# Gigamon®

# GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

**GigaVUE Cloud Suite**

Product Version: 6.5
Document Version: 1.0
Last Updated: Friday, February 9, 2024

(See Change Notes for document updates.)

# Change Notes

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

| Product Version | Document Version | Date Updated | Change Notes |
|---|---|---|---|
| 6.5.00 | 1.0 | 12/11/2023 | The original release of this document with 6.5.00 GA |

# Contents

# GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)

GigaVUE Cloud Suite for VMware provides an intelligent filtering technology that allows virtual machine (VM) traffic flows of interest to be selected, forwarded, and delivered to the monitoring infrastructure centrally attached to the Gigamon Deep Observability Pipeline, thereby eliminating any traffic blind spots in the enterprise private clouds or service provider NFV deployments.

This guide describes how to install, deploy, and operate the GigaVUE V Series Nodes in VMware.

Topics:

- Overview of GigaVUE Cloud Suite for VMware
- Architecture for GigaVUE Cloud Suite for VMware NSX-T
- Introduction to Supported Features in GigaVUE Cloud Suite for VMware NSX-T
- Volume-Based License
- Supported Hypervisors for VMware
- Points to Note (VMware NSX-T)
- Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T
- Install and Upgrade GigaVUE-FM
- Deployment Options for GigaVUE Cloud Suite for VMware (NSX-T)
- Deploy GigaVUE Cloud Suite for VMware (NSX-T)
- Upgrade GigaVUE V Series Node for VMware NSX-T
- Cloud Overview Page
- Configure Monitoring Session
- Migrate Application Intelligence Session to Monitoring Session
- Monitor Cloud Health
- Configure VMware Settings

# Overview of GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware acquires, optimizes, and distributes selected traffic to your monitoring and security tools. GigaVUE Cloud Suites for VMware provides tight integration with orchestration tools to deliver intelligent network traffic visibility for workloads running in Virtual machine in VMware. GigaVUE-FM , part of the Cloud Suite, works with VMware vCenter to automatically deploy GigaVUE V Series Node to support a growing private cloud infrastructure. GigaVUE-FM leverages dynamic service chaining and workload relocation monitoring to ensure visibility and policy integrity.

GigaVUE Cloud Suite for VMware provides the following benefits:

**Flexible Traffic Acquisition:** Acquires traffic through port mirroring in VMware ESXi.

**Automated Visibility Provisioning:** Dynamically provisions and applies traffic policies as new tenants come on board or as groups scale.

**Increased Tool Efficiency:** Reduces load on tools by selectively filtering, de-duplicating, and load balancing traffic sent to security and performance monitoring tools.

**Application Intelligence solution:** You can use Application Intelligence to identify thousands of applications and utilize over 7,000 application metadata elements.

## Components for GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware comprises multiple elements that enable traffic acquisition, aggregation, intelligence and distribution, along with centralized, single-pane-of-glass orchestration and management. The solution consists of these components:

| 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 Suite for VMware. |
| | GigaVUE-FM generates an end-to-end topology view through a single-pane-of-glass GUI, which gives you insights into which cloud instances are or are not part of the deep observability pipeline. A single instance of GigaVUE-FM can manage hundreds of visibility nodes across on-premises and multi-cloud environments. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform. |
| **GigaVUE® V Series Node** | A visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or back haul to on premise device or tools. |

# Architecture for GigaVUE Cloud Suite for VMware NSX-T

This section provides an overview of the GigaVUE V Series Node deployment on the VMware NSX-T platform and describes the procedure for setting up the traffic monitoring sessions using the GigaVUE V Series Nodes. The GigaVUE V Series Nodes support traffic visibility on the NSX-T NVDS switch.

GigaVUE-FM creates, manages and deletes the GigaVUE V Series Nodes in the VMware NSX-T based on the configuration information provided by the user. GigaVUE-FM can communicate directly with the GigaVUE V Series Nodes.

The following diagram provides a high-level overview of the deployment:
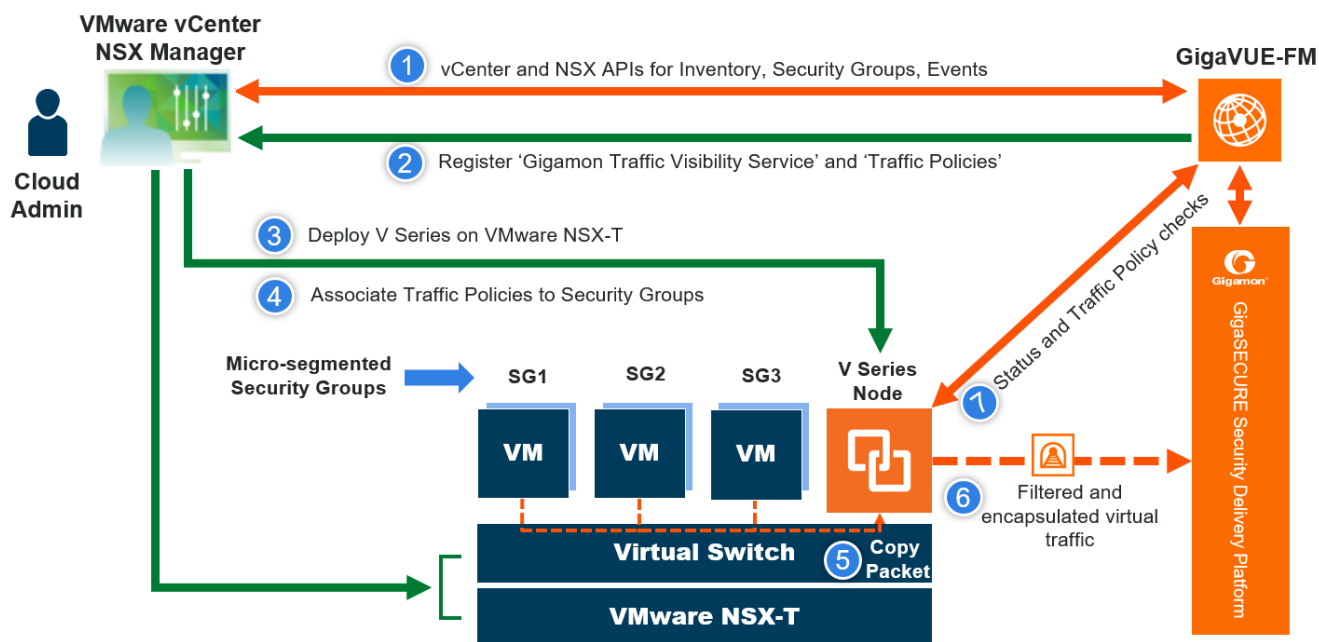
Refer to the following Gigamon Validated Designs for more detailed information:

- Deploying GigaVUE Cloud Suite for VMware NSX-T 3.1.2 using V Series
- Deploying GigaVUE Cloud Suite for VMware NSX-T using V Series
- Deploying GigaVUE Cloud Suite for VMware NSX-T 3.0 using V Series
- Deploying GigaVUE Cloud Suite for VMware NSX-T 2.5.1 using V Series

# Introduction to Supported Features in GigaVUE Cloud Suite for VMware NSX-T

GigaVUE Cloud Suite for VMware (NSX-T) supports the following features:

- Increase or Decrease GigaVUE V Series Node
- Sharing the Same Host across Different Monitoring Domains
- Analytics for Virtual Resources
- Cloud Health Monitoring

## Increase or Decrease GigaVUE V Series Node

You can add more nodes or remove nodes from an existing monitoring domain using GigaVUE-FM or VMware NSX-T manager, based on method you have deployed the GigaVUE V Series Nodes.

Refer to the following topics for more detailed information:

- Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM
- Increase or Decrease GigaVUE V Series Nodes using VMware NSX-T Manager

## Sharing the Same Host across Different Monitoring Domains

GigaVUE-FM has the ability to share a host between VMware ESXi and VMware NSX-T monitoring domain. You can deploy multiple V Series nodes from VMware NSX-T monitoring domain and one V Series Node from VMware ESXi monitoring domain on the same host. This way the workload virtual machines connected to NSX segments can be monitored using the V Series nodes deployed in NSX-T monitoring domain and workload virtual machines connected to regular VSS / VDS networks can be monitored using the V Series node deployed in the ESXi monitoring domain.

> **NOTE:** If a Virtual Machine has NICs attached to both VMware NSX-T segments and ESXi VDS or VSS port groups then GigaVUE-FM cannot provide visibility to those virtual machines in ESXi platform.

## Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects.

Refer to Analytics for Virtual Resources for more detailed information.

## Cloud Health Monitoring

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components.

For more information on how to configure cloud health monitoring, refer to the topic Monitor Cloud Health.

# Volume-Based License

All the GigaVUE V Series Nodes connected to GigaVUE-FM periodically report statistics on the amount of traffic that flows through the V Series Nodes. The statistics provide information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics.

Licensing for Cloud Suite is volume-based. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your V Series Nodes to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes becomes irrelevant for Gigamon's accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility on the actual amount of data, each licensed application is using on each node, and tracks the overuse, if any.

Volume-based licenses are available as monthly subscription licenses with a service period of 1 month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

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

## Base Bundles

In volume-based licensing scheme, licenses are offered as bundles. The following three base bundle types are available:

- CoreVUE
- NetVUE
- SecureVUEPlus

The bundles are available as SKUs[1]. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

### Bundle Replacement Policy

Refer to the following notes:

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

---

[1]Stock Keeping Unit. Refer to the What is a License SKU? section in the FAQs for Licenses chapter.

## Add-on Packages

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

**Rules for add-on packages:**

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

For more information about SKUs refer to the respective Data Sheets as follows:

| GigaVUE Data Sheets |
| --- |
| GigaVUE Cloud Suite for VMware Data Sheet |
| GigaVUE Cloud Suite for AWS Data Sheet |
| GigaVUE Cloud Suite for Azure Data Sheet |
| GigaVUE Cloud Suite for OpenStack |
| GigaVUE Cloud Suite for Nutanix |
| GigaVUE Cloud Suite for Kubernetes |

## How GigaVUE-FM Tracks Volume-Based License Usage

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

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
- When a license goes into grace period, you will be notified with an audit log.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will not be undeployed.

  For releases prior to 6.4:

  - The monitoring sessions using the corresponding license will be undeployed (but not deleted from the database).
  - When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

## Manage Volume-based Licenses

To manage active Volume-based License:

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

   This page lists the following information about the active Volume-based Licenses:

   | Field | Description |
   | --- | --- |
   | SKUs | Unique identifier associated with the license |
   | Bundles | Bundle to which the license belongs to |
   | Volume | Total daily allowance volume |
   | Starts | License start date |
   | Ends | License end date |
   | Type | Type of license (Commercial, Trial, Lab and other license types). |
   | Activation ID | Activation ID |
   | Entitlement ID | Entitlement ID |

   **NOTE:** The License Type and Activation ID are displayed by default in the VBL Active page. To display the Entitlement ID field, click on the column setting configuration option to enable the Entitlement ID field.

   The expired licenses are displayed in the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar. This page lists the following information about the inactive Volume-based Licenses:

   | Field | Description |
   | --- | --- |
   | SKUs | Unique identifier associated with the license. |
   | Bundles | Bundle to which the license belongs to. |
   | Ends | License end date |
   | Grace Period | Number of days the license is in grace period |
   | Deactivation Date | Date the license got deactivated. |
   | Revocation Code | License revocation code. |
   | Status | License status. |

   **NOTE:** The License Type, Activation ID and Entitlement ID fields are not displayed by default in the VBL Inactive page. To display these fields, click on the column setting configuration option and enable these fields.

Use the following buttons to manage your VBL.

| Button | Description |
|---|---|
| Activate Licenses | Use this button to activate a Volume-based License. Refer to Activate Volume-based Licenses for more information. |
| Email Volume Usage | Use this button to send the volume usage details to the email recipients. |
| Filter | Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page. |
| Export | Use this button to export the details in the VBL active page to a CSV or XLSX file. |
| Deactivate | Use this button to deactivate the licenses. You can only deactivate licenses that are in grace period or that have expired. |

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

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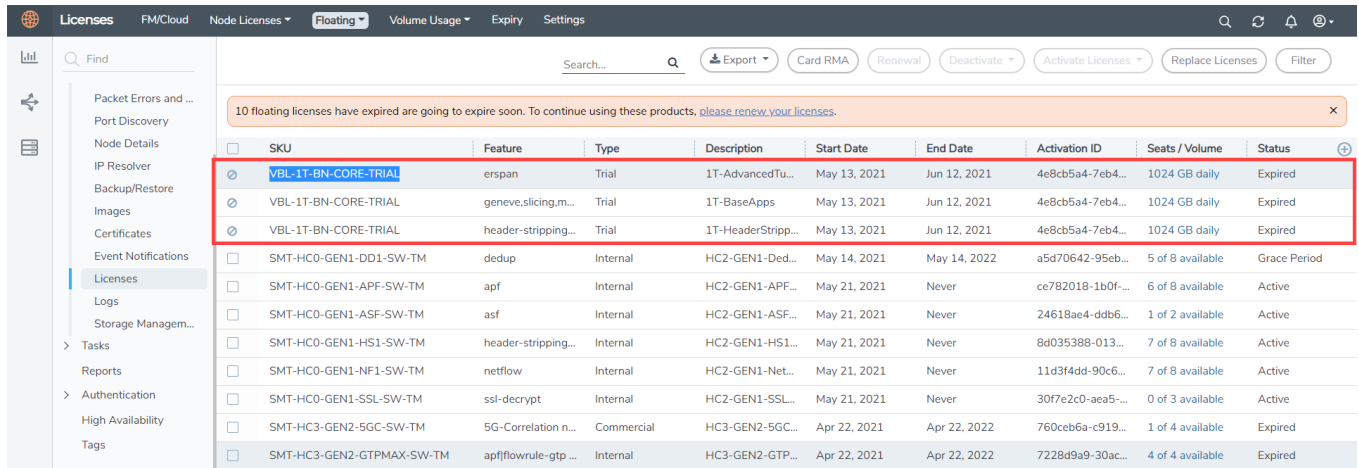
## Activate Volume-based Licenses

To activate Volume-based licenses:

1. On the left navigation pane, click ⚙.
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.
3. Click **Activate Licenses**. The **Activate License** page appears. Perform the following steps:
   a. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the What is a Fabric Inventory File? section for more details.
   b. Navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
   c. Return to GigaVUE-FM and add the additional licenses.

## Default Trial Licenses

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



This license includes the following applications:

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

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

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

## Delete Default Trial Licenses

GigaVUE-FM allows you to deactivate the default trial licenses from this page. To deactivate the license:

1. On the left navigation pane, click ⚙ .
2. Go to **System > Licenses >Floating**. Click **Activated**.
3. Click **Deactivate** > **Default Trial VBL**.

The VBL trial licenses is deactivated and is no longer listed in the Activated page. However, you can view these deactivated licenses from the Deactivated page.

## Supported Hypervisors for VMware

The following table lists the supported hypervisor versions for vCenter, VMware ESXi and VMware NSX-T.

| GigaVUE V Series Node Supported Hypervisors | Tested Platforms | | | |
|---|---|---|---|---|
| | | vCenter Server | \ESXi | GigaVUE-FM |
| vSphere ESXi | v6.7 | v6.7U3 | v6.7U3 | v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01 |
| | v7.0 | v7.0 | v7.0 | v5.10.02, v5.11.01, v5.12.00, v5.13.00, v5.13.01, v5.14.00, v5.15.00, v5.16.00, v6.0.00, v6.1.00 |
| | v7.0 | v7.0U3 | v7.0U3 | v5.15.00, v5.16.00, v6.0.00,v6.1.00, v6.2.00, v6.3.00, v6.4.00, v6.5.00 |
| | v8.0 | v8.0 | v8.0 | v6.3.00, v6.4.00, v6.5.00 |
| vSphere NSX-T | v3.1.0 | v7.0 | v7.0 | v5.11.01, v5.12.00 |
| | v3.1.2 | v7.0 | v6.7U3, v7.0U1 | v5.12.00, v5.13.00, v5.13.01 |
| | v3.1.3 | v7.0 | v6.7U3, v7.0U1 | v5.13.01, v5.14.00, v6.0.00 |
| | v3.2.0 | v7.0, v7.0U3 | v6.7U3, v7.0U1, v7.0U3 | v5.14.01, v5.15.00, v5.16.00, v6.0.00 |
| | v3.2.1 | v7.0U3 | v6.7U3, v7.0U1, v7.0U3 | v6.0.00, v6.1.00, v6.2.00 |
| | v3.2.2 | v7.0U3 | v7.0U3 | v6.3.00, v6.4.00 |
| | v3.2.3 | v7.0U3 | v7.0U3 | v6.5.00 |
| | v4.0.0 | v7.0U3 | v7.0U3 | v6.0.00, v6.1.00, v6.2.00, v6.3.00 |
| | v4.1.0 | v7.0U3 | v7.0U3 | v6.3.00, v6.4.00, v6.5.00 |

# Points to Note (VMware NSX-T)

- The steps in the documentation assume that VMware NSX-T is installed and configured. Refer to VMware Documentation for configuration details.
- GigaVUE-FM supports service insertion only for overlay transport zone associated with the E-W traffic. Service insertion is not supported for VLAN transport zone associated with the N-S traffic or when the VMware NSX-T manager in federation mode. However, the traffic from the workload virtual machines in NSX-T federated environments can be acquired using UCT-V. Refer to Configure GigaVUE Fabric Components using Third party Orchestration on NSX-T Federation Environment in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration for more detailed information on how to deploy UCT-V, UCT-V Controller to acquire traffic from NSX-T federated environment.

# Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T

The following are the prerequisites for integrating GigaVUE V Series Nodes with VMware NSX-T:

- ESXi hosts must be prepared as NSX-T Data Center transport nodes by using transport node profiles.
- ESXi hosts where workload VMs that needs to be monitored must be attached to the overlay transport zone.
- GigaVUE-FM supports service insertion only for overlay transport zone associated with the E-W traffic. Service insertion is not supported on VLAN transport zone associated with the N-S traffic or when the VMware NSX-T manager in federation mode.
- Before deploying GigaVUE V Series Nodes using GigaVUE-FM, Service segment must be created in the NSX-T manager on Overlay Transport Zone. Refer to  Create a Service Segment in VMware NSX-T for step-by-step instructions on how to create service segment.
- Refer to Supported Hypervisors for VMware for supported VMware vCenter, VMware ESXi and VMware NSX-T versions.
- Only IPv4 traffic is supported.
- If a guest VM running on an ESXi host is connected to a VLAN segment. and that ESXi host is not configured to an Overlay Transport zone, then the traffic destined to a service VM is disrupted. Such a configuration can also cause traffic to be routed to a black hole.
- For more detailed VMware requirements on East-West traffic monitoring, refer to the below links and select the appropriate NSX-T version.
    - NSX-T Data Center Requirements for East-West Traffic - For versions 3.x.x
    - NSX Requirements for East-West Traffic - For versions 4.x.x
- Refer to Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T for ESXi host resource requirement to deploy GigaVUE V Series Nodes.

- GigaVUE V Series Node device OVA image file.

> **NOTE:** An external HTTP(S) server for hosting the GigaVUE V Series image OVFs and VMDK file (extracted from the OVA file) when using **Use External Image** Option in Monitoring Domain. Refer to Create Monitoring Domain for VMware NSX-T for more detailed information on what is an external image and how to configure it.

The GigaVUE V Series Node OVA image files can be downloaded from Gigamon Customer Portal.

**Unsupported Configurations when using VMware NSX-T:**

- Service Insertion is not supported on Global NSX-T managers in federation mode. Use Local NSX-T Managers for deploying our solution in this case.
- Service Insertion is not supported on Multi tenancy environments.
- GigaVUE-VM and GigaVUE V Series Node visibility solutions cannot be deployed on the same NSX-T manager.
- Multiple monitoring domains cannot be configured with same NSX-T manager.

Refer to the following topics for the requirements:

- Network Firewall Requirements
- Recommended Form Factor (Instance Types)
- Required VMware Virtual Center Privilege
- Required Roles in VMware NSX-T
- Disable Certification Validation in VMware NSX-T
- Default Login Credentials

# Network Firewall Requirements

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

| Source | Destination | Source Port | Destination Port | Protocol | Service | Purpose |
|--------|-------------|-------------|------------------|----------|---------|---------|
| GigaVUE-FM | ESXi hosts | Any (1024-65535) | 443 | TCP | https | Allows GigaVUE-FM to communicate with vCenter, NSX-T and all ESXi hosts. |
| | NSX-T Manager | | | | | |
| | vCenter | | | | | |
| GigaVUE-FM | GigaVUE V Series Node | Any (1024-65535) | 8889 | TCP | Custom API | Allows GigaVUE-FM to communicate with GigaVUE |

| | | | | | | V Series Node |
|---|---|---|---|---|---|---|
| Administrator | GigaVUE-FM | Any (1024-65535) | 443 | TCP | https | Management connection to GigaVUE-FM |
| | | | 22 | | ssh | |
| GigaVUE-FM | GigaVUE V Series Node | Any (1024-65535) | 5671 | TCP | Custom TCP | Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node |
| Remote Source | GigaVUE V Series Node | Custom Port (VXLAN and UDPGRE),N/A for GRE | 4789 | UDP | VXLAN | Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only) |
| | | | N/A | IP 47 | GRE | |
| | | | 4754 | UDP | UDPGRE | |
| GigaVUE V Series Node | Tool/ HC Series instance | Custom Port (VXLAN),N/A for GRE | 4789 | UDP | VXLAN | Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool |
| | | | N/A | IP 47 | GRE | |
| GigaVUE V Series Node | Tool/ HC Series instance | N/A | N/A | ICMP | echo Request | Allows V Series node to health check tunnel destination traffic (Optional) |
| | | | | | echo Response | |
| GigaVUE V Series Node | GigaVUE-FM | Any (1024-65535) | 5671 | TCP | Custom TCP | Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM |

| GigaVUE-FM NSX-T Manager vCenter ESXi host | External Image Server URL | Any (1024-65535) | Custom port on web Server | TCP | http | Access to image server to image lookup and checks, and downloading the image |
|---|---|---|---|---|---|---|
| NSX-T Manager vCenter ESXi host | GigaVUE-FM | Any (1024-65535) | 443 | TCP | http | When using GigaVUE-FM as the image server for uploading the GigaVUE V Series Image. |

## Recommended Form Factor (Instance Types)

The form factor (instance type) size of the GigaVUE V Series Node is configured on the OVF file and packaged as part of the OVA image file. The following table lists the available form factors and sizes based on memory and the number of vCPUs for a single V series node. Instances sizes can be different for GigaVUE V Series Nodes in different ESXi hosts and the default size is Small.

| Type | Memory | vCPU | Disk space |
|---|---|---|---|
| Small | 4GB | 2vCPU | 8GB |
| Medium | 8GB | 4 vCPU | 8GB |
| Large | 16GB | 8 vCPU | 8GB |

## Required VMware Virtual Center Privilege

This section lists the minimum privileges required for the GigaVUE-FM user in vCenter.

| Category | Required Privilege | Purpose |
|---|---|---|
| **vApp** | • vApp application configuration | V Series Node Deployment |
| **Virtual machine** | **Interaction** <br> ▪ Power on <br> ▪ Power Off | • V Series Node Deployment <br> • Used to power on and power off GigaVUE V Series Node. |

## Required Roles in VMware NSX-T

This section lists the minimum roles required for the GigaVUE-FM user in VMware NSX-T.

**Deploying GigaVUE V Series Node using GigaVUE-FM**

When deploying GigaVUE V Series Node using GigaVUE-FM, the following is the minimum required role combination:

For **NSX-T version 3.2.x** and **NSX-T version 4.x.x**, select the following Role combination:

- NETX Partner Admin and Security Admin

For **NSX-T version 3.1.x**, select LDAP with any one of the following Role combinations:

- NETX Partner Admin and Security Operator
- NETX Partner Admin and Network Operator

Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM section for more detailed information on how to deploy GigaVUE V Series Nodes using GigaVUE-FM

**Deploying GigaVUE V Series Nodes using VMware NSX-T**

When deploying GigaVUE V Series Node using VMware NSX-T manager, the minimum required role is NETX Partner Admin.

Refer to Deploy GigaVUE V Series Nodes using VMware NSX-T Manager  section for more detailed information on how to deploy GigaVUE V Series Nodes using VMware NSX-T Manager.

## Disable Certification Validation in VMware NSX-T

When using uncertified GigaVUE V Series Node image, due to certificate validation requirement in VMware NSX-T, GigaVUE V Series Node deployment may fail. Before deploying the GigaVUE V Series Nodes, disable the certificate validation as follows.

1. Login to each NSX-T manager using CLI with root credentials.
2. Open **/config/vmware/auth/ovf_validation.properties** file
3. Set a value for **THIRD_PARTY_OVFS_VALIDATION_FLAG** as **2**. The definition of the legends are as follows:
   - 0: only VMware-signed OVFs are allowed for deployment
   - 1: only VMware-signed and well-known CA-signed OVFs are allowed for deployment
   - 2: no validation
4. Save and Exit the file.

## Default Login Credentials

You can login to the GigaVUE V Series Node, GigaVUE V Series proxy, and UCT-V Controller by using the default credentials.

| Product | Login credentials |
|---------|-------------------|
| GigaVUE V Series Node | You can login to the GigaVUE V Series Node by using ssh. The default username and password is:<br>Username: gigamon<br>Password: Gigamon123! |

# Install and Upgrade GigaVUE-FM

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

- o Installation: Refer to GigaVUE-FM Installation and Upgrade Guide available in the Gigamon Documentation Library.
- o Upgrade: Refer toUpgrade GigaVUE-FM topic in GigaVUE-FM Installation and Upgrade Guide.

# Deployment Options for GigaVUE Cloud Suite for VMware (NSX-T)

This section provides detailed information on the multiple ways in which GigaVUE Cloud Suite for VMware can be configured to provide visibility for physical and virtual traffic. Based on the method in which you want to deploy the GigaVUE V Series Nodes, there are two ways in which you can configure GigaVUE Cloud Suite for VMware (NSX-T). Refer to the Prerequisites for Integrating V Series Nodes with NSX-T section for prerequisites that are required to be configured. For more detailed information and the work flow refer the following topics:

- Deploy GigaVUE V Series Nodes using GigaVUE-FM
- Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

## Deploy GigaVUE V Series Nodes using GigaVUE-FM

| Step No | Task | Refer the following topics |
|---------|------|----------------------------|
| 1 | Create users in GigaVUE-FM and VMware NSX-T for communication. | Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM |
| 2 | Upload the GigaVUE V Series Node Image (OVA FIle) into GigaVUE-FM (optional- use only when using GigaVUE-FM as the image server) | Upload GigaVUE V Series Node Image into GigaVUE-FM |
| 3 | Create a service segment in NSX-T | Create a Service Segment in VMware NSX-T |
| 4 | Create a Monitoring Domain | Create Monitoring Domain for |

| Step No | Task | Refer the following topics |
|---|---|---|
| | | VMware NSX-T |
| 5 | Deploy GigaVUE V Series Nodes using GigaVUE-FM | Configure GigaVUE V Series Nodes for VMware NSX-T<br><br>Refer to *Deploy GigaVUE V Series Nodes using GigaVUE-FM* section |
| 6 | Create Monitoring session | Create a Monitoring Session |
| 7 | Create a Ingress and Egress Tunnels to tunnel traffic | Create Ingress and Egress Tunnel |
| 8 | Add Applications to the Monitoring Session | Add Applications to Monitoring Session |
| 9 | Deploy Monitoring Session | Deploy Monitoring Session |
| 10 | View Monitoring Session Statistics | View Monitoring Session Statistics |
| 11 | Create NSX-T Group and Service chain | Create NSX-T Group and Service Chain |

## Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

| Step No | Task | Refer the following topics |
|---|---|---|
| 1 | Create users in GigaVUE-FM and VMware NSX-T for communication. | Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM |
| 2 | Upload the GigaVUE V Series Node Image (OVA FIle) into GigaVUE-FM (optional- use only when using GigaVUE-FM as the image server) | Upload GigaVUE V Series Node Image into GigaVUE-FM |
| 3 | Create a service segment in NSX-T | Create a Service Segment in VMware NSX-T |
| 4 | Create a Monitoring Domain | Create Monitoring Domain for VMware NSX-T |
| 5 | Deploy GigaVUE V Series Nodes using GigaVUE-FM | Configure GigaVUE V Series Nodes for VMware NSX-T<br><br>Refer to *Deploy GigaVUE V Series Nodes using VMware NSX-T* Manager section |
| 6 | Create Monitoring session | Create a Monitoring Session |
| 7 | Create a Ingress and Egress Tunnels to tunnel traffic | Create Ingress and Egress Tunnel |
| 8 | Add Applications to the Monitoring Session | Add Applications to Monitoring Session |
| 9 | Deploy Monitoring Session | Deploy Monitoring Session |
| 10 | View Monitoring Session Statistics | View Monitoring Session Statistics |
| 11 | Create NSX-T Group and Service chain | Create NSX-T Group and Service Chain |

# Deploy GigaVUE Cloud Suite for VMware (NSX-T)

To integrate V Series nodes with NSX-T, perform the following steps:

- Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM
- Create a Service Segment in VMware NSX-T
- Upload GigaVUE V Series Node Image into GigaVUE-FM
- Install Custom Certificate
- Create Monitoring Domain for VMware NSX-T
- Configure GigaVUE V Series Nodes for VMware NSX-T
- Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM
- Increase or Decrease GigaVUE V Series Nodes using VMware NSX-T Manager

## Create Users in VMware vCenter, VMware NSX-T, and GigaVUE-FM

For VMware NSX-T and GigaVUE-FM to communicate, an user must be created in VMware NSX-T Manager, VMware vCenter, and GigaVUE-FM.

> **NOTE:** GigaVUE-FM connects to NSX-T Manager that supports TLSv1.0, TLSv1.1, and TLSv1.2.

Refer to the following topics for step-by-step instructions on how to create users in vCenter, NSX-T Manager and GigaVUE-FM:

- Create User in VMware vCenter
- Create User in NSX-T manager
- Create user in GigaVUE-FM

### Create User in VMware vCenter

For GigaVUE-FM to communicate with vCenter, you must first create a user with the minimum required privileges in VMware vCenter.

Refer to Required VMware vCenter Privileges for the minimum privileges required in Vmware vCenter.

### Create User in NSX-T manager

For GigaVUE-FM to communicate with NSX-T, you must first create a user with the minimum required role in NSX-T manager.

To create a user in VMware NSX-T:

1. In NSX-T, navigate to **System > Settings > User Management** and click **User Role Assignment** tab.
2. On the **User Role Assignment** tab, click **ADD**. Select the Roles based on the GigaVUE V Series Node deployment type as mentioned in Required Roles in VMware NSX-T.
3. Click **Save** and then a GigaVUE-FM user is created in NSX-T.

## Create user in GigaVUE-FM

For VMware NSX-T Manager to be able to communicate with GigaVUE-FM, you need to create a user in GigaVUE-FM who has the admin role.

Refer to  Add Users section in *GigaVUE Administration Guide* for detailed and step-by-step instructions on how to create users in GigaVUE-FM.

Tips: You can follow these tips to easily identify the user created for VMware NSX-T.

- In the **Name** field, enter the name of the call back user. For example, you can use NSX-T Manager Callback as the user name to help you associate this user with the NSX-T Manager.
- In the **Username** field, enter a username for the user. For example, you can use nsxv to help you remember that this user is associated with NSX-T.

The username and password created for vCenter, NSX-T Manager, and GigaVUE-FM in this section will be used when creating Monitoring Domain in GigaVUE-FM. Refer to Create Monitoring Domain for VMware NSX-T for step-by-step instructions on how to create monitoring domain.

## Create a Service Segment in VMware NSX-T

Registering the NSX-T details on GigaVUE-FM is a prerequisite to create the service segment.

To create a service segment in VMware NSX-T:

1. On the NSX manager, go to **Security** and select **Network Introspection** from the left navigation pane. The **Network Introspection Settings** page opens. Select Service Segment from the top navigation bar. Then, the Service Segment page appears.
2. On the Service Segment page, click **ADD SERVICE SEGMENT** and a new row appears to create a service segment.
3. Enter the name and map it to the overlay transport zone created for the VMs.
4. Click **Save**.

The segment created in this section will be used as service attachment when deploying GigaVUE V Series Nodes using GigaVUE-FM. Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information on how to deploy GigaVUE V Series Node using GigaVUE-FM.

## Upload GigaVUE V Series Node Image into GigaVUE-FM

You can upload your V Series Node image into GigaVUE-FM. This step is optional, follow the steps given below only if you wish to use GigaVUE-FM as an internal image server.

