Gigamon®

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.12

Document Version: 1.0

(See Change Notes for document updates.)

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.12	1.0	10/27/2025	The original release of this document with 6.12.00 GA.

Contents

Gigamon Containerized Broker

Gigamon Containerized Broker (GCB) is a containerized component that runs inside a container. It provides the network broker features. GCB can perform traffic acquisition, aggregation, basic filtering, replication, and tunneling with encryption support.

You can run GCB as its own Pod in your Kubernetes service, where your workloads are running. GCB receives traffic from many sources, depending on your setup and goals.

This guide provides an overview of Gigamon Containerized Broker and describes how to install and deploy the GCB components in your Pods.

Topics:

To learn more about Universal Cloud Tap - Container (UCT-C), refer to Universal Cloud Tap - Container Guide.

About Gigamon Containerized Broker

The Gigamon Containerized Broker (GCB) is a containerized component that provides the network broker features in a containerized form. Kubernetes orchestrator, not GigaVUE-FM, deploys GCB.

Following are the modules implemented in GCB:

- **Traffic Acquisition using CNI Modules**: GCB supports traffic acquisition by reading the traffic from the Container Network Interface (CNI) modules like AWS ENI, Calico, and Flannel. During initialization, GCB receives the configuration information from the Gigamon's YAML file. Kubernetes CNI (Container Network Interface) supports ingress, egress, and management process. GCB uses the YAML settings to configure itself on the worker node and start capturing traffic.

  NOTE: After GCB registration, you cannot change the number of CNI, and CNI types. If required, a new GCB instance configured and registered.

- **Traffic Aggregation:** When GCB is running in its own Pod, GCB itself serves as a traffic aggregator.
- **Filtering Module:** GCB supports basic filtering, forwarding policy, and enrichment. You can define protocol-based filters in the YAML file. It pushes filtering rules to GCB, and you can update these rules while while GCB is running.
- **Tunneling Modules:**GCB supports L2GRE and VXLAN tunneling modules.
- **Encryption Module** - GCB maintains the required certificates to support TLS and HTTPS encryption.

GCB and GigaVUE-FM Interaction

This topic explains different ways of interaction between GCB and GigaVUE-FM:

- GCB Registration
- GCB Deregistration
- GCB Heartbeats
- GCB Statistics
- Monitoring Domain and Traffic Policy

GCB Registration

When starting in a Kubernetes environment, GCB automatically registers itself with GigaVUE-FM. When GigaVUE-FM is unreachable, GCB tries to connect with five retries of increasing time periods. If the GigaVUE-FM is unreachable even after all retries, the deployment fails. GCB only supports the IPv4 protocol.

GCB Deregistration

When terminated normally, GCB sends the deregistration message to GigaVUE-FM. If GCB shuts down abruptly, it might not deregister. As a result,

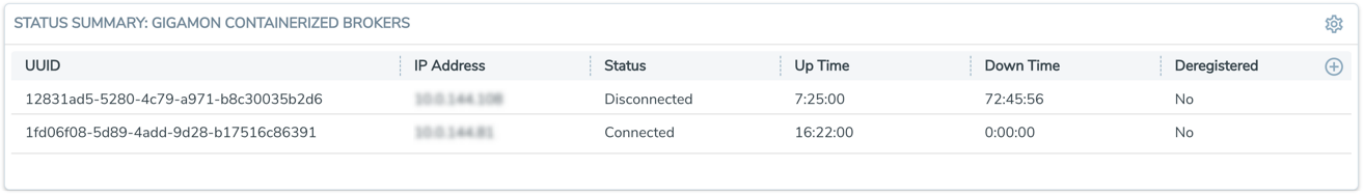
- The GCB Pods might move to the other GCB node.
- The feeding UCT Containers are moved to the other GCB.
- GigaVUE-FM does not store information of the GCB Pod.

GCB Heartbeats

GCB sends heartbeats Periodically to GigaVUE-FM. By default, the status of GCB appears **Connected**.

GCB status according to the hearbeat behaviour:

- **Disconnected**: 3 consecutive heartbeats missed.
- **Pending**: 2 consecutive heartbeats are missed.
- If GigaVUE-FM does not receive GCB heartbeats for 30 days, then GigaVUE-FM removes the GCB, considering it as stale.



GCB Statistics

GCB sends traffic statistics and associated GCB Pods to GigaVUE-FM. GigaVUE-FM dashboard displays the details of 10 highest and 10 lowest GCB traffic statistics.

GCB continues to send the statistics even when traffic does not flow. The GCB statistics are not stored in cache even when GigaVUE-FM is not reachable by GCB at that instant of time.

Monitoring Domain and Traffic Policy

You can configure and manage the Monitoring Domains, Traffic Policies, Connections, Metadata fields, and Source Inventories of GCB in GigaVUE-FM. For details on the REST APIs of GCB, refer to the *GigaVUE-FM REST API Reference*.

- A Traffic Policy is a combination of Rules and Tunnels.
- A rule contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic.
- A tunnel is a communication path in which the traffic matching the filtered criteria is routed to the destination. The tunnel supports ipv4 and ipv6 addresses.

GCB Traffic Health Monitoring

GigaVUE-FM checks the following to monitor the traffic health of GCB:

- Configuration Health
- Traffic Health
- Resource Utilization Health
- Connectivity Health

In GigaVUE-FM, you can view, drill down or alarm source, filter, and manage one or more alarms. When configuring, GigaVUE-FM allows to set the threshold conditions so that the GCB node raises alarms when those threshold conditions are met.

Configure Alarms in GCB

You can configure alarms in GCB, after registering it with GigaVUE-FM. To register, refer to GCB Registration.

