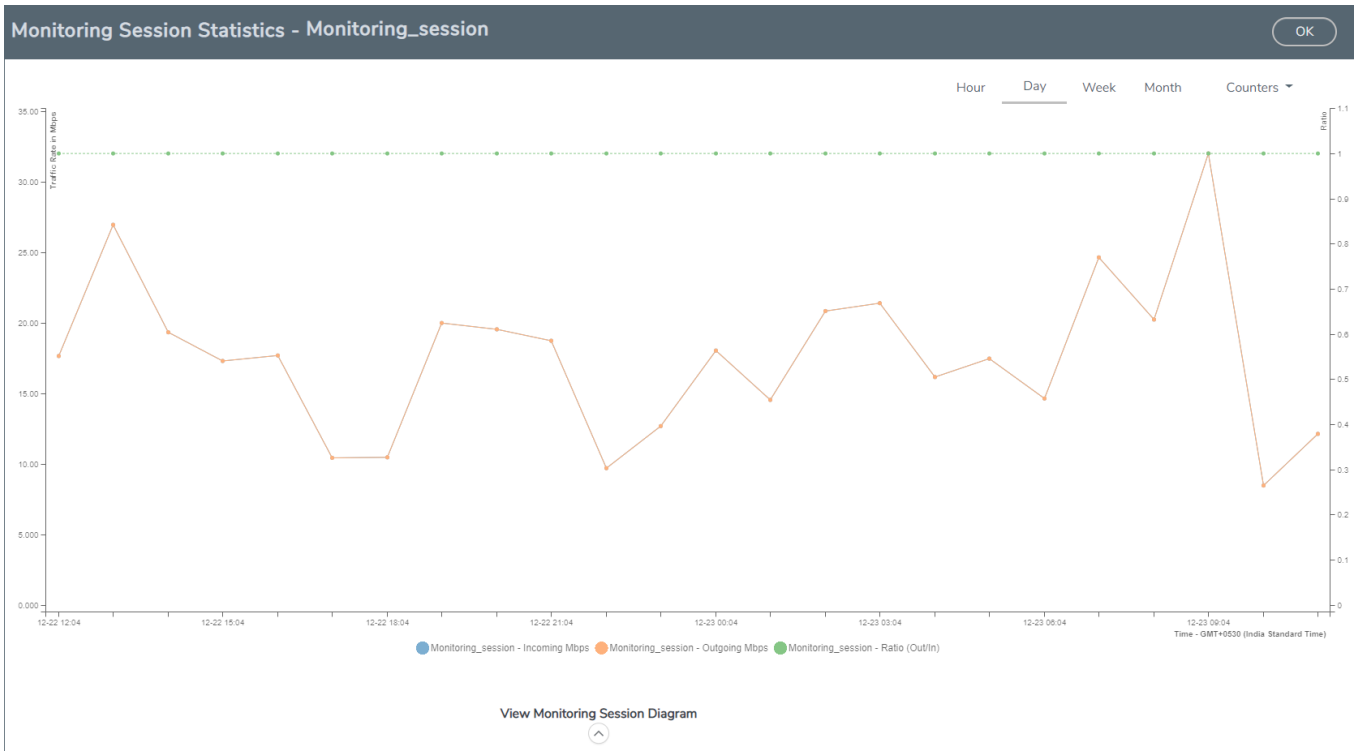
2. From the **Transformations** drop-down list, select one or more header transformations.

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

3. Click **Save**. The selected transformation is applied to the packets passing through the link.
4. Click **Deploy** to deploy the monitoring session.