To upload the V Series image into GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Settings > OVA Files**. The OVA Files page appears.
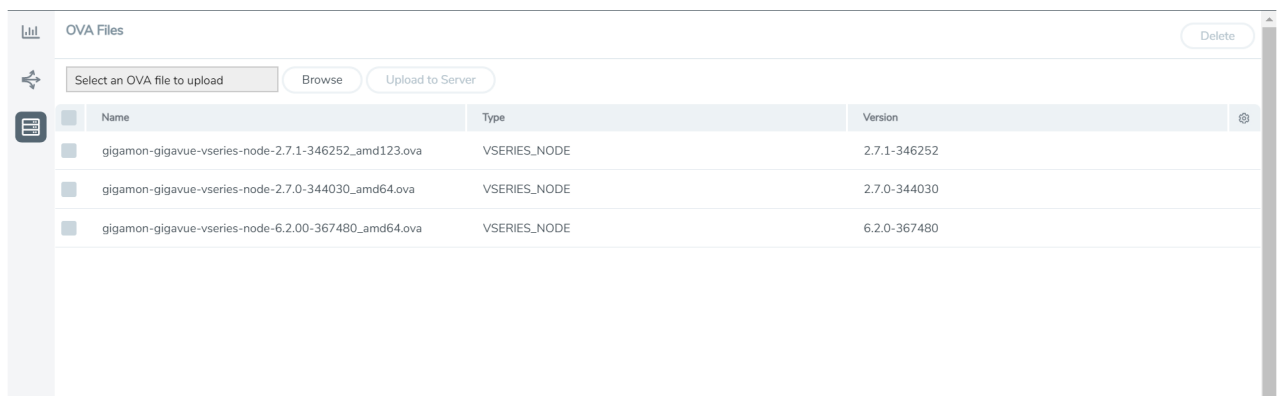


2. In the OVA Files page, click **Browse** to select the *gigamon-gigavue-vseries-node-x.x.x-0-xxxxxx.ova* file.

3. Click **Upload** to Server to upload the selected OVA image file to GigaVUE-FM server.

> **NOTE:** The maximum number of OVA files that can be uploaded to GigaVUE-FM for VMware NSX-T is three.

## Install Custom Certificate

GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controllers have default self-signed certificates installed. The communication between GigaVUE-FM and the fabric components happens in a secure way using these default self-signed certificates, however you can also add custom certificates like SSL/TLS certificate to avoid the trust issues that occurs when the GigaVUE V Series Nodes, GigaVUE V Series Proxy, or UCT-V Controllers run through the security scanners.

You can upload the custom certificate in two ways:

- Upload Custom Certificates using GigaVUE-FM
- Upload Custom Certificate using Third Party Orchestration

## Upload Custom Certificates using GigaVUE-FM

To upload the custom certificate using GigaVUE-FM follow the steps given below:

1. Go to **Inventory > Security > Custom SSL Certificate**. The **Custom Certificate Configuration** page appears.
2. On the Custom Certificate Configuration page, click **Add**. The **New Custom Certificate** page appears.
3. Enter or select the appropriate information as shown in the following table.

| Field | Action |
|---|---|
| Certificate Name | Enter the custom certificate name. |
| Certificate | Click on the Upload Button to upload the certificate. |
| Private Key | Click on the Upload Button to upload the private key associated with the certificate. |

4. Click **Save**.

You must also add root or the leaf CA certificate in the Trust Store. For more detailed information on how to add root CA Certificate, refer to Trust Store topic in *GigaVUE Administration Guide*.

The certificates uploaded here can be linked to the respective GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller in the Fabric Launch Configuration Page. Refer to *Configure GigaVUE Fabric Components in GigaVUE-FM* topic in the respective cloud guides for more detailed information.

## Upload Custom Certificate using Third Party Orchestration

You can also upload custom certificates to GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controller using your own cloud platform at the time of deploying the fabric components. Refer to the following topics on more detailed information on how to upload custom certificates using third party orchestration in the respective platforms:

For integrated mode:

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

For generic mode:

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

## Create Monitoring Domain for VMware NSX-T

This chapter describes how to create a monitoring domain for deploying GigaVUE V Series Nodes in VMware NSX-T environment through GigaVUE-FM. You must establish a connection between GigaVUE-FM and VMware NSX-T environment. Creating a monitoring domain in GigaVUE-FM allows you to establish a connection between yourVMware NSX-T environment and GigaVUE-FM.

> **Points to Note:**
>
> - Each NSX-T manager can support a maximum of one monitoring domain.
> - When editing a Monitoring domain that has GigaVUE V Series Nodes deployed, the **Use External Image** and **Use FM to Launch Fabric** toggle buttons are disabled. However, for a monitoring domain which does not have any GigaVUE V Series Nodes deployed the **Use External Image** toggle button is enabled.

**Prerequisites:**

- If you wish to use **Use External Image** option, before create a monitoring domain ensure all the contents of the OVA file are extracted into VMDK and OVF files and are placed in the directory which represents the Image URL.
- If you wish to use GigaVUE-FM as your image server, then before creating a monitoring domain save the OVA files to the dedicated directory. Refer to Upload GigaVUE V Series Node Image into GigaVUE-FMfor more detailed instructions on how to upload the OVA files to GigaVUE-FM.

To create monitoring domain in GigaVUE-FM for VMware NSX-T:

1.  Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2.  On the **Monitoring Domain** page, click **New**. The **VMware Configuration** page appears.

3. In the **VMware Configuration** page, enter or select the following details:

| Field | Description |
|---|---|
| **Monitoring Domain** | Name of the monitoring domain. |
| **Connection Alias** | Name of the connection. |
| **Virtual Center** | IP address or Hostname of the vCenter. |
| **Username** | Username of the vCenter user. |
| **Password** | vCenter password used to connect to the vCenter |
| **NSX-T Manager** | IP address or Hostname of your VMware NSX-T. |
| **NSX-T Username** | Username of your NSX-T account. |
| **NSX-T Password** | Password of your NSX-T account. |
| **FM Username** | Username of your GigaVUE-FM account |
| **FM Password** | Password of your GigaVUE-FM account. |
| **Use External Image** | This toggle button allows you to choose between an external image or internal image. If you wish to use the **Use External Image** option, you can use an external server (http or https server) to place all the OVF files and provide the URL of the web server. Else you can upload the OVA files to GigaVUE-FM and use it as an internal image server.<br><br>a. **Yes** to use an external image. To use an external image, enter the web server URL of the directory where VMDK, and OVF files are available. The Web Server URL must be in the following format: *http(s)://<server-IP:port>/<path to where the OVF files are saved>* and the port can be any valid number. The default port number is 80.<br><br>b. **No** to use an internal image. To use an internal image, select the uploaded OVA files from the **Select an image** drop-down menu. |
| **Use FM to Launch Fabric** | Enable this toggle button if you wish to deploy GigaVUE V Series Nodes using GigaVUE-FM.<br><br>**NOTE:** If you disable this option, then you must deploy GigaVUE V Series Nodes using VMware NSX-T manager. Refer to Deploy GigaVUE V Series Nodes using VMware NSX-T Manager section for more detailed information. |

4. Click **Save**.

The newly created monitoring domain appears in the list view of the **Monitoring Domain** page.

To edit a monitoring domain, select the deployed monitoring domain and click **Actions**. From the drop-down list, select **Edit**, the VMware configuration page appears.

Next Steps:

1. **Use FM to Launch Fabric** is enabled: You are navigated to the **VMware NSX-T Fabric Deployment** page. Refer to Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information on how to deploy GigaVUE V Series Node using GigaVUE-FM.

2. **Use FM to Launch Fabric** is disabled: You must deploy GigaVUE V Series Nodes using VMware NSX-T Manager. Refer to Deploy GigaVUE V Series Nodes using VMware NSX-T Manager for more detailed instruction on how to deploy GigaVUE V Series Nodes using VMware NSX-T manager.

# Configure GigaVUE V Series Nodes for VMware NSX-T

This section provides step-by-step information on how to deploy GigaVUE V Series Nodes.

GigaVUE V Series Nodes can be deployed in GigaVUE-FM using two ways. You can either directly use VMware NSX-T manager to deploy your GigaVUE V Series Nodes or use GigaVUE-FM to deploy your GigaVUE V Series Nodes.

> **Points to Note:**
>
> - When VMware NSX-T is configured in a cluster on multiple hosts, ensure all the hosts are in a connected state. Even if one of the hosts is in a disconnected state then GigaVUE V Series Node host-based deployment will be unsuccessful.
> - If a GigaVUE V Series Node is restarted, then the existing flows that is received by that GigaVUE V Series Node will not be forwarded to the other available GigaVUE V Series Nodes (if any). However, the new flows will be forwarded to any available GigaVUE V Series Node.

Refer to the following section for more detailed information:

- Deploy GigaVUE V Series Nodes using GigaVUE-FM
- Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

Deploy GigaVUE V Series Nodes using GigaVUE-FM

After creating a monitoring domain in GigaVUE-FM for VMware NSX-T, which establishes a connection between VMware NSX-T manager and GigaVUE-FM, GigaVUE-FM launches the **VMware NSX-T Fabric Deployment** page. Refer to Create Monitoring Domain for VMware NSX-T section for more detailed information on how to a create monitoring domain in GigaVUE-FM for VMware NSX-T.

**Deploy GigaVUE V Series Node from GigaVUE-FM**

1. After creating a monitoring domain, you are navigated to the **VMware Fabric Launch Configuration** page.

2. You can also open **VMware Fabric Launch Configuration** page from the **Monitoring Domain** page. To launch the **VMware Fabric Launch Configuration** from the Monitoring Domain, go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**. Click **Actions > Deploy Fabric**. The **VMware Fabric Launch Configuration** page appears.

VMware NSX-T Fabric Deployment

**Deployment Name***

Enter a deployment name

**Datacenter***

Select a datacenter

**Cluster***

Select a cluster

**Enable Custom Certificates**

**Datastore***

Select a datastore

**SSL Key**

Select

**Name Server**

Use Comma to seperate va

**Management**

**Network***

Select a switch or port group

**MTU**

Enter a MTU

**IP Type**

DHCP

**Tunnel**

**Network***

Select a switch or port group

**MTU**

Enter a MTU

**IP Type**

DHCP

**Gateway IP**

Enter a Gateway IP

**Use IPv6**

**User Password:** *(gigamon)*

**Confirm User Password**

**Form Factor**

Small, 2vCPU, 4GB RAM, 8GB Disk

**Service Attachment**

Select service attachment

**Deployment Type**

Select deployment type

**Deployment Count**

3. Select or enter the following details in the VMware Fabric Launch Configuration page:

| Field | Description |
|---|---|
| **Deployment Name** | Name of the deployment (NSX-T service deployment) |
| **Datacenter** | vCenter Data Center with the NSX-T hosts to be provisioned with V Series nodes |
| **Cluster** | Cluster where you want to deploy GigaVUE V Series Nodes |
| **Enable Custom Certificates** | Enable this option to validate the custom certificate during SSL Communication. GigaVUE-FM validates the Custom certificate with the trust store. If the certificate is not available in Trust Store, communication does not happen, and a handshake error occurs.<br><br>**NOTE:** If the certificate expires after the successful deployment of the fabric components, then the fabric components move to failed state. |
| **Custom SSL Certificate** | Select the custom certificate from the drop-down menu. You can also upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For more detailed information, refer to Install Custom Certificate. |
| **Datastore** | Network datastore shared among all NSX-T hosts. |
| **Name Server** | The server that stores the mapping between the domain names and the IP address. The maximum number of name servers that can be entered is three. Enter the valid IPv4 address, separated by comma. |
| **Management** | |
| Network | Management network for V Series nodes |
| IP Type | Select the management network IP type as Static or DHCP |
| IP Pool<br><br>**NOTE:** This field appears only when the Management **IP type** is Static. | Select the IP Pool |
| MTU | The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000. |
| **Tunnel** | |
| Network | Tunnel Network for the V Series nodes |
| IP Type | Select the tunnel network IP address type as Static or DHCP |
| Gateway IP (optional) | Gateway IP address of the Tunnel Network |
| IP Pool<br><br>**NOTE:** This field appears only when the Tunnel **IP type** is Static. | Select the IP Pool |

| Field | Description |
|---|---|
| MTU | The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection. Enter value between 1280 to 9000. |
| **User Password: (gigamon)** | SSH Password for the built-in user, '**gigamon**' on the V Series node |
| **Confirm Password** | Confirm the SSH Password of the V Series node |
| **Form Factor** | Instance size of the V Series node. (eg: Small, Medium or Large) |
| **Service Attachment** | Service segment created in VMware NSX-T Manager. Refer to Create a Service Segment in VMware NSX-T for more detailed instructions on how to create service segment in VMware NSX-T. |
| **Deployment Type** | Type of GigaVUE V series Node deployment. It can be either Clustered or Host-Based deployment type.<br><br>**NOTE:** Select the deployment type as Clustered if you wish to increase or decrease the number of nodes in a cluster using GigaVUE-FM. Refer Deploy GigaVUE V Series Nodes using GigaVUE-FM for more detailed information. |
| **Deployment Count** (for Clustered deployment type) | Number of GigaVUE V Series Nodes (Service Instances) to deploy |

4. Click **Deploy**. After the V series node is deployed in vCenter, it appears on the Monitoring Domain page under the deployment name of the selected Monitoring Domain. You can select a specific service deployment by clicking on the deployment name on the Monitoring Domain page.



To view the fabric launch configuration specification of a fabric node, click on a GigaVUE V Series Node, and a quick view of the Fabric Launch Configuration appears on the Monitoring Domain page.

> **NOTE:** The deployed GigaVUE V Series Node name is created automatically by VMware NSX-T. Do not change the name of the GigaVUE V Series Node in the vCenter.

## Deploy GigaVUE V Series Nodes using VMware NSX-T Manager

You can deploy your V Series Nodes using VMware NSX-T manager. The GigaVUE V Series nodes register themselves with GigaVUE-FM using the information provided by the user in the NSX-T manager. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM.

Refer to the following sections for details:

- Getting Started
- Deploying GigaVUE V Series Nodes in VMware NSX-T Manager
- Delete GigaVUE V Series Nodes and Monitoring Domain

**Getting Started**

To register your V Series Nodes using VMware NSX-T manager, follow the steps given below:

1.  Create a monitoring domain in GigaVUE-FM. Refer to Create Monitoring Domain for VMware NSX-T for detailed instructions.

2.  In the **VMware Configuration** page, select **No** for the **Use FM to Launch Fabric** field as you wish to deploy V Series Nodes using VMware NSX-T manager.



> **NOTE:** When creating the Monitoring Domain for deploying GigaVUE V Series Nodes, you can use the VMware NSX-T username and password that has atleast "NETX Partner Admin" role assigned to it.

3.  After creating your monitoring domain, you can use VMware NSX-T manager to deploy your nodes.

**Deploying GigaVUE V Series Nodes in VMware NSX-T Manager**

1.  In the Service Deployment page of the VMware NSX-T manager, select **Deployment**. Then select GigaVUE Cloud Suite from the **Partner Service** drop-down. For detailed information, refer to Deploy a Partner Service topic in VMware Documentation.

2. After selecting the **Deployment template** and **Deployment Specification**, click **Configure Attributes**. The **Configure Attributes** page appears.

3. In the **Configure Attributes** page, enter the Service VM Host Name and Admin user password details. If you wish to use custom certificate for GigaVUE V Series Node, then enter the **SSL Private Key** and the **SSL Certificate**. For more details on Custom Certificate refer to Install Custom Certificate topic for more detailed information on Custom Certificates.

4. Once the V Series Node is successfully deployed, the deployed node is registered with GigaVUE-FM after the run time status of the node is displayed as **UP** in VMware NSX-T manager.

The GigaVUE V Series Node deployed in your VMware NSX-T manager appears on the Monitoring Domain page of GigaVUE-FM. In GigaVUE-FM the **Status** of the node is displayed as **Launching** and once the node is successfully registered the **Status** is changed to **Ok.**

| | | Monitoring Domain | Connection | Name | Management IP | Type | Version | Status |
|---|---|---|---|---|---|---|---|---|
| ∨ | ☐ | nsxt-202-13-md | | | | | | |
| ∨ | ☐ | | nsxt-202-45-md | | | | | ⊘ Connected |
| | ☐ | | | Gigamon Inc._vp-3rd-... | | V Series Node | | ⊘ Ok |

> • IPv6 address is not supported for gateway of the tunnel interface when nodes are deployed through the VMware NSX-T manager.
>
> • When you deploy nodes using VMware NSX-T manager, ensure all your V Series Nodes are of same version. GigaVUE-FM does not support V Series Nodes with different version in the Monitoring Domain.
>
> • The deployed GigaVUE V Series Node name is created automatically by VMware NSX-T. Do not change the name of the GigaVUE V Series Node in the vCenter.

**Delete GigaVUE V Series Nodes and Monitoring Domain**

> **NOTE:** When you deploy your V Series Nodes using VMware NSX-T manager, you cannot directly delete your V Series Node in GigaVUE-FM. In this case, the Delete button in GigaVUE-FM is disabled, so the Service Deployment in NSX-T Manager must be deleted first.

To delete a GigaVUE V Series node deployed using VMware NSX-T Manager, follow the steps given below:

1. Delete the **Policy** and **Service Chain** in the VMware NSX-T manager.

2. Then, delete the Monitoring Session in GigaVUE-FM.

3. Delete the node in VMware NSX-T manager. Then, the node will be unregistered from

the Monitoring Domain in GigaVUE-FM.
4. Finally, delete the Monitoring Domain in GigaVUE-FM.

## Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM

You can add more nodes or remove nodes from an existing monitoring domain using GigaVUE-FM. These steps are applicable only when you deploy GigaVUE V Series Nodes using GigaVUE-FM.

> **NOTE:** Increasing or Decreasing the number of nodes in a cluster is only applicable when using Clustered based deployment.

Refer to the following topics for more detailed information on how to add or remove GigaVUE V Series Node deployed using GigaVUE-FM for an existing monitoring domain :

- Add V Series Nodes to Existing Monitoring Domain
- Decrease V Series Nodes from Existing Monitoring Domain

### Add V Series Nodes to Existing Monitoring Domain

To increase the number of V Series Node in an existing monitoring domain follow the steps given below:

1. On the Monitoring domain page, select the monitoring domain to which you wish to add more V Series Nodes.
2. Click on the **Actions** button and select **Deploy Fabric**.
3. The VMware Fabric Deployment page opens. Enter the details as mentioned in Increase or Decrease GigaVUE V Series Nodes using GigaVUE-FM

    > - The Deployment type must be Clustered to have multiple deployment on the same cluster.
    > - A cluster can have only one Host Based Deployment, however there can be multiple clustered deployment on the same cluster.

4. Enter the number of V Series Nodes you wish to add in the **Deployment Count** column.
5. Click Deploy.

    The newly added V Series Nodes will be displayed under the existing monitoring domain with the new Deployment Name.

### Decrease V Series Nodes from Existing Monitoring Domain

To decrease the number of nodes in an existing monitoring domain follow the steps given below:

1. On the Monitoring domain page, select the **Deployment** from which you wish to remove the V Series Nodes or select the entire monitoring domain to remove all the deployments from the monitoring domain.

   > **NOTE:** You can select the Deployment either by using the check-box on the left side or by clicking on the deployment name

2. Click on the **Actions** button and select **Delete Deployment**.
3. All the V Series Nodes under that deployment will be deleted.

   The number of V Series Nodes in the monitoring domain will be decreased by the number of nodes in the deployment that were deleted.

**Example use-case for Increase or Decrease V Series Nodes using GigaVUE-FM**

This feature can be used in a scenario where you are migrating from GigaVUE-VM visibility solution to GigaVUE V Series visibility solution, you can simply add the V Series node to the existing monitoring domain instead of undeploying and redeploying the monitoring domain every time you wish to add more V Series nodes to the monitoring domain.

## Increase or Decrease GigaVUE V Series Nodes using VMware NSX-T Manager

You can now add more nodes or remove nodes from an existing monitoring domain using VMware NSX-T Manager. These steps are applicable only when you deploy GigaVUE V Series Nodes using VMware NSX-T Manager.

Refer to the following topics for more detailed information on how to add or remove GigaVUE V Series Node deployed using NSX-T manager for an existing monitoring domain :

- Add V Series Nodes to Existing Monitoring Domain
- Decrease V Series Nodes from Existing Monitoring Domain

### Add V Series Nodes to Existing Monitoring Domain

To increase the number of V Series Node in an existing monitoring domain using VMware NSX-T Manager follow the steps given below:

1. On the Service Deployment page of the VMware NSX-T manager, select **Deployment**. This page lists the service deployments that are already deployed.
2. Then, click **Deploy Service** button. For more details on how to deploy a service refer Deploy a Partner Service.
3. Enter the same details as given for the service mapped to the existing monitoring domain in GigaVUE-FM to which you wish to add more nodes.
4. In the **Clustered Deployment Count**, enter the number of nodes you wish to add to

the existing monitoring domain.

5. Click **Save**.

Once the Service deployment is successful and the nodes are deployed, you can view the nodes on the monitoring domain page of GigaVUE-FM.

**Example** - Consider a scenario where the monitoring domain in GigaVUE-FM has two V Series Nodes. To increase the number of nodes in this monitoring domain, go to VMware NSX-T Manager and create a new service using the steps mentioned above. Then, the number of V Series Nodes in the monitoring domain in GigaVUE-FM goes up by the number you have mentioned in **Clustered Deployment Count** column in the VMware NSX-T.

### Decrease V Series Nodes from Existing Monitoring Domain

To decrease the number of nodes in an existing monitoring domain using VMware NSX-T follow the steps given below:

1. On the **Service Deployment** page of the VMware NSX-T manager, select **Deployment**.
2. The service deployment page lists the service deployments that are already deployed. .
3. Select the service deployment that you want to delete. The GigaVUE V Series Nodes that are part of that service deployment will be deleted from the host. These GigaVUE V Series Nodes will also be removed from the monitoring domain in the GigaVUE-FM. This way the number of service VMs (V Series nodes) can be decreased in a monitoring domain

**Example** - Consider a scenario where the monitoring domain in GigaVUE-FM has five V Series Nodes. To reduce the number of nodes in this monitoring domain, go to VMware NSX-T Manager and delete a service deployment using the steps mentioned above. Then, the number of V Series Nodes in the monitoring domain in GigaVUE-FM goes down by the number you have mentioned in **Clustered Deployment Count** column of the service you have deleted.

# Upgrade GigaVUE V Series Node for VMware NSX-T

GigaVUE V Series Nodes can be deployed in two ways. You can either directly use VMware NSX-T manager to deploy your GigaVUE V Series Nodes or use GigaVUE-FM to deploy your GigaVUE V Series Nodes. Based on the method you deploy GigaVUE V Series Nodes, you can upgrade them in two ways. Refer to the following topic for more detailed information.

- Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM
- Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager

# Upgrade GigaVUE V Series Nodes Deployed using GigaVUE-FM

Before upgrading the nodes ensure that all the current V Series nodes are of same version. To upgrade GigaVUE V Series Node in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select a deployed monitoring domain and click **Actions**. From the drop-down list, select **Upgrade Fabric**, the **V Series Node Upgrade** dialog box appears.



3. Use the **Use External Image** toggle button to choose between internal and external image.
   - **Yes** to use an external image. Enter the Image URL of the latest V Series Node OVA image
   - **No** to use an internal image. To use an internal image, select the uploaded OVA files from the **Select an image** drop-down menu.
4. Click the **Change Form Factors** check box to modify the form factor (instance) size.

   > **NOTE:** Both the new and the current V Series nodes appears on the same monitoring domain until the new nodes replaces the current and the status changes to **Ok**.

5. Click **Upgrade**.

You can view the status of the upgrade in the Status column of the **Monitoring Domain** page.

To view the detailed upgrade status click **Upgrade in progress** or **Upgrade successful**, the **V Series Node Upgrade Status** dialog box appears.



Click **Clear** to delete the logs of successfully upgraded nodes.

> **NOTE:** Monitoring Domain upgrade can be only done when there is a single service deployment in the monitoring domain.

## Upgrade GigaVUE V Series Node Deployed using VMware NSX-T Manager

> **NOTE:** When you deploy your V Series Nodes using VMware NSX-T manager, you cannot directly upgrade V Series Node in GigaVUE-FM. In this case, the upgrade button in GigaVUE-FM is disabled.

To upgrade V Series Nodes deployed using VMware NSX-T, follow the steps given below:

1. Delete the existing V Series Node in VMware NSX-T Manager.
2. Click **Actions > Edit** in the Monitoring Domain page. The **VMware Configuration** page appears.
3. Enter the new **Image URL** or select a new image if **Use External Image** toggle button is disabled.
4. Then, deploy the new V Series Nodes in the VMware NSX-T manager

# Cloud Overview Page

The overview page is a central location to view and monitor all the monitoring sessions in a single place. You can use this overview page to spot issues which will help in troubleshooting, or perform basic actions like view, edit, clone, and delete. This page provides a quick overview of basic statistics, V Series Alarms, Connection Status and Volume Usage vs Allowance and a table to summarize the active monitoring sessions details. You can also edit the monitoring session from this page instead of navigating to the monitoring session page in each platform.

You can view cloud overview page in the following ways:

Overall Cloud Overview Page

Platform specific Cloud Overview Page

## Overall Cloud Overview Page

To view the Overall Cloud Overview Page, Go to **Traffic > Virtual > Orchestrated Flows > Overview**

## Platform specific Cloud Overview Page

To view Plaftform Specific Cloud Overview Page, Go to **Traffic** > **Virtual** > **Orchestrated Flows** > and select your cloud platform.

The **Monitoring Sessions** page appears as shown:
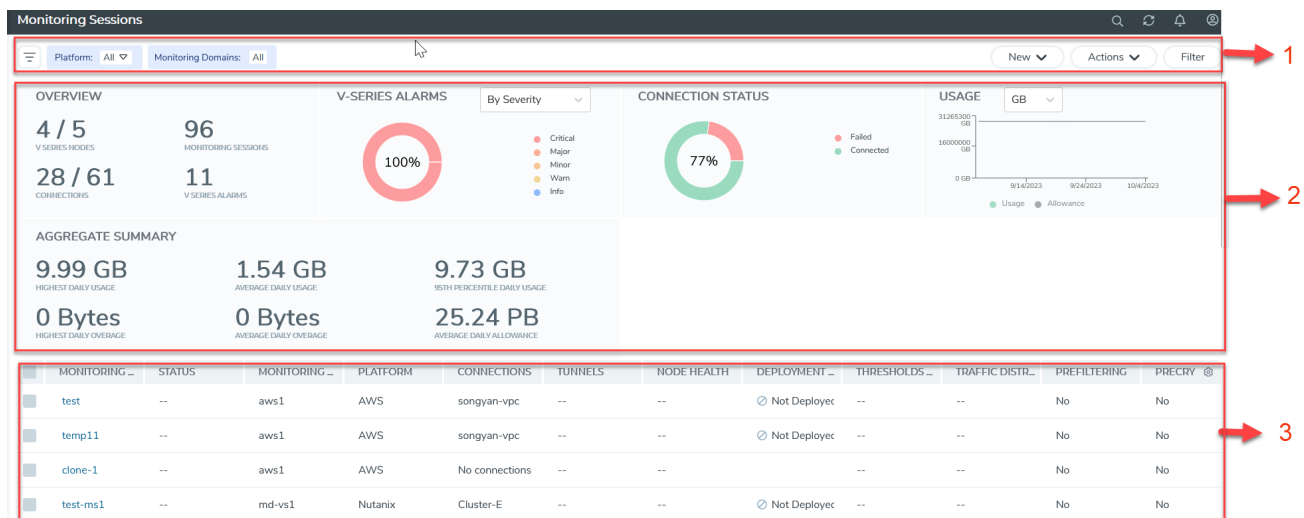


For easy understanding of the Monitoring Session page, the above figure is split into three major sections as described in the following table:

| Number | Section | Description |
|---|---|---|
| 1 | Top Menu | Top Menu |
| 2 | Charts | Viewing Charts |
| 3 | Monitoring Session Details | In Overall Cloud Overview Page, you can view the monitoring session details of all the cloud platforms. Refer to the section Viewing Monitoring Session Details of all Cloud Platforms In Platform specific Overview Page, you can view the monitoring session details of the individual cloud platforms. |

## Top Menu

The Top menu consists of the following: options:

| Options | Description |
|---|---|
| Filters | You can filter the monitoring session based on a criterion or combination of criteria such as based on the platform, monitoring session and V Series Node Id by applying filters. For more information, refer to Filters |
| **New** Drop-down list box | You create a new monitoring session and new monitoring domain. To create new monitoring session and monitoring domain refer to Create a Monitoring Session topic. |
| **Action** Drop-down list box | You can do the following actions through the **Action** Drop down list box: <ul><li>**Edit** - Opens the Edit page for the selected monitoring session.</li><li>**Delete** - Deletes the selected monitoring session.</li><li>**Clone** - Duplicates the selected monitoring session.</li><li>**Deploy** - Deploys the selected monitoring session.</li><li>**Undeploy** - Un-deploys the selected monitoring session.</li><li>**Apply Threshold** - Applies the threshold template created for monitoring cloud traffic health.</li><li>**Apply Policy** - Enables Precryption, Prefiltering, or Secure Tunnel.</li></ul> For more information, refer to Cloud Monitoring Session topic. |

### Filters

You can filter the monitoring session based on a criterion or combination of criteria such as based on the platform, monitoring session and V Series Node Id by applying filters.

You can apply the filters in two ways:

- Filter on the left corner
- Filter on the right corner

**Filter on the left corner**

You can view the monitoring sessions by filtering the monitoring domain based on the platform.

1. Select the required platform from the **Platform** drop- down list box.

2. Click ▤ and select the monitoring domain.

The monitoring domain selected appears on the top menu bar.

**Filter on the right corner** Filter

You can view the monitoring sessions by filtering the monitoring domain based on a criterion or by providing multiple criteria as follows:

- Monitoring Session
- Status
- Monitoring Domain
- Platform
- Connections
- Tunnel
- Deployment Status

## Viewing Charts

You can view the following charts on the overview page:

- Overview
- V Series Alarms
- Connection Status
- Usage (VBL)
- Aggregate Summary

## Overview

The overview dashboard displays the number of GigaVUE V Series Nodes active in GigaVUE-FM, the number of Monitoring sessions and connections configured in all the platforms, and the number of alarms triggered in V Series Nodes.

## V Series Alarms

The V Series Alarms widget presents a pie chart that helps you to view the V Series alarms generated quickly. Each type of alarm triggered is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of V Series alarms triggered.

## Connection Status

The connection status presents a pie chart that helps you to quickly view the connection status of connections configured in the monitoring domain. The success and failed connection status is differentiated by the color in the graph, which is specified by the legend. Hovering the mouse over an area in the chart displays the total number of connections.

## Usage

The Usage widget displays the traffic that flows through the GigaVUE V Series Nodes. Each bar in the graph indicates the volume usage on a particular day. Hovering the mouse over a bar in the graph displays the volume allowance and volume usage on that day.

## Aggregate Summary

The aggregate summary displays the highest daily volume usage, average daily volume usage, highest daily volume over usage, average daily volume over usage, 95th percentile daily volume usage and the average daily volume allowance.

## Viewing Monitoring Session Details of all Cloud Platforms

You can view the following monitoring session details:

| Details | Description |
|---|---|
| Monitoring Sessions | Name of the monitoring session. When you click the name of the session, you can view the following options:<br><br>• **View**- When you click this option, you can view a split window displaying the details of the monitoring sessions such as **Statistics**, **Connections**, **V Series Nodes**, **Source Health**, **Http2 Logging**. For more information, refer to Viewing Monitoring Session Details of Individual Cloud Platforms<br>• **Edit** - When you click this option, you can view the **Edit Monitoring Session** page. |
| Status | Health status of the monitoring session. |
| Monitoring Domain | Name of the Monitoring Domain to which the monitoring session is associated. |
| Platform | Cloud platform in which the session is created. |
| Connections | Connection details of the monitoring session. |
| Tunnels | Tunnel details related to the monitoring session |
| Node Health | Health of the node. |
| Deployment Status | Status of the deployment |
| Threshold Applied | Specifies whether the threshold is applied or not |
| Traffic Distribute | Specifies information about traffic distribution. |
| Prefiltering | Specifies whether Prefiltering is configured or not |
| Precryption | Specifies whether Precryption is configured or not. |
| SBI logging | Specifies whether SBI logging is configured or not. |
| Traffic Mirroring | Specifies whether Traffic Mirroring is configured or not. |

**NOTE:** Click the settings icon ⚙ to select the columns that should appear in the monitoring session.

## Viewing Monitoring Session Details of Individual Cloud Platforms

For a monitoring session, you can view the following details of the monitoring session:

| Details | Description |
|---------|-------------|
| Statistics | You can view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can view the statistics for all the V Series nodes or only for the Gigamon V Series node. You can also filter the statistics based on the elements associated with the monitoring session. For more information, refer to View Monitoring Session Statistics. |
| Connections | You can view the connection details of the monitoring session. You can view details such as the name of the connection, deployment status, number of targets, and targets source health. |
| V Series Nodes | You can view the V Series nodes associated with the monitoring session. You can also view details such as name of the V Series Node, Host VPC, MD connection, Version, and Management IP. |
| Source Health | You can view the health of the source connected to the monitoring session. |
| Http2 Logging | You can view the details of the 5G SBI logging details. For more information about 5G SBI, refer to 5G-Service Based Interface Application |

To view the details, click the name of the monitoring session, and then click **View**. A split window appears displaying the details.

# Configure Monitoring Session

GigaVUE-FM collects inventory data on all V series nodes deployed in your environment through vCenter connections. You can design your monitoring session to include or exclude the target VMs that you want to monitor. You can also choose to monitor egress, ingress, or all traffic. When a new target VM is added to your environment, GigaVUE-FM automatically detects it and based on the selection criteria, the detected target VMs are added into your monitoring session. Similarly, when a traffic monitoring target VM is removed, it updates the monitoring sessions to show the removed instance. Before deploying a monitoring session, you need to deploy a V Series node in each host where you want to monitor the traffic.