To configure Alarms,

1. Go to **Inventory** > **Container** > **Gigamon Containerized Broker**.
2. From the **Settings** drop-down list box, select **Settings**.
3. Select the **GCB UUID**, and then select **Thresholds** near the GCB UUID to configure the health monitoring threshold:
   You can configure the following:

- Configuration HealthTo configure the thresholds for monitoring the configuration health, expand **Configuration Health** and configure the parameters as described in the table.
- Traffic Health: To configure the thresholds for monitoring the traffic health, expand **Data Transmission** and configure the parameters as described in the table.
- Resource HealthTo configure the thresholds for monitoring the traffic health, expand **Invalid RxData**and configure the parameters as described in the table.
- Connectivity Health: To configure the thresholds for monitoring the traffic health, expand **Transaction Logging** and configure the parameters as described in the table.

Configuration Health

To monitor the configuration health, you can configure the thresholds for the following:

S. No.	Name	Monitors	Description	Trigger Value Type	Trigger Value Range	Minimum - Maximum Timer Interval	Default Trigger Value	Default time	Conditions	Severity	Status
1	ServiceIdTableMiss	Either of source or destination table does not exist, or both the tables does not exist.	Alarms are raised when the user fails to upload any one of src / dst table or both ServiceIdTableMiss.	Integer	1-10	300-6000	1	300 sec	above	Critical	ON
2	SvcIdLookupMiss	Entry lookup miss in svc-id table	Alarms are raised when service ID lookup fails for incoming traffic SvcIdLookupMiss.	Integer	10-5000	300-6000	1000	300 sec	above	Major	ON
3	GCBLogfile Truncated	Indicates the logging file truncation (Notification)	Alarms are raised when gcb http pod log is rotated and fresh logging starts GCBLogfile Truncated .	Integer	1-10	300-6000	5	300 sec	above		ON

Traffic Health

To monitor the traffic health, you can configure the thresholds for the following:

S. No.	Name	Monitors	Description	Trigger Value Type	Trigger Value Range	Minimum - Maximum Timer Interval	Default Trigger Value	Default time	Conditions	Severity	Status
1	TransmitErrors	Errors in transmitting packets out through tunnel.	Alarms are raised when tx errors are observed in the http pod TransmitErrors.	Integer	10-100	60-600	100	60 sec	above	Major	ON
2	TransactionLoggingErrors	Transaction Logging failures	Alarms are raised when transaction logging to the designated file fails TransactionLoggingErrors.	Integer	10-100	60-600	100	60 sec	above	Major	OFF
3	PacketReordererTimeouts	Packet reordering triggered timeout or transaction packet discards	Alarms are raised when reordering of the incoming packet is not successful/completed in the defined time interval PacketReordererTimeouts	Integer	1-100	60-600	1	60 sec	above	Major	OFF

Resource Health

To monitor the resource health, you can configure the thresholds for the following:

S. No.	Name	Monitors	Trigger Value Type	Description	Trigger Value Range	Minimum - Maximum Timer Interval	Default Trigger Value	Default time	Conditions	Severity	Status
1	InvalidPostDataReceived	Missing the POST data or Invalid Binary data or wrong pcap files	Integer	Alarms are raised when invalid post data is received by the pod InvalidPostDataReceived.	1-10	60-600	10	300 sec	above	Major	ON

Connectivity Health

To monitor the connectivity health, you can configure the thresholds for the following:

S. No.	Name	Monitors	Description	Trigger Value Type	Trigger Value Range	Minimum - Maximum Timer Interval	Default Trigger Value	Default time	Conditions	Severity	Status
1	PcapperConnectionFailure	Datapath connection failure	Alarms are raised when connectivity fails between pcapper and http service pcapper connection	Integer	1-10	60-300	3	60 sec	equal	Critical	ON
2	Controller2FM Connectivity	GigaVUE-FM reachability issues from GCB-Controller		Integer	1-10		3	300 sec	equal	Critical	OFF
3	GCB2Controller Connectivity	Controller unreachable from GCB		Integer	1-10		3	300 sec	equal	Critical	OFF

The YAML updates are as follows:

```
- name: GCB_ALARM_GROUP_NAME
value: "alarm group name"
# 0 - disabled, 1 - enabled
- name: GCB_ALARM_HMON_SUPPORTED
```

```
      value: '0'
```

For more information about Alarms, refer to the Alarms section in the GigaVUE Administration Guide.

GCB Diameter Traffic Processing

The Gigamon Containerized Broker (GCB) processes Service Based Interface Application (SBI) and Diameter traffic from the Pcapper.

GigaVUE-FM supports a new traffic type parameter. You can opt between SBI or Diameter values. With the introduction of Diameter Traffic, each monitoring domain now supports two traffic policies - one for SBI traffic and one for Diameter traffic. You can add filter rules to each policy based on metadata..

Supported featuress for SBI and Diameter traffic:

Features	SBI	Diameter
Reorder packets	Supported	Supported
Transaction Logging	Supported	Supported
Service Identification	Supported	Supported

To configure Diameter Traffic Processing, see Configuration of GCB Diameter Traffic Processing

This section also describes about:

- Service Identification
- Pod Status
- Upgrade

Service Identification

In GigaVUE-FM, you can enable or disable service identification for SBI and Diameter Traffic for GCB.

Pod Status

GigaVUE-FM supports a new pod status called Terminated. The status and the conditions are explained in the following table:

Status	Condition
Terminated	GCB de-registers with GigaVUE-FM.
Pending	GCB loses heartbeat with GigaVUE-FM. for more than 10 minutes, but less than 15 minutes.
Disconnected	GCB loses heartbeat with GigaVUE-FM. for more than 15 minutes..
Connected	If GCB is not in the status mentioned in the previous rows, then GigaVUE-FM. set it as connected.