View Monitoring Session Statistics

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



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

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

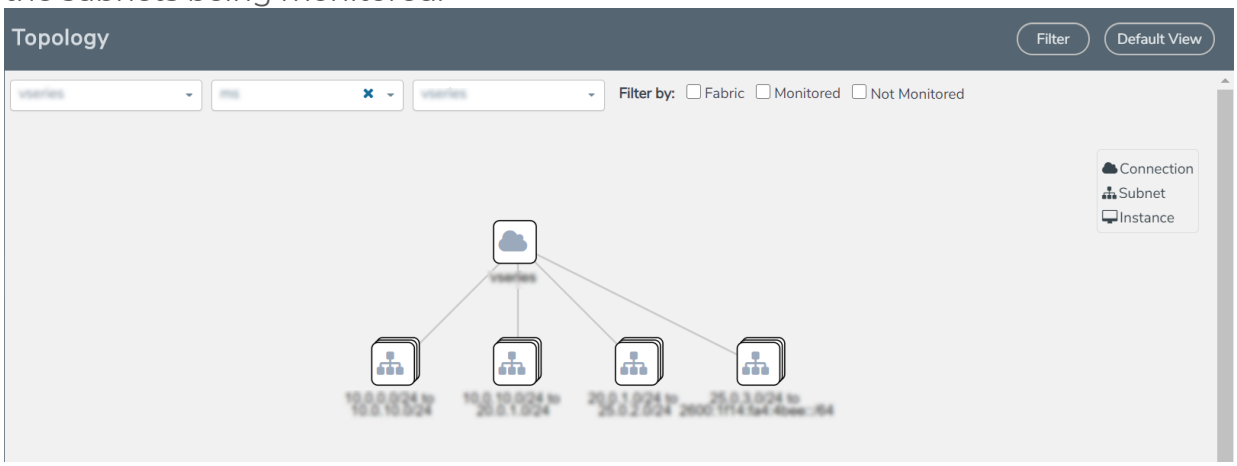
Visualize the Network Topology

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:

1. From the left navigation pane, select **Traffic > VIRTUAL > Orchestrated Flows > AnyCloud**. The Monitoring Session page appears.
2. Select **Topology** tab.
3. Select a connection from the **Select connection...** list. The topology view of the subnets and instances is displayed.

4. (Optional) Select a monitoring session from the **Select Monitoring Session...**list. The topology view of the monitored subnets and instances in the selected session are displayed.
5. Select one of the following check boxes:
   - **Source**: Displays the topology view of the source target interfaces that are being monitored.
   - **Destination**: Displays the topology view of the destination target interfaces where the traffic is being mirrored.
   - **Other**: Displays the topology view of the VMs installed with G-vTAP Agents within the subnets being monitored.



6. (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.

Administer GigaVUE Cloud Suite for AnyCloud

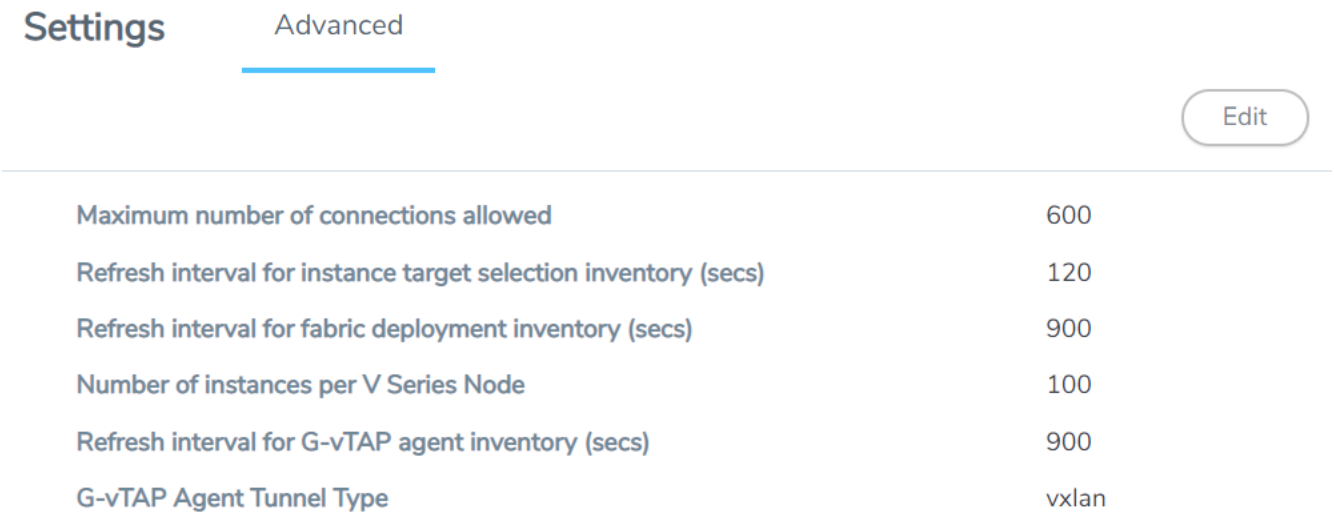
You can perform the following administrative tasks:

- Configure AnyCloud Settings
- Role Based Access Control

Configure AnyCloud 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 > AnyCloud > Settings** to edit the AnyCloud settings.



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

Settings	Description
Maximum number of connections allowed	Specifies the maximum number of connections you can establish in GigaVUE-FM.
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of Virtual Machines.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for updating the state of non-instance information such as subnets, security groups, images, and VMs.
Number of instances per GigaVUE Cloud Suite V Series Node	Specifies the maximum number of instances that can be assigned to the GigaVUE Cloud Suite V Series node.
Refresh interval for G-vTAP Agent inventory (secs)	Specifies the frequency for discovering the G-vTAP Agents available.
G-vTAP Agent Tunnel Type	Specifies the tunnel type of the G-vTAP Agent.

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 Configurations • Sys Dump • Syslog • Cloud licenses • Cloud Inventory	• Configure GigaVUE Cloud Components • Create Monitoring Domain and Launch Visibility Fabric
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

V Series 2 is supported only for fabric components deployed using third-party orchestration.

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Proxy	GigaVUE V Series 2 Nodes
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

GigaVUE-FM Version Compatibility for V Series 1 Configuration

GigaVUE-FM	G-vTAP Agent Version	G-vTAP Controller Version	GigaVUE V Series Controller	GigaVUE V Series 1 Nodes
5.15.00	v1.8-5	v1.8-5	v1.7-1	v1.7-1
5.14.00	v1.8-4	v1.8-4	v1.7-1	v1.7-1
5.10.01, 5.11.00, 5.11.01, 5.12.00, 5.13.00, 5.13.01, 5.14.00	v1.7-1	v1.7-1	v1.7-1	v1.7-1

Additional Sources of Information

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

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

Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 5.15 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
G-TAP A Series 2 Installation Guide
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON

GigaVUE Cloud Suite 5.15 Hardware and Software Guides
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
Administration
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
Fabric Management
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Configuration and Monitoring how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 2 Guide
GigaVUE Cloud Suite for AWS–GigaVUE V Series 1 Guide
GigaVUE Cloud Suite for Azure Guide
GigaVUE Cloud Suite for OpenStack Guide
Gigamon Containerized Broker Guide
GigaVUE Cloud Suite for VMware—GigaVUE V Series Guide
GigaVUE Cloud Suite for AnyCloud Guide
GigaVUE Cloud Suite for Kubernetes Guide
GigaVUE Cloud Suite for Nutanix Guide
GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
GigaVUE Cloud Suite for AWS Secret Regions Guide
Reference
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices

GigaVUE Cloud Suite 5.15 Hardware and Software Guides
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.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

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)

G

Gb

Gb (lower-case b) is defined as Gigabit and is a unit of bandwidth measured. It is the capacity to transfer information.

GB (all caps)

GB (all-caps) means Gigabyte which is a unit of storage capacity of HDD, USB drives, flash drives, SD cards.

L

leader

leader in clustering node relationship (formerly master)

M

member node

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

My Term

My definition

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)