> **NOTE:**
> - Link transformation and multiple links between two entities are not supported in V Series nodes of ESXi.
> - Pre-filtering is not supported on VMware ESXi running with V Series nodes.

Refer to the following topics for details:

- Create a Monitoring Session
- Interface Mapping
- Create Ingress and Egress Tunnel
- Create a New Map
- Add Applications to Monitoring Session
- Deploy Monitoring Session
- View Monitoring Session Statistics

## Create a Monitoring Session

A monitoring session defines how traffic should be processed and send to the tunnel endpoints.

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

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

> **NOTE:** You can have multiple monitoring sessions per monitoring domain.

You can create multiple monitoring sessions within a monitoring domain.

To create a new monitoring session:

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

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

| Field | Description |
|---|---|
| **Alias** | The name of the monitoring session. |
| **Monitoring Domain** | The name of the monitoring domain that you want to select. |
| **Connection** | The connection(s) that are to be included as part of the monitoring domain. You can select the required connections that need to be part of the monitoring domain. |
| **Distribute traffic** | Enabling the "Distribute Traffic" option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. |

4.  Click **Create**. The Monitoring Session details page appears displaying the specified session information and target VMs.

> **NOTE:** In a Monitoring Session, if a selected VM is connected to VSS and VDS, then the GigaVUE-FM can create tapping for both VSS and VDS network.

The Monitoring Session page also has the following buttons:

| Button | Description |
|---|---|
| **Edit** | Opens the Edit page for the selected monitoring session. <br><br> > **NOTE:** In case of an error while editing a monitoring session, undeploy and deploy the monitoring session again. |
| **Delete** | Deletes the selected monitoring session. |
| **Clone** | Duplicates the selected monitoring session. |
| **Deploy** | Deploys the selected monitoring session. |
| **Undeploy** | Undeploys the selected monitoring session. |
| **Apply Threshold** | You can use this button to apply the threshold template created for monitoring cloud traffic health. Refer to Monitor Cloud Health for more detailed information on cloud traffic health, how to create threshold templates and how to apply threshold templates. |

## Edit Monitoring Session

In the edit monitoring session canvas page, you can add and configure applications, tunnel endpoints, raw endpoints, and maps.

Refer to the following topics for detailed information:

- Create Ingress and Egress Tunnels
- Add Applications to Monitoring Session
- Create Raw Endpoint
- Create a New Map

The **Edit Monitoring Session** page has the following buttons:

| Button | Description |
|---|---|
| **Show Targets** | Use to refresh the subnets and monitored instances details that appear in the **Instances** dialog box. |
| **Interface mapping** | Use to change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping topic for more details. |
| **Dashboard** | The dashboard displays the statistics for all the applications, end points and the maps available in the monitoring session. |
| **Ok / Cancel** | **Ok:** Use to save the configurations in the monitoring session when the monitoring session is in undeployed state.<br><br>**Cancel**: After the monitoring session is deployed, if you have made any changes and wish to remove them, use this option. |
| **Options** | You can enable or disable User Defined Applications here. You can also create and threshold template and apply it to the monitoring session. |
| **Deploy** | Deploys the selected monitoring session. Refer to Deploy Monitoring Session topic for more details. |

## Interface Mapping

You can change the interface of individual GigaVUE V Series Nodes deployed in a monitoring session. After deploying the monitoring session, if you wish to change the interfaces mapped to an individual GigaVUE V Series Node, you can use the **Interface Mapping** button to map the interface to the respective GigaVUE V Series Nodes. To perform interface mapping:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.

2. Select a Monitoring session from the list view and click **Actions > Edit**. The Edit Monitoring session page appears.

3. In the Edit Monitoring session canvas page, click on the **Interface Mapping** button.

4. The **Select nodes to deploy the Monitoring Session dialog box** appears. Select the GigaVUE V Series Nodes for which you wish to map the interface.

5. After selecting the GigaVUE V Series Node, select the interfaces for each of the REPs and the TEPs deployed in the monitoring session from the drop-down menu for the selected individual GigaVUE V Series Nodes. Then, click **Deploy**.

## Create Ingress and Egress Tunnel

Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a monitoring session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, UDPGRE, or ERSPAN tunnel.

> **NOTE:** GigaVUE-FM allows you to configure Ingress Tunnels in the Monitoring Session, when the **Traffic Acquisition Method** is UCT-V.

To create a new tunnel endpoint:

1. After creating a new monitoring session, or click **Actions > 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.

| X | **Add Tunnel Spec** | | Save | Add To Library |
| --- | --- | --- | --- | --- |

Alias                  Alias *

Description       Description (optional)

Type                 Select a type...

Select a type...
ERSPAN
L2GRE
VXLAN

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. <br><br> **NOTE:** Do not enter spaces in the alias name. |
| **Description** | The description of the tunnel endpoint. |
| **Type** | The type of the tunnel. <br> Select ERSPAN, or L2GRE, or VXLAN, TLS-PCAPNG, UDP, or UDPGRE to create a tunnel. |
| **VXLAN** | |
| **Traffic Direction** <br> The direction of the traffic flowing through the GigaVUE V Series Node. | |
| **In** | Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node. |
| | **IP Version** — The version of the Internet Protocol. Select IPv4 or IPv6. |
| | **Remote Tunnel IP** — For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. |
| | **VXLAN Network Identifier** — Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215. |
| | **Source L4 Port** — Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A. |
| | **Destination L4 Port** — Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B. |
| **Out** | Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. |
| | **Remote Tunnel IP** — For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint. |
| | **MTU** — The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500. |
| | **Time to Live** — Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64. |
| | **DSCP** — Differentiated Services Code Point (DSCP) are the values, |

| Field | Description |
|---|---|
| | which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority. |
| **Flow Label** | Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575 |
| **VXLAN Network Identifier** | Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215. |
| **Source L4 Port** | Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A. |
| **Destination L4 Port** | Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B. |

**UDPGRE**

**Traffic Direction**

The direction of the traffic flowing through the GigaVUE V Series Node.

| In | Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node. |
|---|---|
| | **IP Version** | The version of the Internet Protocol. Select IPv4 or IPv6. |
| | **Remote Tunnel IP** | For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. |
| | **Key** | Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295 |
| | **Source L4 Port** | Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A. |
| | **Destination L4 Port** | Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B. |

**L2GRE**

**Traffic Direction**

The direction of the traffic flowing through the GigaVUE V Series Node.

| Field | Description | |
|-------|-------------|---|
| In | Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the GigaVUE V Series Node. | |
| | **IP Version** | The version of the Internet Protocol. Select IPv4 or IPv6. |
| | **Remote Tunnel IP** | For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. |
| | **Key** | Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295. |
| Out | Choose **Out** (Encapsulation) for creating an Egress tunnel from the V Series node to the destination endpoint. | |
| | **Remote Tunnel IP** | For Egress tunnel, Remote Tunnel IP is the IP address of the tunnel destination endpoint. |
| | **MTU** | The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500. |
| | **Time to Live** | Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64. |
| | **DSCP** | Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority. |
| | **Flow Label** | Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575. |
| | **Key** | Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter value between 0 and 4294967295. |
| **ERSPAN** | | |
| **Traffic Direction** The direction of the traffic flowing through the GigaVUE V Series Node. | | |

| Field | Description | |
|---|---|---|
| In | **IP Version** | The version of the Internet Protocol. Select IPv4 or IPv6. |
| | **Remote Tunnel IP** | For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. |
| | **Flow ID** | The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023. |
| **TLS-PCAPNG** | | |
| **Traffic Direction** The direction of the traffic flowing through the GigaVUE V Series Node. | | |
| In | **IP Version** | The version of the Internet Protocol. only IPv4 is supported. |
| | **Remote Tunnel IP** | For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. |
| | **MTU** | The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500. |
| | **Source L4 Port** | Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A. |
| | **Destination L4 Port** | Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B. |
| | **Key Alias** | Select the Key Alias from the drop-down. |
| | **Cipher** | Only SHA 256 is supported. |
| | **TLS Version** | Only TLS Version1.3. |
| | **Selective Acknowledgments** | Enable to receive the acknowledgments. |
| | **Sync Retries** | Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6. |
| | **Delay Acknowledgments** | Enable to receive the acknowledgments when there is a delay. |

| Field | Description | |
|-------|-------------|---|
| **Out** | **IP Version** | The version of the Internet Protocol. only IPv4 is supported. |
| | **Remote Tunnel IP** | For Ingress tunnel, Remote Tunnel IP is the IP address of the tunnel source. |
| | **MTU** | The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500. |
| | **Time to Live** | Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64. |
| | **DSCP** | Differentiated Services Code Point (DSCP) are the values, which network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 as the lowest priority. |
| | **Flow Label** | Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. Accepted value is between 0 and 1048575 |
| | **Source L4 Port** | Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A. |
| | **Destination L4 Port** | Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B. |
| | **Cipher** | Only SHA 256 is supported. |
| | **TLS Version** | Only TLS Version1.3. |
| | **Selective Acknowledgments** | Enable to receive the acknowledgments. |
| | **Sync Retries** | Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6. |
| | **Delay Acknowledgments** | Enable to receive the acknowledgments when there is a delay. |
| **UDP:** | | |

| Field | Description | |
|-------|-------------|---|
| **Out** | **L4 Destination IP Address** | Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. Refer to Application Metadata Exporter for more detailed information on what AMX application is and how to configure it. |
| | **Source L4 Port** | Port from which the connection will be established to the target. For Example, if A is the source and B is the destination, this port value belongs to A. |
| | **Destination L4 Port** | Port to which the connection will be established from the source. For Example, if A is the source and B is the destination, this port value belongs to B. |

4. Click **Save**.

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

To apply threshold template to Tunnel End Points, select the required tunnel end point on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold template, refer to *Monitor Cloud Health* topic.

Tunnel End Points configured can also be used to send or receive traffic from GigaVUE HC Series and GigaVUE TA Series. Provide the IP address of the GigaVUE HC Series and GigaVUE TA Series as the Source or the Destination IP address as required when configuring Tunnel End Points.

After configuring the tunnels and deploying the monitoring session, you can view the names of egress tunnels configured for a monitoring session, on the Monitoring Session details page. The Egress Tunnel column displays the name of the egress tunnel configured for a particular monitoring session. When multiple egress tunnels are configured for a monitoring session, then the Egress Tunnel column displays the number of egress tunnels configured in that monitoring session. Hover over the number of egress tunnels to display the names of the egress tunnels used in that particular monitoring session.

Tunnel End Points created will be listed in the **Tunnel Specifications** page. You can create, edit, and delete tunnel end point from this page. Refer to Create Tunnel Specifications for more detailed information on how to create tunnel end points.

## Create a New Map

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

For new users, the free trial bundle will expire after 30 days, and the GigaVUE-FM prompts you to buy a new license. For licensing information, refer to *GigaVUE Licensing Guide*.

A map is used to filter the traffic flowing through the GigaVUE V Series Nodes. It is a collection of one or more rules (R). The traffic passing through a map can match one or more rules defined in the map.

Keep in mind the following when creating a map:

| Parameter | Description |
|---|---|
| **Rules** | A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic. |
| **Priority** | Priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority. |
| **Pass** | The traffic from the virtual machine will be passed to the destination. |
| **Drop** | The traffic from the virtual machine is dropped when passing through the map. |
| **Traffic Filter Maps** | A set of maps that are used to match traffic and perform various actions on the matched traffic. |
| **Inclusion Map** | An inclusion map determines the instances to be included for monitoring. This map is used only for target selection. |

| Exclusion Map | An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection. |
|---|---|
| **Automatic Target Selection (ATS)** | A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the monitoring session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: <br>• mac Source <br>• mac Destination <br>• ipv4 Source <br>• ipv4 Destination <br>• ipv6 Source <br>• ipv6 Destination <br>• VM Name Destination <br>• VM Name Source <br>• VM Tag Destination - Not applicable to Nutanix. <br>• VM Tag Source - Not applicable to Nutanix. <br>• VM Category Source - Applicable only to Nutanix <br>• VM Category Destination - Applicable only to Nutanix. <br>• Host Name -Applicable only to Nutanix and VMware. <br>The traffic direction is as follow: <br>• For any rule type as Source - the traffic direction is egress. <br>• For Destination rule type - the traffic direction is ingress. <br>• For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. <br><br> **NOTE:** If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC. |
| **Group** | A group is a collection of maps that are pre-defined and saved in the map library for reuse. |

To create a new map:

1. After creating a new monitoring session, or click **Actions > Edit** on an existing monitoring session, the GigaVUE-FM canvas appears.

2. In the canvas, select **New > New Map**, drag and drop a new map template to sthe workspace. The New Map quick view appears.
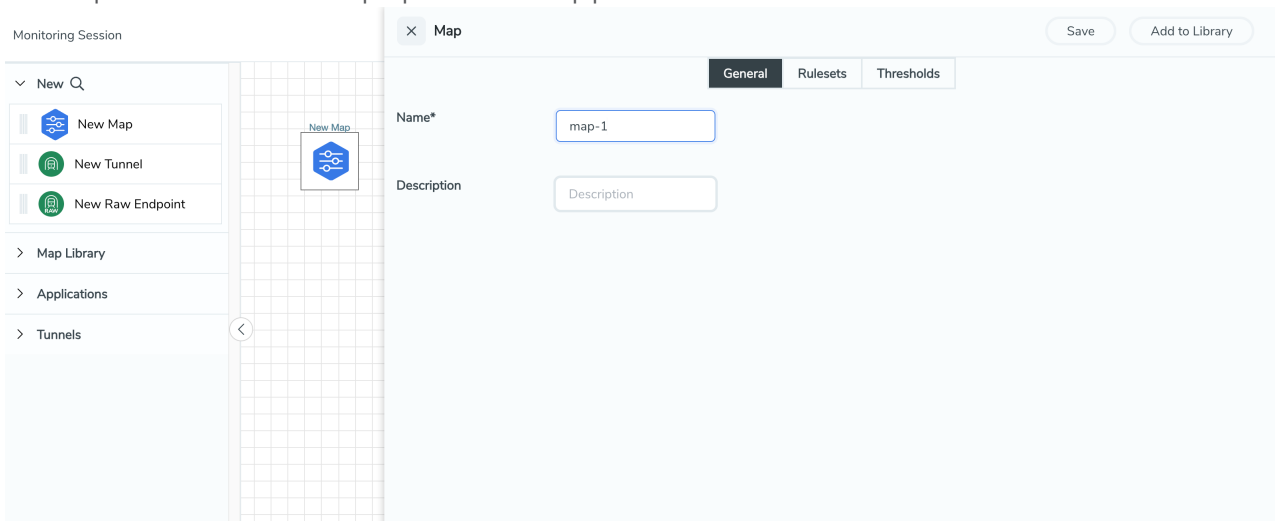


3. On the New Map quick view, click on **General** tab and enter the required information as described in the following table:

| Field | Description |
|---|---|
| **Name** | Name of the new map |
| **Description** | Description of the map |

> Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
> - Traffic Map—Only Pass rules for ATS
> - Inclusion Map—Only Pass rules for ATS
> - Exclusion Map—Only Drop rules for ATS

4. Click on **Rule Sets** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. Refer to Example-Create a New Map using Inclusion and Exclusion Maps for more detailed information on how to configure Inclusion and Exclusion maps using ATS.

   a. **To create a new rule set:**

      i. Click **Actions > New Rule Set**.

      ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.

      iii. Enter the Application Endpoint in the Application EndPoint ID field.

      iv. Select a required condition from the drop-down list.

      v. Select the rule to **Pass** or **Drop** through the map.

   b. **To create a new rule:**

      i. Click **Actions > New Rule**.

      ii. Select a required condition from the drop-down list. Click [...] and select **Add Condition** to add more conditions.

      iii. Select the rule to **Pass** or **Drop** through the map.

5. Click **Save**.

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

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

To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, click on the Threshold tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.

**Rules and Notes:**

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.

You can also perform the following action in the Monitoring session canvas.

- Click a map and select **Details** to edit the map
- Click a map and select **Delete** to delete the map.
- Click the **Show Targets** button to refresh the subnets and monitored instances details that appear in the **Instances** dialog box.

- Click [icon] to expand the **Targets** dialog box. To view details about a GigaVUE V Series Node, click the arrow next to the VM.

- In the Instances window, click [icon] to filter the list of instances.