Upgrade

You must upgrade the GCB controller and the GCB HTTP pod to the same version. Do not use different versions. Unmatched versions can cause problems.

Configuration of GCB Diameter Traffic Processing

This section explains information regarding the following:

- Configure Traffic Policy
- Configure GCB Settings

Rules and Notes

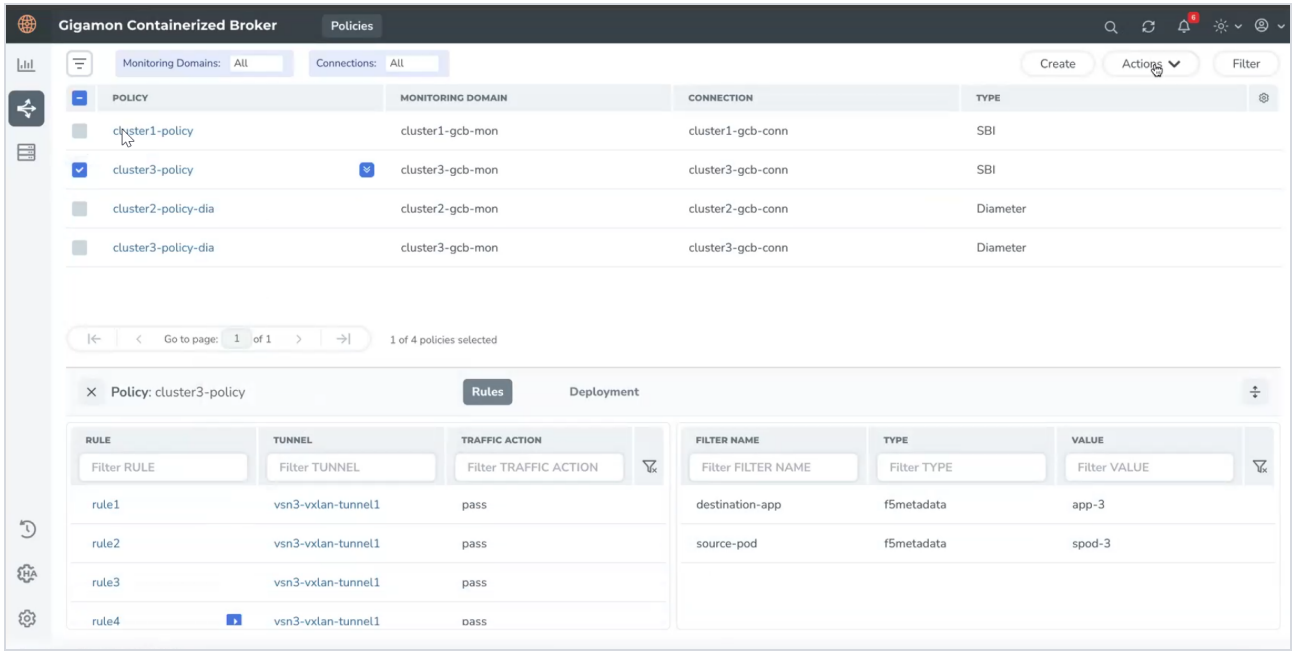
- Each GCB instance requires a minimum of 3 CPUs for better performance.

Configure Traffic Policy

To create a Traffic Policy in GigaVUE-FM,

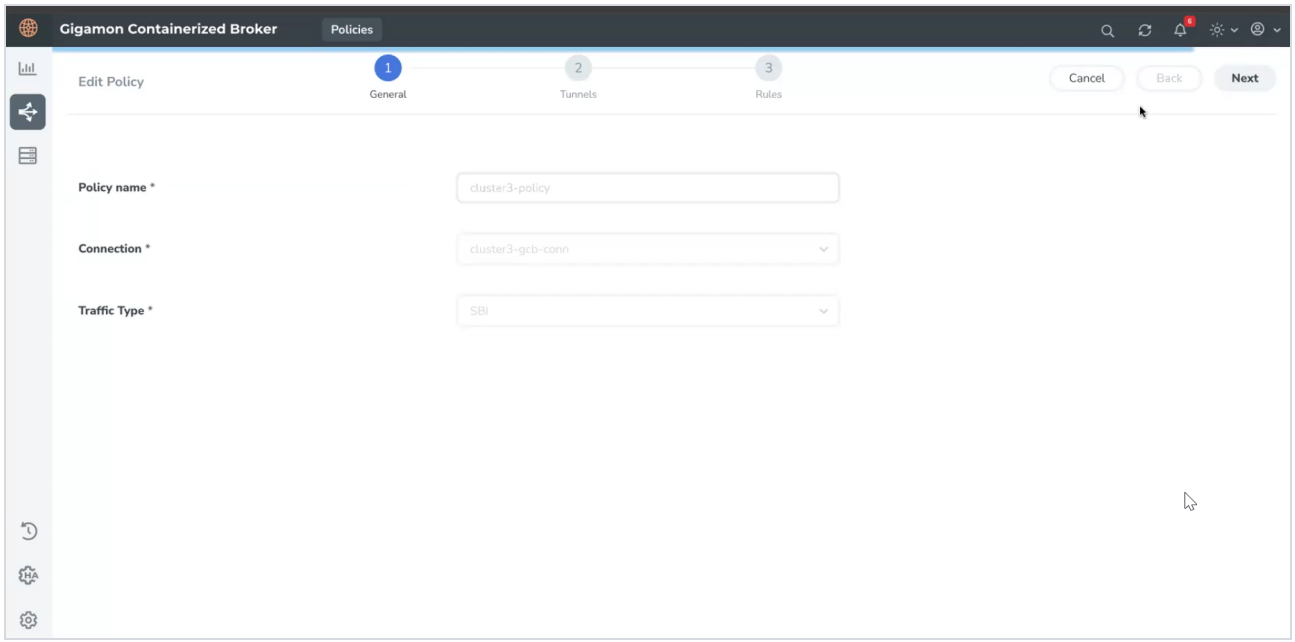
1. From the left pane of GigaVUE-FM, select **Traffic** > **CONTAINER** > **Gigamon Containerized Broker**.

   The Traffic Policy page appears



2. On the **Traffic Policy** page, select **Create**.

   The Create Policy page appears.



3. In the **General** tab page, enter or select the required information:
   a. **Policy Name:** Enter a name for the policy. The Policies with the same name are allowed when the traffic source for one policy is SBI and another is Diameter. In such cases, Traffic Type helps to differentiate between SBI and Diameter traffic.
   b. **Connection:** Select a connection for the policy.
   c. **Traffic Type:** Select one of the following traffic types:
      - **SBI:** To create rules for the Service Based Interface (SBI) Application traffic.
      - **Diameter:** To create rules for the Diameter traffic.
4. Select **Next** to switch to the **Tunnels** tab.
5. Enter or select the required information:
   a. **Tunnel Name:** Name of the tunnel.
   b. **Remote IP Address:** IP Address of the Tunnel.
   c. **Tunnel Type:** Select L2GRE or VXLAN as the tunnel type.
   d. **Tunnel Key:** Enter a value for the tunnel key.
   e. **Destination Port:** If the tunnel type is VXLAN, enter the tunnel destination port number.
   f. **Tool MTU:** Enter the Tool MTU value. Enter a value between 156 and 9216. When GCB sends the TCP packets through VXLAN or GRE tunnels, GigaVUE-FM uses the specified Tool MTU value to segment the captured packets before sending them to the tool to avoid fragmentation.

      - By default, GigaVUE-FM displays the Interface MTU value from the GCB Settings page in the Tool MTU field. For more details on Interface MTU value, refer to the General Settings section in Configure GCB Settings.
      - Modifying the Tool MTU value is effective only if the functionality is enabled in GCB Settings.
      - If you do not specify any Tool MTU value, the packets are not segmented.
      - GigaVUE-FM displays an error if the specified Tool MTU value exceeds the Interface MTU value (default value configured in GCB Settings).

6. Switch to **Rules** tab. Click ⊕ to add another filter and click ⊖ to remove an existing filter.

7. Enter or Select information for the following:

   a. **Name:** Enter a name for the Rule.

   b. **Destination Name:** Select a tunnel destination.

   c. **Pass:** Select Pass to allow the packets. Select **New Filter** from the **Actions** drop-down to add filters for the rule.

   d. **Type:** Select one of the following types:

   - **F5 Metadata:** Provide a Metadata field name and value when you select this option. Such fields that are part of request-metadata and answer-metadata, enter with a "." notation. For example: answer-metadata.error.
   - **Kubernetes:** Provide a value for the service, when you select this option.

     NOTE: For Diameter Traffic, Kubernetes filter type is not supported.

   e. **Filter Value:** Enter a value for the filter type.

   NOTE: GCB supports 128 policy rules, each with two filters.

8. Select **Create**.

   The new Traffic Policy deploys itself in GCB.

The Traffic Policy processes the traffic and forwards the traffic to the tunnel destination IP address.

Configure GCB Settings

You can configure and edit the following GCB settings in GigaVUE-FM:

- General Settings
- SBI Settings
- Diameter Settings

General Settings

In the General Settings, you can view the following details in a list view:

- Monitoring Domain
- Connection GCB UUID
- Name
- IP Address

- Group: For GCB, use a different group name while registering GCB HTTP pod.
- Status: In the General settings, you can also specify the purge interval to automatically remove the settings disconnected for a long duration.

To view or edit the general settings,

1. In GigaVUE-FM, navigate to **Inventory** > **CONTAINER** > **Gigamon Container Broker Settings** > **Settings**, the Settings page appears. From the **Settings** page, on the **General** section, you can view details of the monitoring domain that are configured in GCB.
2. Select a GCB UUID.
   The Wizard displays a split view of the following:
   - General Settings
   - SBI
   - Diameter Settings
   - Thresholds
3. Select **General Settings**>**Edit** to edit/view the following individual settings:
   - Log level
   - Log File Size
   - PCAP File Generation
   - Number of PCAP files generated
   - Tool MTU
   - Interface MTU (read-only value)
   - Tunnel Keepalive

- You can choose to enable or disable the **Tool MTU** option for individual GCB or a GCB group:
  a. Enable - If enabled, GigaVUE-FM segments the packets received by the configured pods before sending them to the tool.
  b. Disable - If disabled, the packet segmentation does not happen, and the packets are forwarded to the tool in their actual state.
- GigaVUE-FM displays a default Interface MTU value, and you cannot edit this value. Interface MTU value provides information about the platform's infrastructure MTU value. You cannot change the platform MTU value. As a result, a read-only value is displayed. The Tool MTU value should always be lesser than the Interface MTU value. For details on Tool MTU value, refer to Configuration of GCB Diameter Traffic Processing.