## Example- Create a New Map using Inclusion and Exclusion Maps

Consider a monitoring session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. In the **General** tab, enter the name as Map 1 and enter the description. In the **Rule sets** tab, enter the priority and Application Endpoint ID.
3. Select the condition as VM Name and enter the **target**. This includes the instances target-1-1, target-1-2, target-1-3, target-2-1, and target-2-2.
4. Click on the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
   a. In the **General** tab, enter the name as Inclusionmap1 and enter the description. In the **Rule Sets**, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1**. Then the instance with VM name **target-1-1, target-1-2,** and **target-1-3** will be included.
6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
   a. In the **General** tab, enter the name as Exclusionmap1 and enter the description. In the **Rule Sets** tab, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then the instance **target-1-3** will be excluded.

   Based on this configuration, the Automatic Target Selection will select the instances target-1-1 and target-1-2 as target.

## Map Library

To reuse a map,

1. In the Monitoring Session page, Click **Actions > Edit**. The Edit Monitoring Session page opens.
2. Click the map you wish to save as a template. Click **Details**. The Application quick view appears.
3. Click **Add to Library**. Save the map using one of the following ways:

4.  Select an existing group from the **Select Group** list or create a **New Group** with a name.

5.  Enter a description in the **Description** field, and click **Save**.

The Map is saved to the **Map Library** in the Edit Monitoring Session Canvas page. This map can be used from any of the monitoring session. To reuse the map, drag and drop the saved map from the Map Library.

## Add Applications to Monitoring Session

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

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- Header Stripping
- 5G-Service Based Interface Application
- Application Metadata Exporter
- SSL Decrypt
- NetFlow

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

## Deploy Monitoring Session

To deploy the monitoring session:

1.  Drag and drop the following items to the canvas as required:
    - Maps from the **MAP LIBRARY** section
    - Inclusion and Exclusion maps from the Map Library to their respective section at the bottom of the workspace.
    - GigaSMART apps from the **APPLICATIONS** section
    - Egress tunnels from the **TUNNELS** section

2. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

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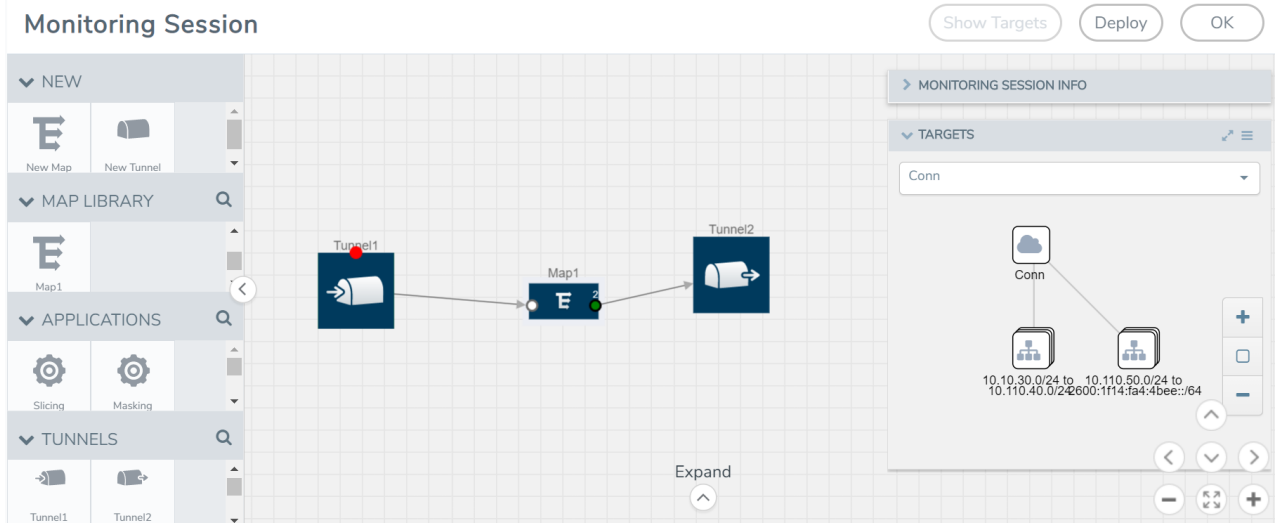


3. (Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method) Click **Show Targets** to view details about the subnets and monitored instances. The instances and the subnets that are being monitored are highlighted in orange.

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

   - Partial Success—The session is not deployed on one or more instances due to V Series node failure.
   - Failure—The session is not deployed on any of the V Series nodes.
   The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

## 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.

On the Monitoring Sessions page, click the name of the monitoring session, and then click **View**. A split window appears displaying the **Statistics**, **Connections**, **V Series Nodes**, **Source Health** and **Http2 Logging** of the monitoring session as shown:
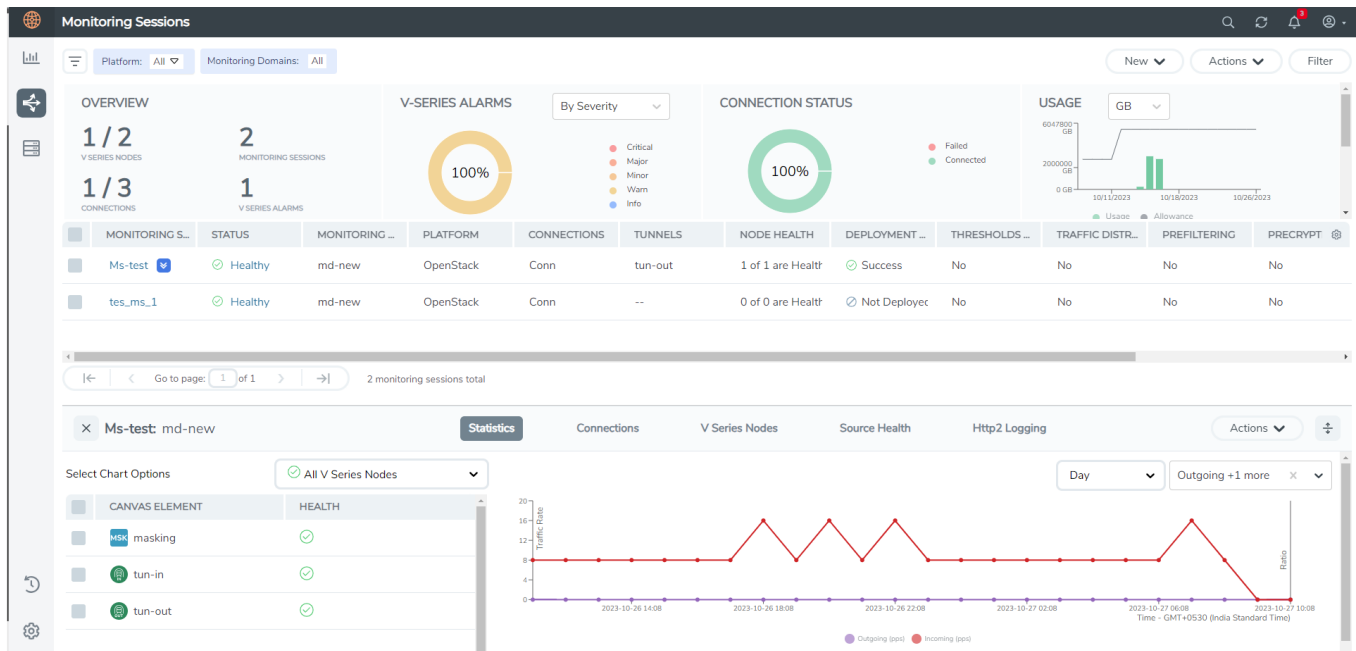
To know more about the statistics of the session, click **Statistics**.

You can view the statistics by applying different filters as per the requirements of analysing the data. GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- You can view the **Statistics** in full screen. To view in full screen, click the **Actions** drop-down list at the right corner of the window, and select **Full Screen**. **Statistics** appear in full screen.

- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can select the options from the drop-down list box.

- You can filter the traffic and view the statistics based on factors such as **Incoming**, **Outgoing**, **Ratio (Out/In), Incoming Packets**, **Outgoing Packets**, **Ratio (Out/In) Packets**. You can select the options from the drop-down list box.

- You can also view the statistics of the monitoring session deployed in the individual V Series Nodes. To view the statistics of the individual V Series Node, select the name of the **V Series Node** from the drop-down list for which you want to view the statistics from the V Series node drop-down menu on the top left corner of the Monitoring Session Statistics page.

- You can view the statistics of the elements involved in the monitoring session. To view the statistics, click on the **Select Chart Options** page and select the elements associated with the session.

- Directly on the graph, you can click on **Incoming(Mbps)**, **Outgoing (Mbps)**, or **Ratio (Out/In) (Mbps)** to view the statistics individually.

> Raw EndPoint (REP) is a part of the monitoring session but can also receive the bypassed traffic that is not filtered by the map, so it is recording more packets than expected. For example, if the map has a rule as IPv4, but the REP can receive the bypassed (non-ipv4) traffic. The recorded number of packets from the V Series node can be more than expected.

## View Health Status on the Monitoring Session Page

You can view the health status of the monitoring session and the components deployed, in the monitoring session page. Refer to Monitor Cloud Health for more detailed information on how to configure cloud health and view health status.

To view the health status on the Monitoring Session page:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. The Monitoring Session page appears. The list view in the Monitoring Domain page displays the details of the Monitoring Session.

The following columns in the monitoring session page are used to convey the health status:

### Status

This column displays the health status (both traffic and configuration) of the entire monitoring session. The status is marked healthy only if both the traffic and configuration health status is healthy, even if either of them is unhealthy, then the health status is moved to unhealthy.

### Node Health

This column displays the configuration and traffic health status of the monitoring session deployed in V Series Nodes. This column provides information on the number of GigaVUE V Series Nodes that have healthy traffic flow and monitoring session successfully deployed to the total number of V Series Nodes that have monitoring session deployed.

> **NOTE:** Node Health only displays the health status, so if the V Series Node is down it will not be reflected in the monitoring session page.

### Targets Source Health

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Connections** tab.

This column displays the configuration health status of the monitoring session deployed in targets. This column provides information on the number of monitoring sessions successfully deployed on a particular target to the total number of monitoring session deployed on that particular target.

You can view the health status of the individual targets and also the error message associated with them, by clicking on the Target Source Health column.

## Visualize the Network Topology

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

To view the topology diagram in GigaVUE-FM:

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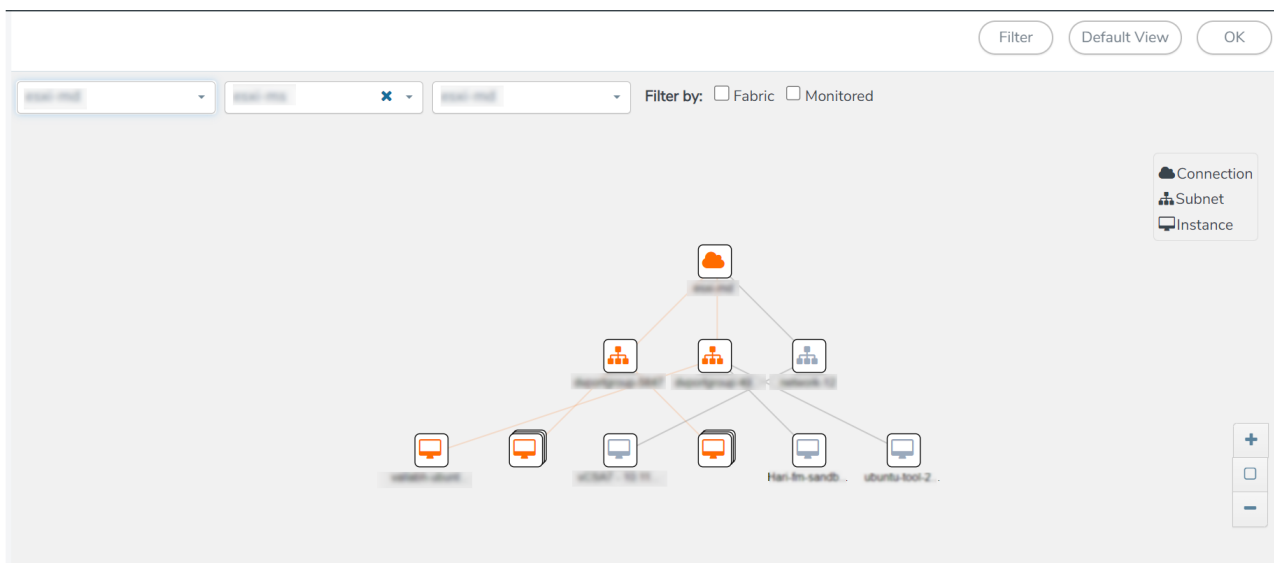


5. (Optional) Hover over or click the subnet or VM Group icons to view the subnets or instances present within the group.

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

- Use the **Filter** button to filter the instances based on the VM name, VM IP, Subnet ID, or Subnet IP, and view the topology based on the search results.

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

# Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, Application Intelligence solution can be configured from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for virtual environment from the **Application Intelligence** page. The following operations can only be performed using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

It is highly recommended to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM will migrate all your virtual Application Intelligence sessions and their connections seamlessly. All sessions will be rolled back to their original states if the migration fails.

> **Points to Note:**
>
> - You must have **fm_admin** role in GigaVUE-FM to perform this migration. Refer to Configure Role-Based Access and Set Permissions for more detailed information how to create Users and assign Roles to the user.
> - If any of the existing Application Intelligence Session is in PENDING or SUSPENDED, then the migration will not be triggered. Resolve the issue and start the migration process.
> - If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration, then the migration will not be triggered. Resolve the issue and start the migration process.
> - If an existing Monitoring Session has a same name as the Application Intelligence Session, then the migration will not be triggered. Change the existing Monitoring Session name to continue with the migration process.

> ▤ • If any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set, you cannot continue with the migration. In the Monitoring Session either only Pass All or Advanced Rules as Drop is supported in the fifth Rule Set. Please delete this session and start the migration.
>
> • When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for migrating the Application Intelligence Session in these scenarios.

To migrate your existing Application Intelligence Session to Monitoring Session Page, follow the steps given below:

1. On the left navigation pane, select **Traffic > Solutions >Application Intelligence**. You cannot create a new Application Intelligence Session from this page.
2. When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
3. Review the message and click  **Migrate.**
4. The **Confirm Migration** dialog box appears. The list Application Intelligence Session that will be migrated appears here.
5. Review the message and click **Migrate**.
6. GigaVUE-FM checks for the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
7. Click on the **Go to Monitoring Session Page** button to view the Application Intelligence Session that are migrated to the monitoring session page.

All the virtual Application Intelligence Sessions in the Application Intelligence page is migrated to the Monitoring Session Page.

## Post Migration Notes for Application Intelligence

After migrating Application Intelligence session to Monitoring Session page, you must consider the following things:

1. If you wish to enable Secure tunnels after migrating the Application Intelligence Session, follow the steps given below.

   a. Enable Secure Tunnels in the **Options** page. Refer to Enable Prefiltering, Precryption, and Secure Tunnel topic more detailed information on how to enable secure tunnel for a monitoring Session.

   b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The monitoring session is undeployed.

   c. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.

   d. Add the Application Intelligence applications.

   e. Modify the Number of Flows as per the below table:

| Cloud Platform | Instance Size | Maximum Number of Flows |
|---|---|---|
| VMware | Large (8 vCPU and 16 GB RAM) | 200k |
| AWS | Large (c5n.2xlarge) | 300k |
| | Medium (t3a.xlarge) | 100k |
| Azure | Large (Standard_D8s_V4) | 500k |
| | Medium (Standard_D4s_v4) | 100k |
| Nutanix | Large (8 vCPU and 16 GB RAM) | 200k |

> **NOTE:** Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

   f. Click **Deploy**. Refer to Application Intelligence topic for more detailed information on how to deploy the Application Intelligence applications.

2. When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating theApplication Intelligence Session to the Monitoring Session and redeploying the monitoring session, a momentary loss in the statistical data of the Application Visualization application will be seen while redeploying the monitoring session.

3. After migrating the Application Intelligence Session to monitoring session, if you wish to make any configuration changes, then the GigaVUE V Series Node version must be greater than or equal to 6.3.00.

# Monitor Cloud Health

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components. Refer to the following topics for more detailed information on configuration health, traffic health and how to view the health status:

- Configuration Health Monitoring
- Traffic Health Monitoring
- View Health Status

## Configuration Health Monitoring

The configuration health status provides us detailed information about the configuration and deployment status of the deployed monitoring session.

This feature is supported for the following fabric components and features on the respective cloud platforms:

**For V Series Nodes:**

- AWS
- Azure
- OpenStack
- VMware
- Nutanix

**For UCT-Vs:**

- AWS
- Azure
- OpenStack

**For VPC Mirroring:**

- AWS

**For OVS Mirroring and VLAN Trunk Port:**

- OpenStack

To view the configuration health status, refer to the Configuration Health Monitoring section.