- The Tunnel Keepalive function helps to keep the sessions on V Series Node alive when traffic is not available. You can choose to enable or disable the **Tunnel Keepalive** option for individual GCB or a GCB group:
  a. Enable: If enabled, keepalive packets is sent to the tool to check if the tool can process the data packets. Keepalive packets will be sent at periodic intervals of one second.
  b. Disable: If disabled, keepalive packets is not sent to the tool.

4. Select **Save**.
   General Settings is updated.

NOTE: To apply all the settings to the members of Group, enable the **Unify All Settings** check box.

SBI Settings

1. In GigaVUE-FM, navigate to **Inventory** > **CONTAINER** > **Gigamon Container Broker Settings** > **Settings**.
   The Settings page appears.
2. From the **Settings** page, on the **General** section, you can view details of the Monitoring Domain configured in GCB.
3. Select a **GCB UUID**, and the Wizard provides a split view of the following:
   - General Settings
   - SBI
   - Diameter Settings
   - Thresholds
4. Select **SBI** > **Edit** to edit/view the following Individual and Group settings.

Individual Settings	Group Settings
• SBI transaction Logging • Write SBI Transaction Log to a file • Write SBI Transaction Log to stdout • SBI Transaction Log Format • SBI Transaction Log File Size	• Enable/Disable packet reordering functionality. • Use Sequence number for packet reordering. • Use timestamp for packet reordering. • Packet reordering timeout in milliseconds. • Maximum number of requests stored in queue. • Packet reordering drop policy. • SBI Service Translation enable/disable.

5. Select **Save**.
   The SBI Settings reflects the updates.

Diameter Settings

1. In GigaVUE-FM, navigate to **Inventory** > **CONTAINER** > **Gigamon Container Broker Settings** > **Settings**. The Settings page appears.
2. From the **Settings** page, on the General section, you can view the details of the monitoring domain configured in GCB.
3. Select a **GCB UUID**. The wizard provides a split view of the following details:
   - General Settings
   - SBI
   - Diameter Settings
   - Thresholds
4. Select **Diameter** > **Edit** to edit/view the following Individual and Group settings.

Individual Settings	Group Settings
• Diameter transaction Logging • Write Diameter Transaction Log to a file • Write Diameter Transaction Log to stdout • Diameter Transaction Log Format • Diameter Transaction Log File Size	• Enable/Disable packet reordering functionality. • Use timestamp for packet reordering. • Packet reordering timeout in milliseconds. • Maximum number of requests stored in queue. • Packet reordering drop policy. • SBI Service Translation enable/disable.

5. Select **Save**.
   The Diameter Settings reflect the updates.

GCB for Service Mesh and HTTPS/2 Support with Metadata

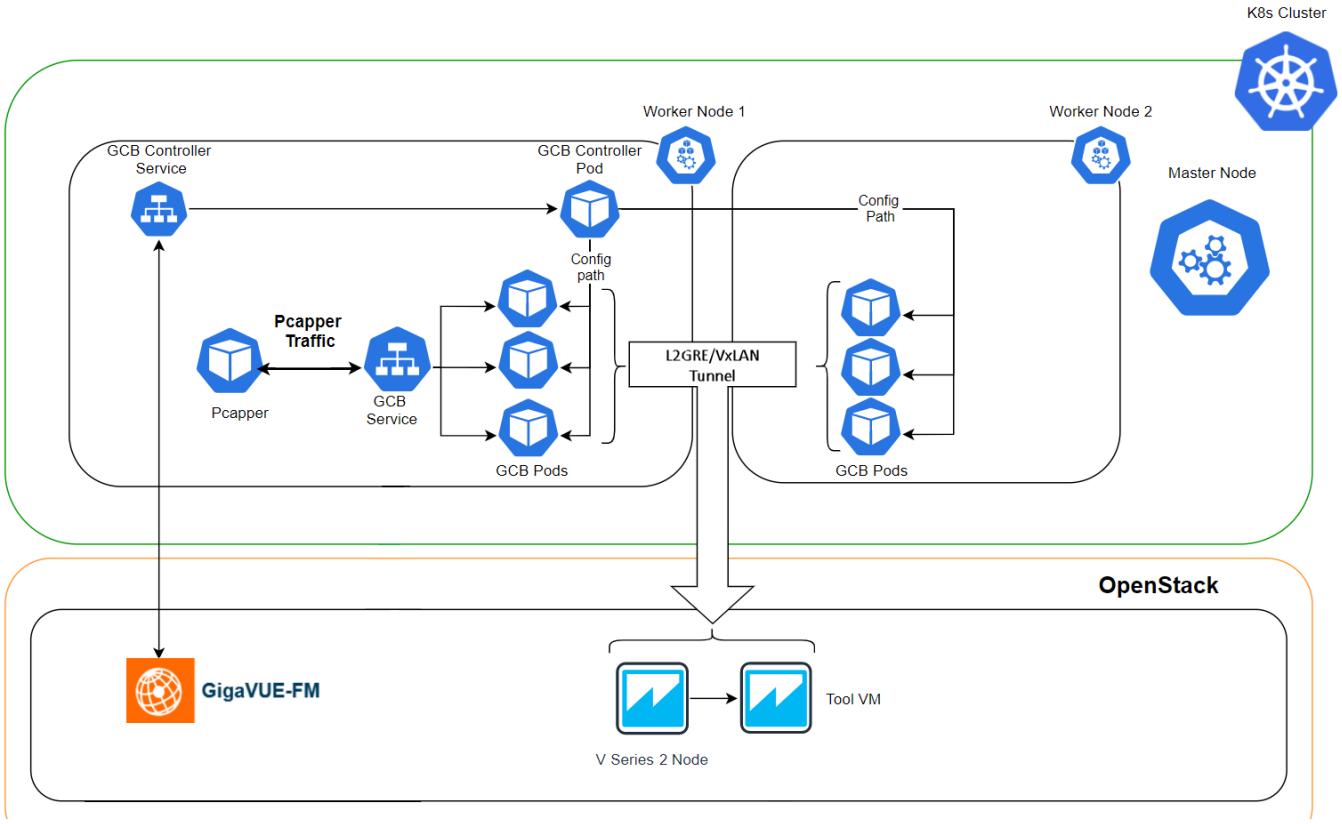
In this section, you learn about:

- The overview of Gigamon Containerized Broker for service mesh and HTTPS/2 support with metadata
- The steps to install and deploy GCB components.

For details, refer to the following topics:

Architecture of GCB for Service Mesh and HTTPS/2 Support with Metadata

The following diagram illustrates the architecture of Gigamon Containerized Broker for service mesh and HTTPS/2 support with metadata environment:



1. The GCB Controller is registered with GigaVUE-FM and the traffic policy is deployed on the GCBs.
2. Communication of configuration, data, and statistics to and from GCB is performed through the GCB Controller Service. GigaVUE-FM communicates with the GCB Pods through the GCB Controller.
3. Each GCB Pod is registered with GigaVUE-FM and the traffic policy is deployed on the GCBs.
4. The Pcapper collects the network traffic and sends the HTTP packets to GCB Controller.
5. In the GCB service, the received HTTP packets are load balanced across the available GCB Pods.
6. GCB Pods filters the packets based on the metadata.
7. The filtered HTTP packets from GCB Pods are tunneled directly to the Tools or through the GigaVUE V Series nodes on OpenStack environment. For details, refer to the *GigaVUE Cloud Suite for OpenStack Configuration Guide*.
8. GCB Controller collects the data from GCB Pods and sends the collected statistics and heartbeats to GigaVUE-FM.

Get Started with GCB for Service Mesh and HTTPS/2 Support with Metadata

In this section, you learn how to initiate GCB and GigaVUE-FM deployment with the required licenses and network requisites.

For details, refer to the following sections,

- Components of GCB for Service Mesh and HTTPS/2 Support with Metadata
- License Information
- Network requirements

Components of GCB for Service Mesh and HTTPS/2 Support with Metadata

The Gigamon Containerized Broker for service mesh and HTTPS/2 support with metadata works with the following components:

- **GigaVUE-FM fabric manager:** Refers toa 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 GCB.
- **GCB Pod:** Refers to the primary GCB module that
  - Receives the data from Pcapper
  - Filters the traffic.
  - Tunnels the filtered traffic directly to the tools or through the V Series nodes

  GCB Pod also sends the statistics and heartbeats to GCB Controller.
- **GCB Controller:**Refers to the management component of GCBto control and communicate with GCB Pods. GCB Controller:
  - Collects the heartbeats and stats from GCB Pods
  - Sends the collected statistics and heartbeats to GigaVUE-FM.

License Information

All GCB Pods in your environment regularly send traffic statistics to the GCB Controller. The controller then sends a summary of these statistics to GigaVUE-FM for Volume-Based Licensing.

In a Volume-Based Licensing model, your license allows specific applications to process a set amount of data during the license term. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose.

GigaVUE-FM tracks the total data volume that GCBprocesses. If usage exceeds the licensed limit, GigaVUE-FM detects and reports the overuse.

Network Firewall Requirements

The following table describes the Kubernetes network requirements for GCB to work efficiently.

Direction	Type	Protocol	Port	CIDR	Purpose
Gigamon Containerized Broker deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM.
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with GCB Controller.
Outbound	HTTPS	TCP	42042	Any IP address	Allows GCB to communicate with GigaVUE-FM to send statistics data.

Configure GCB for Service Mesh and HTTPS/2 Support with Metadata

Setting up GCB for Service Mesh and HTTPS/2 Support with Metadata involves the following two steps:

- Deploy GCB in Kubernetes
- Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through GigaVUE-FM

The Red Hat supported base images of the GCB applications are built on the top of Red Hat Universal Base Image or Red Hat Enterprise Linux Image. The GCB images are **Red Hat Certified** for Red Hat OpenShift platform.

Deploy GCB in Kubernetes

NOTE: GigaVUE-FM supports managing both the latest and the old versions of GCBs at the same time.

To fully deploy GCB,

1. Enable external access to the Kubernetes environment

   Set up ingress, external public IPs, and load balancers) to allow communication between GCB and GigaVUE-FM.

2. Verify firewall rules on all Kubernetes nodes

   Ensure they meet the requirements described in the Network Requirements.

3. Make GCB images available

   Add the GCB images to a private Docker registry or allows access to pull the files from the Docker Hub registry. You can scale up or down the GCB instances based on your traffic load.

4. Deploy the GCB Controller Service and Pods

   You can use either Deploy GCB Controller Service and Pods using YAML files or Deploy GCB Controller Service and Pods using Helm Chart.

5. Deploy GCB HTTP Service and Pods

   You can use either Deploy GCB HTTP Service and Pods using YAML files or Deploy GCB HTTP Service and Pods.

Refer to the following topics for GCB Controller and HTTP services and Pods:

- Deploy GCB Controller Service
- Deploy GCB HTTP Service and Pods

> **NOTE:** To upgrade the GCB solution, follow the above-mentioned procedure to deploy the latest version of GCB Controller and then deploy the latest version of GCB HTTP.