# Traffic Health Monitoring

GigaVUE-FM allows you to monitor the traffic health status of the entire monitoring session and also the individual V Series Nodes for which the monitoring session is configured. Traffic health monitoring focuses on identifying any discrepancies (packet drop or overflow etc) in the traffic flow. When any such discrepancies are identified, GigaVUE-FM propagates the health status to corresponding monitoring session. GigaVUE-FM monitors the traffic health status in near real-time. GigaVUE V Series Node monitors the traffic, when the traffic limit goes beyond the upper or lower threshold values that is configured, it notifies GigaVUE-FM, based on which traffic health is computed.

> **NOTE:** When GigaVUE-FM and GigaVUE V Series Nodes are deployed in different cloud platforms, then the GigaVUE-FM public IP address must be added to the **Data Notification Interface** as the Target Address in the Event Notifications page. Refer to section in the *GigaVUE Administration Guide* for configuration details.

This feature is supported for GigaVUE V Series Nodes on the respective cloud platforms:

**For V Series Nodes:**

- AWS
- Azure
- OpenStack
- VMware
- Third Party Orchestration

The following section gives step-by-step instructions on creating, applying, and editing threshold templates across a monitoring session or an application, and viewing the traffic health status. Refer to the following section for more detailed information:

- Supported Resources and Metrics
- Create Threshold Template
- Apply Threshold Template
- Edit Threshold Template
- Clear Thresholds

Keep in mind the following points when configuring a threshold template:

- By default Threshold Template is not configured to any monitoring session. If you wish to monitor the traffic health status, then create and apply threshold template to the monitoring session.
- Editing or redeploying the monitoring session will reapply all the threshold policies associated with that monitoring session.

- Deleting or undeploying the monitoring session will clear all the threshold policies associated with that monitoring session.
- After applying threshold template to a particular application, you need not deploy the monitoring session again.

## Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring

| Resource | Metrics | Threshold types | Trigger Condition |
|---|---|---|---|
| Tunnel End Point | 1. Tx Packets <br> 2. Rx Packets <br> 3. Tx Bytes <br> 4. Rx Bytes <br> 5. Tx Dropped <br> 6. Rx Dropped <br> 7. Tx Errors <br> 8. Rx Errors | 1. Difference <br> 2. Derivative | 1. Over <br> 2. Under |
| RawEnd Point | 1. Tx Packets <br> 2. Rx Packets <br> 3. Tx Bytes <br> 4. Rx Bytes <br> 5. Tx Dropped <br> 6. Rx Dropped <br> 7. Tx Errors <br> 8. Rx Errors | 1. Difference <br> 2. Derivative | 1. Over <br> 2. Under |
| Map | 1. Tx Packets <br> 2. Rx Packets <br> 3. Packets Dropped | 1. Difference <br> 2. Derivative | 1. Over <br> 2. Under |
| Slicing | 1. Tx Packets <br> 2. Rx Packets <br> 3. Packets Dropped | 1. Difference <br> 2. Derivative | 1. Over <br> 2. Under |
| Masking | 1. Tx Packets <br> 2. Rx Packets <br> 3. Packets Dropped | 1. Difference <br> 2. Derivative | 1. Over <br> 2. Under |
| Dedup | 1. Tx Packets | 1. Difference | 1. Over |

| | | | |
|---|---|---|---|
| | 2. Rx Packets<br>3. Packets Dropped | 2. Derivative | 2. Under |
| HeaderStripping | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| TunnelEncapsulation | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| LoadBalancing | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| SSLDecryption | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| Application Metadata | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| AMI Exporter | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| Geneve | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |
| 5G-SBI | 1. Tx Packets<br>2. Rx Packets<br>3. Packets Dropped | 1. Difference<br>2. Derivative | 1. Over<br>2. Under |

## Create Threshold Template

To create threshold templates:

1. There are two ways to navigate to the Threshold Template page, they are:

   a. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Then, click on the **Threshold Template** tab in the top navigation bar.

   b. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a monitoring session, click **Actions > Edit**. In the Edit Monitoring Session page, click **Options > Threshold**.

2. The **Threshold Template** page appears. Click **Create** to open the **New Threshold Template** page.

3. Enter the appropriate information for the threshold template as described in the following table.

| Field | Description |
|---|---|
| **Threshold Template Name** | The name of the threshold template. |
| **Thresholds** | |
| Monitored Objects | Select the resource for which you wish to apply the threshold template. Eg: TEP, REP, Maps, Applications like Slicing, Dedup etc |
| Time Interval | Frequency at which the traffic flow needs to be monitored. |
| Metric | Metrics that needs to be monitored. For example: Tx Packets, Rx Packets. |
| Type | **Difference**: The difference between the stats counter at the start and end time of an interval, for a given metric. <br> **Derivative**: Average value of the statistics counter in a time interval, for a given metric. |
| Condition | **Over**: Checks if the statistics counter value is greater than the 'Set Trigger Value'. <br><br> **Under**: Checks if the statistics counter value is lower than the 'Set Trigger Value'. |
| Set Trigger Value | Value at which a traffic health event is raised, if statistics counter goes below or above this value, based on the condition configured. |
| Clear Trigger Value | Value at which a traffic health event is cleared, if statistics counter goes below or above this value, based on the condition configured. |

4. Click **Save**. The newly created threshold template is saved, and it appears on the **Threshold Template** page.

## Apply Threshold Template

You can apply your threshold template across the entire monitoring session and also to a particular application.

**Apply Threshold Template to Monitoring Session**

To apply the threshold template across a monitoring session, follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. To apply a threshold template across a monitoring session, select the template you wish to apply across the monitoring session from the Threshold Template drop-down menu.
4. Click **Done**.

**Apply Threshold Template to Applications**

To apply the threshold template to a particular application in the monitoring session follow the steps given below:

> **NOTE:** Applying threshold template across monitoring session will not over write the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it over writes the existing threshold value for that particular application.

1. On the **Monitoring Session** page. Click **Actions > Edit**. The Edit Monitoring Session page with canvas page appears.
2. Click on the application for which you wish to apply or change a threshold template and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
4. Click **Save**.

## Edit Threshold Template

To edit a particular threshold template follow the steps given below:

1. On the Threshold Template page, Click **Edit**. The **Edit Threshold Template** page appear.
2. The existing threshold templates will be listed here. Edit the templates you wish to modify.
3. Click **Save**.

> **NOTE:** Editing a threshold template does not automatically apply the template to monitoring session. You must apply the edited template to monitoring session for the changes to take effect.

**Clear Thresholds**

You can clear the thresholds across the entire monitoring session and also to a particular application.

**Clear Thresholds for Applications**

To clear the thresholds of a particular application in the monitoring session follow the steps given below:

1. On the **Monitoring Session** page. Click **Actions > Edit**. The Edit Monitoring Session page with canvas page appears.
2. Click on the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Click on the **Thresholds** tab. Click **Clear All** and then Click **Save**.

**Clear Thresholds across the Monitoring Session**

To clear the applied thresholds across a monitoring session follow the steps given below:

1. In GigaVUE-FM, on the left navigation pane, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears.
2. Select the monitoring session and click **Actions > Apply Thresholds**.
3. The **Apply Thresholds** page appears. Click **Clear**.

> **NOTE:** Clearing thresholds at monitoring session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application refer to Clear Thresholds for Applications

# View Health Status

You can view the health status of the monitoring session on the Monitoring Session details page. The health status of the monitoring session is healthy only if both the configuration health and traffic health are healthy.

**View Health Status of an Application**

To view the health status of an application across an entire monitoring session:

1. After creating a Monitoring Session, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. Select a monitoring session, click **Actions > Edit**. The Edit Monitoring Session Page appears.
2. Click on the application for which you wish to see the health status and select **Details**. The quick view page appears.
3. Click on the **HEALTH STATUS** tab.

This displays the configuration health and traffic health of the application and also the thresholds applied to that particular application.

> **NOTE:** The secure tunnel status is refreshed for every 5 minutes, and the GigaVUE-FM does not display UCT-V secure tunnel status that is older than 7 minutes. If the secure tunnel in the UCT-V is removed, it takes up to 7 minutes to reset the status on the GigaVUE-FM.

**View Health Status for Individual GigaVUE V Series Nodes**

You can also view the health status of the view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Statistics** tab.
3. Select the GigaVUE V Series Node from the **All V Series Nodes** drop-down menu.

**View Application Health Status for Individual V Series Nodes**

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

1. On the Monitoring Session page, click the name of the monitoring session and click **View**.
2. Select the **Statistics** tab.
3. Select the GigaVUE V Series Node from the **All V Series Nodes** drop-down menu.
4. The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

You can also view the cloud health Status in the Monitoring Session Page, refer to View Health Status on the Monitoring Session Page topic for more detailed information on how to view cloud health status in the Monitoring Session page.

# Configure VMware 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.

To configure the VMware Settings:

Go to **Inventory > VIRTUAL > VMware NSX-T (V Series)**, and then click **Settings > Advanced Settings** to edit the VMware V Series NSX-T settings.

Advanced Settings

| | |
|---|---|
| Maximum number of vCenter connections allowed | 20 |
| Refresh interval for VM target selection inventory (secs) | 300 |
| Refresh interval for fabric deployment inventory (secs) | 86400 |
| Traffic distribution tunnel range start | 8000 |
| Traffic distribution tunnel range end | 8512 |
| Traffic distribution tunnel MTU | 9001 |
| Maximum V Series node up wait time in minutes | 5 |

Refer to the following table for details:

| Settings | Description |
|---|---|
| **Maximum number of vCenter connections allowed** | Specifies the maximum number of vCenter connections you can establish in GigaVUE-FM |
| **Refresh interval for VM target selection inventory (secs)** | Specifies the frequency for updating the state of target VMs in VMware vCenter |
| **Refresh interval for fabric deployment inventory (secs)** | Specifies the frequency for updating the state of GigaVUE-FM fabrics deployed in VMware vCenter |
| **Traffic distribution tunnel range start** | Specifies the start range value of the tunnel ID. |
| **Traffic distribution tunnel range end** | Specifies the closing range value of the tunnel ID. |
| **Traffic distribution tunnel MTU** | Specifies the Tunnel MTU value. |
| **Maximum V Series Node up wait time** | Specifies the maximum amount of time taken for the GigaVUE Series Node state to go to OK. |

# Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics[1] you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. Refer to Analytics topic in *GigaVUE Fabric Management Guide* for more detailed information on Analytics.

---

[1]Analytics uses the OpenSearch front-end application to visualize and analyze the data in the OpenSearch database of GigaVUE-FM.

**Rules and Notes:**

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the Clone Dashboard section for more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.

## Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. Refer to the Analytics section in *GigaVUE Fabric Management Guide* for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

To access the dashboards:

1. Go to ▣ -> **Analytics -> Dashboards.**
2. Click on the required dashboard to view the visualizations.

The following table lists the various virtual dashboards:

| Dashboard | Displays | *Visualizations* | Displays |
|---|---|---|---|
| *Inventory Status (Virtual)* | Statistical details of the virtual inventory based on the platform and the health status.<br>You can view the following metric details at the top of the dashboard:<br>• Number of Monitoring Sessions<br>• Number of V Series Nodes<br>• Number of Connections<br>• Number of GCB Nodes<br>You can filter the visualizations based on the following control filters:<br>• Platform<br>• Health Status | *V Series Node Status by Platform* | Number of healthy and unhealthy V Series Nodes for each of the supported cloud platforms. |
| | | *Monitoring Session Status by Platform* | Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms |
| | | *Connection Status by Platform* | Number of healthy and unhealthy connections for each of the supported cloud platforms |
| | | *GCB Node Status by Platform* | Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms |
| *V Series Node Statistics* | Displays the Statistics of the V Series node such as the CPU usage, trend of the | *V Series Node Maximum CPU Usage Trend* | Line chart that displays maximum CPU usage trend of |

| Dashboard | Displays | *Visualizations* | Displays |
|---|---|---|---|
| | receiving and transmitting packets of the V Series node.<br><br>You can filter the visualizations based on the following control filters:<br><br>• Platform<br>• Connection<br>• V Series Node | | the V Series node in 5 minutes interval, for the past one hour.<br><br>NOTE: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V-series nodes do not have service cores, therefore the CPU usage is reported as 0. |
| | | *V Series Node with Most CPU Usage For Past 5 minutes* | Line chart that displays Maximum CPU usage of the V Series node for the past 5 minutes.<br><br>NOTE: You cannot use the time based filter options to filter and visualize the data. |
| | | *V Series Node Rx Trend* | Receiving trend of the V Series node in 5 minutes interval, for the past one hour. |
| | | *V Series Network Interfaces with Most Rx for Past 5 mins* | Total packets received by each of the V Series network interface for the past 5 minutes.<br><br>NOTE: You cannot use the time based filter options to filter and visualize the data. |
| | | *V Series Node Tunnel Rx Packets/Errors* | Displays the reception of packet at the Tunnel RX. This is the input to V Series Node, Grouping |

| Dashboard | Displays | *Visualizations* | Displays |
|---|---|---|---|
| | | | by tunnel identifier comprising {monDomain, conn, VSN, tunnelName}, before aggregation. |
| | | *V Series Node Tunnel Tx Packets/Errors* | TX is for output tunnels from VSN. V Series Node Tunnel Tx Packets/Errors |
| *Dedup* | Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters:<br>• Platform<br>• Connection<br>• VSeries Node | *Dedup Packets Detected/Dedup Packets Overload* | Statistics of the total dedup packets received (ipV4Dup, ipV6Dup and nonIPDup) against the dedup application overload. |
| | | *Dedup Packets Detected/Dedup Packets Overload Percentage* | Percentage of the dedup packets received against the dedup application overload. |
| | | *Total Traffic In/Out Dedup* | Total incoming traffic against total outgoing traffic |
| **Tunnel (Virtual)** | Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated:<br>• **Monitoring session**: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V-series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it.<br>• **V series node**: Management IP of the V Series node. Choose the required V-series node from the drop-down. | *Tunnel Bytes* | Displays received tunnel traffic vs transmitted tunnel traffic, in bytes.<br>• For input tunnel, transmitted traffic is displayed as zero.<br>• For output tunnel, received traffic is displayed as zero. |

| Dashboard | Displays | *Visualizations* | Displays |
|---|---|---|---|
| | • **Tunnel:** Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out.<br><br>The following statistics are displayed for the tunnel: | | |
| | | *Tunnel Packets* | Displays packet-level statistics for input and output tunnels that are part of a monitoring session. |
| | • Received Bytes<br>• Transmitted Bytes<br>• Received Packets<br>• Transmitted Packets<br>• Received Errored Packets<br>• Received Dropped Packets<br>• Transmitted Errored Packets<br>• Transmitted Dropped Packets | | |
| **App (Virtual)** | Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V series node.<br><br>You can select the following control filters, based on which the visualizations will get updated:<br><br>• **Monitoring session**<br>• **V series node**<br>• **Application**: Select the required application. By default, the visualizations displayed includes all the applications.<br><br>By default, the following statistics are displayed:<br><br>• Received Bytes<br>• Transmitted Bytes<br>• Received Packets<br>• Transmitted Packets<br>• Errored Packets<br>• Dropped Packets | *App Bytes* | Displays received traffic vs transmitted traffic, in Bytes. |

| Dashboard | Displays | *Visualizations* | Displays |
|---|---|---|---|
| | | *App Packets* | Displays received traffic vs transmitted traffic, as the number of packets. |
| **End Point (Virtual)** | Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V-series nodes.<br><br>The following statistics that are shown for Endpoint (Virtual):<br><br>• Received Bytes<br>• Transmitted Bytes<br>• Received Packets<br>• Transmitted Packets<br>• Received Errored Packets<br>• Received Dropped Packets<br>• Transmitted Errored Packets<br>• Transmitted Dropped Packets<br><br>The endpoint drop-down shows *<V-series Node Management IP address : Network Interface>* for each endpoint.<br><br>You can select the following control filters, based on which the visualizations will get updated:<br><br>• **Monitoring session**<br>• **V Series node**<br>• **Endpoint:** Management IP of the V Series node followed by the Network Interface (NIC) | *Endpoint Bytes* | Displays received traffic vs transmitted traffic, in Bytes. |
| | | *Endpoint Packets* | Displays received traffic vs transmitted traffic, as the number of packets. |

> **NOTE:** The Tunnel (Virtual), App (Virtual) and Endpoint (Virtual) dashboards do not show data from the previous releases if the *Monitoring Session [Platform : Domain : Connection]* dashboard filter is applied. This is because, this filter relies on the new attributes in the OpenSearch database, which are available only from software version 5.14.00 and beyond.