Deploy GCB Controller Service and Pods

You can deploy the GCB Controller Service and Pods using the YAML files or the Helm Charts. For details, refer to the following sections:

- Deploy GCB Controller Service and Pods using YAML files
- Deploy GCB Controller Service and Pods using Helm Chart

Deploy GCB Controller Service and Pods using YAML files

Deploy GCB Controller Service

Follow the instructions below to deploy GCB Controller Service in your Kubernetes environment using the YAML file.

NOTE: For the GCB images and YAML files, Contact Sales

1. In your Kubernetes orchestrator, edit the GCB Controller image name, commands, and other required information into your YAML file.
   Sample data from the YAML file: Edit your YAML file based on the sample given below. Do not copy and paste this content into your YAML file:

```
apiVersion: v1
kind: Service
metadata:
  name: gigamon-gcb-cntlr-service
  labels:
    app: gcb-cntlr
    service: gigamon-gcb-cntlr-service
    # change the namespace to match your namespace
  namespace: default
spec:
  ports:
  - port: 8443
    protocol: TCP
    name: gcb-rest
    targetPort: 8443
  - port: 42042
    protocol: TCP
    name: gcb-stats
    targetPort: 42042
  selector:
    app: gcb-cntlr
```

   The following table gives a description of all the field values in the YAML file that you update:

Field Values	Description
Port: 8443	The GCB Controller REST service port number.
Port: 42042	This port must be port 42042. This allows GigaVUE-FM to communicate with GCB to send statistical data.

2. Using the YAML file, Kubernetes creates the GCB Controller Service.

Deploy GCB Controller Pods

Follow these instructions to deploy GCB Controller Service in your Kubernetes environment using YAML file:

> **NOTE:** Contact Technical Support or Contact Sales for the GCB images and YAML files.

1. In your Kubernetes orchestrator, edit the GCB Controller image name, commands, and other required information into your YAML file.
   Sample data from the YAML file. Edit your YAML file based on the sample given below. Do not copy and paste this content into your YAML file:

```
name: gcb-cntlr
image: gigamon/gcb-cntlr:cntlr-<version>
command:
- # /gcb-cntlr
- # <FM IP>
- # <FM REST Svc Port>
- # <GCB-Cntlr REST SVC Port>
- # <mTLS Mode: 1(ON)|0(OFF))
- # <Cert Path>
- # <Cert file>
- # <Pvt Key>
- # <CA-Root>
imagePullPolicy: Always
ports:
- containerPort: 8443
- containerPort: 42042
env:
# Service name.Should match name specified in metadata section.
- name: GCB_CNTLR_SERVICE_NAME
 value: "GIGAMON_GCB_CNTLR_SERVICE"
# External LB balancer IP, for controller (FM) to connect to gcb-cntlr
- name: GCB_CNTLR_EXT_IP_DNS
 value: "<external IP for GigaVUE-FM to reach GCB CNTLR>"
# K8S cluster end-point
- name: K8S_CLUSTER_ENDPOINT
 value: "https://<kubernetesapiserverurl>:6443"
# Namespace of pod
- name: GCB_CNTLR_POD_NAMESPACE
 valueFrom:
      fieldRef:
          fieldPath: metadata.namespace
```

Field values in the YAML file that are changed or updated:

Field Values	Description
/gcb-cntlr (image name)	GCB Controller image name and version. Make sure to use the latest image version.
GigaVUE-FM IP	The IP address of GigaVUE-FM with which your GCB is connected.
FM REST Svc Port	The GigaVUE-FM REST service port number. Opened the port on your Kubernetes to allow outbound traffic. This allows GCB Controller to communicate with GigaVUE-FM. Example: 443
GCB-Cntlr REST SVC Port	The GCB Controller REST service port number. Ope this port on your GigaVUE-FM to allow inbound traffic to Kubernetes. This allows GigaVUE-FM to communicate with GCB Controller. Example: 8443

Field Values	Description
mTLS Mode: 1(ON) | 0(OFF)	To specify if mTLS mode between GigaVUE-FM and GCB controller should be On or Off. Values are: • 1 - ON • 0 - OFF
Cert Path	Path of the certificate file. Example: /etc/gcbcerts
Cert file	Name of the certificate file. Example: gcb-cert.pem
Pvt Key	Name of the private key. Example: gcb-pvt-key.pem
CA-Root	Name of the CA root certificate. Example: gcb-ca-root-cert.pem
Ports: • containerPort: 8443 • containerPort: 42042	You must open both the ports. • Ensure that the first container port is the same as GCB-Cntlr REST SVC Port. • Ensure that the second container port is port 42042. This allows GigaVUE-FM to communicate with GCB to send statistics data.
External LB balancer IP	The external load balancer IP/DNS value to allow GigaVUE-FM to communication with GCB Controller within Kubernetes. The GigaVUE-FM IP entry may change when you upgrade or redeploy.
K8S cluster end-point	Kubernetes cluster end point for GigaVUE-FM to access the control plane. Example: https://<kubernetesapiserverurl>:6443

NOTE: Volume Mount is optional for the cases when there is no mTLS authentication. You should enter your volume mount path and a name for the volume mount. For detailed information, refer to the respective YAML files.

2. Using the YAML file, Kubernetes automatically downloads the defined GCB Controller Pods and deploys it to the Kubernetes worker node.

Deploy GCB Controller Service and Pods using Helm Chart

Follow these instructions to deploy GCB Controller Service and Pods in your Kubernetes environment using Helm Chart:

> **NOTE:** Contact Technical Support or Contact Sales for the GCB images and Helm Charts (**gcb-cntlr-<version>.tgz** and **gcb-http-<version>.tgz**).