# GigaVUE V Series Deployment Clean up

On installation failure or incomplete service removal, you must clean up GigaVUE V Series Nodes before reattempting the installation. To clean up the V Series deployments from NSX-T and GigaVUE-FM, perform the following steps:

- Remove Service Profiles
- Remove Service Deployments
- Remove Service Reference
- Remove Service Manager
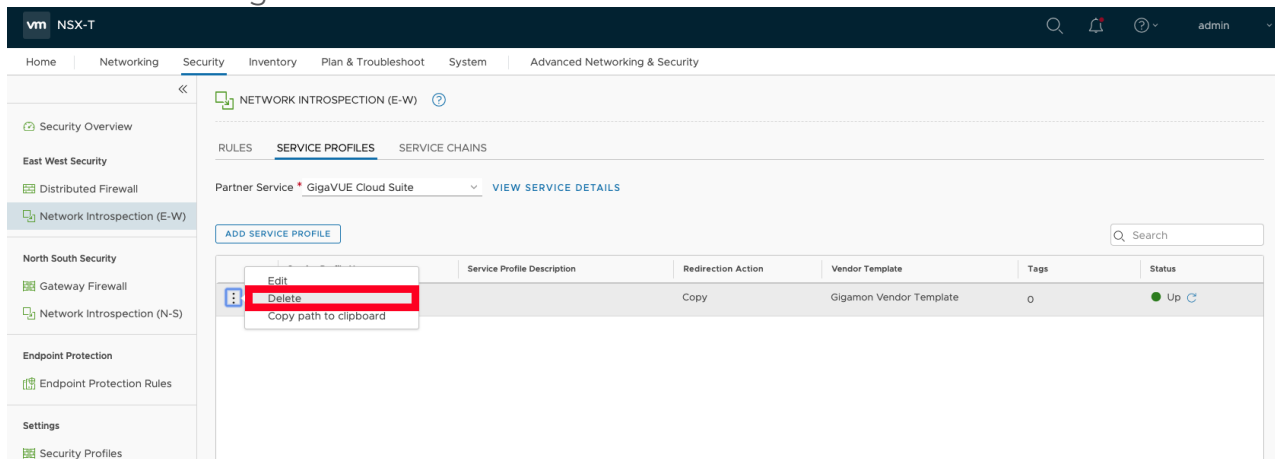- Remove Vendor Template and Service Definition

## Remove Service Profiles

To remove Service Profiles:

1. From NSX-T Manager, navigate to **Security > Network Introspection (E-W)**.
2. In the **SERVICE PROFILES** tab, select the **GigaVUE Cloud Suite** partner service.
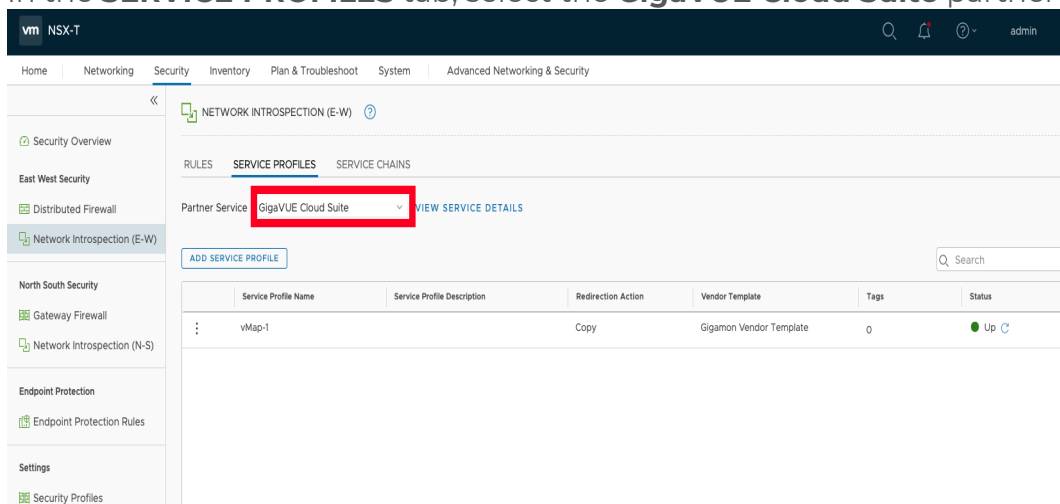


3. Delete all existing Service Profiles.

## Remove Service Deployments

To remove Service Deployments:

1. From NSX-T Manager, navigate to **System > Service Deployments**.
2. In the **DEPLOYMENT** tab, Select the **GigaVUE Cloud Suite** partner service.



3. Delete all the existing Service Deployments.



To remove the Service Deployments through NSX-T API:

1. Login to Postman.
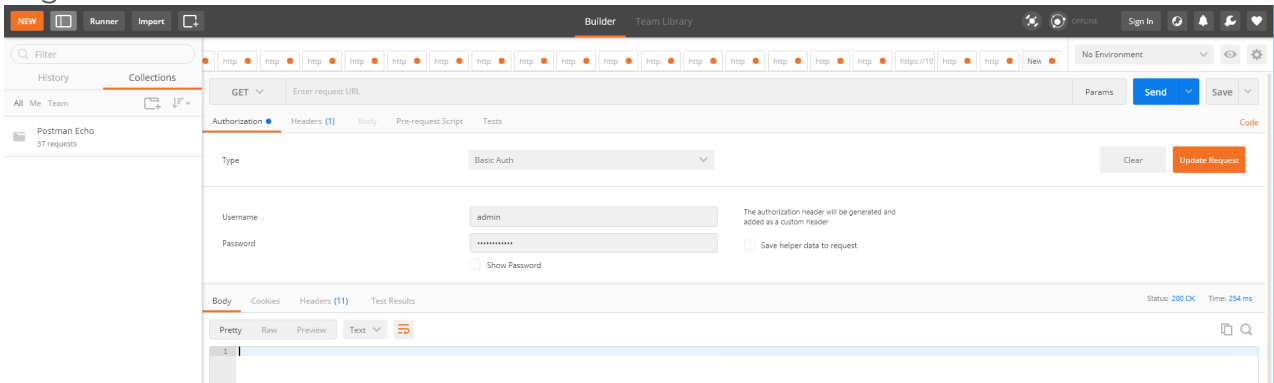


2. Get the Service ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/

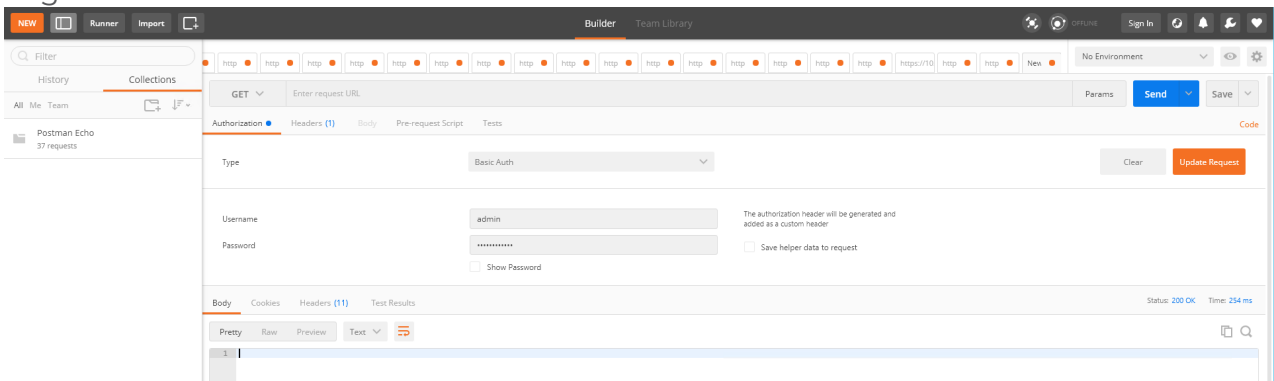3. Get the ID of the Service Deployments.**GET** https://<NSX_Manager_ IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/

4. Delete all Service Deployments.**DELETE** https://<NSX_Manager_ IP>/api/v1/serviceinsertion/services/<Service_ID>/service-deployments/<Service_ Deployment_ID>

## Remove Service Reference

To remove Service References through NSX-T API:

1. Login to Postman.
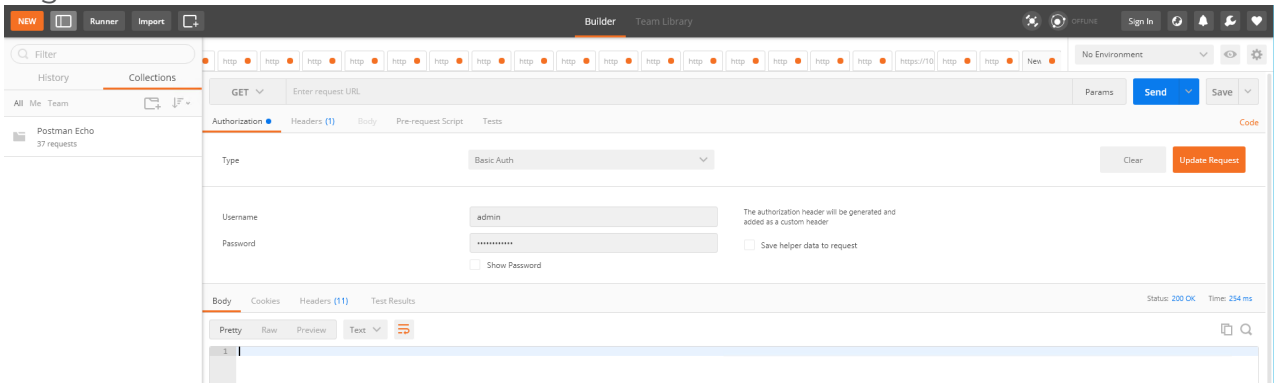


2. Get the Service Reference ID.**GET** https://<NSX_Manager_IP>/policy/api/v1/infra/service-references/

3. Delete the Service Reference.**DELETE** https://<NSX_Manager_ IP>/policy/api/v1/infra/service-references/<Service_Reference_ID>

## Remove Service Manager

To remove Service Manager through NSX-T API:

1. Login to Postman.



2. Get the Service Manager ID.**GET** https://<NSX_Manager_
   IP>/api/v1/serviceinsertion/service-managers/

3. Delete the Service Manager.**DELETE** https://<NSX_Manager_
   IP>/api/v1/serviceinsertion/serivce-managers/<Service_Manager_ID>

## Remove Vendor Template and Service Definition

To remove Vendor Template and Service Definition through NSX-T API:

1. Login to Postman.
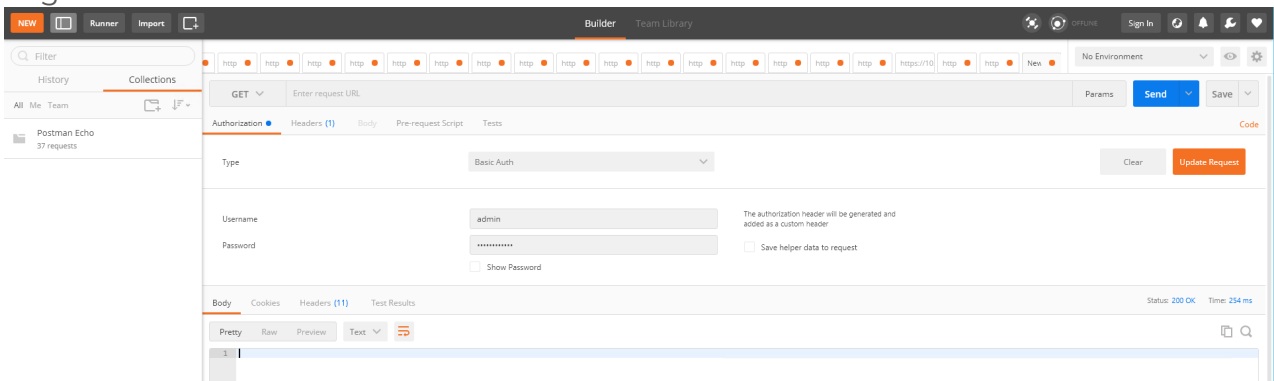


2. Get the Service ID.**GET** https://<NSX_Manager_IP>/api/v1/serviceinsertion/services/

3. Get the Vendor Templates' ID.**GET** https://<NSX_Manager_
   IP>/api/v1/serviceinsertion/services/<Service_ID>/vendor-templates/

4. Delete the Vendor Templates.**DELETE** https://<NSX_Manager_
   IP>/api/v1/serviceinsertion/services/<Service_ID>/vendor-templates/<Vendor_Template_
   ID>

5. Delete the Service.**DELETE** https://<NSX_Manager_
   IP>/api/v1/serviceinsertion/services/<Service_ID>

# 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 VÜE Community

## Documentation

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

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

*Table 1: Documentation Set for Gigamon Products*

| GigaVUE Cloud Suite 6.5 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**<br>how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices |
| **GigaVUE-HC1 Hardware Installation Guide** |
| **GigaVUE-HC2 Hardware Installation Guide** |
| **GigaVUE-HC3 Hardware Installation Guide** |
| **GigaVUE-HC1-Plus Hardware Installation Guide** |
| **GigaVUE-HCT Hardware Installation Guide** |
| **GigaVUE-TA25 Hardware Installation Guide** |
| **GigaVUE-TA25E Hardware Installation Guide** |
| **GigaVUE-TA100 Hardware Installation Guide** |

| GigaVUE Cloud Suite 6.5 Hardware and Software Guides |
|---|
| GigaVUE-TA200 Hardware Installation Guide |
| GigaVUE-TA200E Hardware Installation Guide |
| GigaVUE-TA400 Hardware Installation Guide |
| GigaVUE-OS Installation Guide for DELL S4112F-ON |
| G-TAP A Series 2 Installation Guide |
| GigaVUE M Series Hardware Installation Guide |
| GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW |
| **Software Installation and Upgrade Guides** |
| GigaVUE-FM Installation, Migration, and Upgrade Guide |
| GigaVUE-OS Upgrade Guide |
| GigaVUE V Series Migration Guide |
| **Fabric Management and Administration Guides** |
| GigaVUE Administration Guide<br>covers both GigaVUE-OS and GigaVUE-FM |
| GigaVUE Fabric Management Guide<br>how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features |
| **Cloud Guides**<br>how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms |
| GigaVUE V Series Applications Guide |
| GigaVUE V Series Quick Start Guide |
| GigaVUE Cloud Suite Deployment Guide - AWS |
| GigaVUE Cloud Suite Deployment Guide - Azure |
| GigaVUE Cloud Suite Deployment Guide - OpenStack |
| GigaVUE Cloud Suite Deployment Guide - Nutanix |
| GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) |
| GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T) |
| GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration |
| Universal Cloud Tap - Container Deployment Guide |

| GigaVUE Cloud Suite 6.5 Hardware and Software Guides |
|---|
| **Gigamon Containerized Broker Deployment Guide** |
| **GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide** |
| GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions |
| **Reference Guides** |
| **GigaVUE-OS CLI Reference Guide**<br>library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices |
| **GigaVUE-OS Security Hardening Guide** |
| **GigaVUE Firewall and Security Guide** |
| **GigaVUE Licensing Guide** |
| **GigaVUE-OS Cabling Quick Reference Guide**<br>guidelines for the different types of cables used to connect Gigamon devices |
| **GigaVUE-OS Compatibility and Interoperability Matrix**<br>compatibility information and interoperability requirements for Gigamon devices |
| **GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide**<br>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**<br>new features, resolved issues, and known issues in this release ;<br>important notes regarding installing and upgrading to this release<br><br>**NOTE:** Release Notes are not included in the online documentation.<br><br>**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**<br>how to install, deploy, and operate GigaVUE-FM. |

## How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

## Documentation Feedback

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

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

| Documentation Feedback Form | | |
|---|---|---|
| **About You** | **Your Name** | |
| | **Your Role** | |
| | **Your Company** | |
| | | |
| **For Online Topics** | **Online doc link** | *(URL for where the issue is)* |
| | **Topic Heading** | *(if it's a long topic, please provide the heading of the section where the issue is)* |
| | | |

| For PDF Topics | Document Title | *(shown on the cover page or in page header )* |
| --- | --- | --- |
| | Product Version | *(shown on the cover page)* |
| | Document Version | *(shown on the cover page)* |
| | Chapter Heading | *(shown in footer)* |
| | PDF page # | *(shown in footer)* |
| | | |
| How can we improve? | Describe the issue | *Describe the error or issue in the documentation.* <br> *(If it helps, attach an image to show the issue.)* |
| | How can we improve the content? <br><br> 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 contact 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 VÜE Community

The VÜE 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 VÜE 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.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

**Register today at** community.gigamon.com

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

# Glossary

**D**

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

**F**

forward list

selective forwarding - forward (formerly whitelist)

**L**

leader

leader in clustering node relationship (formerly master)

**M**

member node

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

**N**

no-decrypt list

no need to decrypt (formerly whitelist)

### nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

## P

### primary source

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

## R

### receiver

follower in a bidirectional clock relationship (formerly slave)

## S

### source

leader in a bidirectional clock relationship (formerly master)