1. On your Kubernetes orchestrator, extract the received GCB Controller (service and Pod) **.tgz** package.
   ```
   $ tar -xvf gcb-cntlr-<version>.tgz
   ```
2. Navigate to the gcb-cntlr folder and edit the **values.yaml** file as per your environment. For details, refer to Deploy GCB Controller Service and Deploy GCB Controller Pods.
3. From the extracted gcb-cntlr folder, install the GCB Controller Helm Chart using the following command:
   ```
   $ helm install <Name for the GCB Controller> <Extracted folder path>
   ```

   Example: $ helm install gcb-cntlr gcb-cntlr/

   Using the Helm file, Kubernetes creates the GCB Controller Service, automatically downloads the defined GCB Controller Pods and deploys it to the Kubernetes worker node.

Deploy GCB HTTP Service and Pods

You can deploy the GCB HTTP Service and Pods using the YAML files or the Helm Charts. Refer to the following sections for detailed information.

- Deploy GCB HTTP Service and Pods using YAML files
- Deploy GCB HTTP Service and Pods

Deploy GCB HTTP Service and Pods using YAML files

Deploy GCB HTTP Service

Follow the below instructions to deploy GCB HTTP service in your Kubernetes environment using YAML file:

> **NOTE:** Contact Contact Technical Support or Contact Sales for the GCB images and YAML files.

1. In your Kubernetes orchestrator, edit the GCB Controller image name, commands, and other required information into your YAML file. The following is sample data from the your YAML file. Edit your YAML file based on the sample given below. Do not copy and paste this content in your YAML file:

```
apiVersion: v1
kind: Service
metadata:
  name: gcb-http-service
  labels:
    app: gcb-http
    service: gcb-http-service
  # change the namespace to match your namespace
  namespace: default
spec:
  ports:
  - port: 9443
    name: https
  selector:
    app: gcb-http
```

   The following table gives a description of all the field values in the YAML file that is updated:

Field Value	Description
9443	The GCB Controller REST service port number. This must be opened on your GigaVUE-FM to allow inbound traffic to Kubernetes.

2. Using the YAML file, Kubernetes creates the defined GCB HTTP service.

Deploy GCB HTTP Pods

Follow the instructions below to deployGCBHTTP Pods in your Kubernetes environment using YAML file:

NOTE: Contact Contact Technical Support or Contact Sales for the GCB images and YAML files.

1. In your Kubernetes orchestrator, edit the GCBHTTP Pod image name, commands, and other required information in a YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below.Do notcopy and paste this content into your YAML file:

```
name: gcb-http
command:
- # /gcb-http
- # PORT for RX
- # mTLS-Flag(T/F)
- # CERT_FILE
- # KEY_FILE
- # CA_CERT_FILE
- # CA_VERIFY(T/F)
- # default destination ip (if not configured from GigaVUE-FM)
- # (1=> default, 0=> rule)
- # (1=> L2GRE, 3=> VXLAN)
image: gigamon/gcb-http:<version>
imagePullPolicy: Always
env:
- name: GCB_DEBUG_MODE
  value: "0x031A2F14"
- name: GCB_REORDER_GROUP # This is a mandatory field
  value: "group_6_0_00"  # Group name must be unique
- name: GCB_SERVICE_NAME
  value: "GIGAMON_GCB_HTTP2_SERVICE"
- name: GCB_CNTLR_SVC_DNS
  #value: "<GCB-CNTLR-SVC-NAME.GCB-CNTLR-NAMESPACE>.svc.cluster.local"
  value: "gigamon-gcb-cntlr-service.default.svc.cluster.local"
- name: GCB_CNTLR_REST_SVC_PORT
# port used to receive configuration from GigaVUE-FM
  value: '8443'
- name: GCB_POD_NAMESPACE
valueFrom:
fieldRef:
fieldPath: metadata.namespace
```

The following table gives a description of all the field values in the YAML file that are changed or updated:

Field Value	Description
PORT for RX	HTTP port number for ingress traffic Example: 9443
mTLS-Flag (True/False)	Enable or disable mTLS between Pcapper and GCB.
CERT_FILE	SSL/TLS certificates Example: server-certificate-chain.pem
KEY_FILE	Private key for the certificate Example: server-private-key.pem
CA_CERT_FILE	CA root certificate

Field Value	Description
	Example: ca-root-crt-chain.crt
CA_VERIFY (True/False)	Enable or disable verification of the certificate files.
default destination ip	Default Destination IP (if not being configured from GigaVUE-FM)
(1=> default, 0=> rule)	(0/1) Enter 1 to use the default destination IP, or enter 0 to use the rules configured by GigaVUE-FM
(1=> L2GRE, 3=> VXLAN)	(1/3) Enter 1 to use the L2GRE tunnel type, or enter 3 to use the VXLAN tunnel type.
gigamon/gcb-http:<version>	GCB Controller image name and version. Make sure to use the latest image version.

GCB_DEBUG_MODE	The hex value for GCB debugging. This value must be in the **0xdd [aaaa][b][c]** format, where:
	• aaaa is a hex value for the number of pcap messages to maintain before rollover
	• b is 0 = do not create pcap or 1 = create pcap
	• c is level. Level with 1 =fatal, 2 =error, 3 =info, 4 =debug
	• dd is the log file size multiplier
	  • dd = 0|1 - means default log file size (approx. 100,000 lines)
	  • dd = 08 - means 8 * default log file size (approx. 8*100,0000 lines)
	  • dd = FF = 255 - means (255*100,000 lines)

GCB_CNTLR_SVC_DNS	GCB Controller Service Number. This value must match the metadata used for GCB Controller. Example: gigamon-gcb-cntlr-service.default.svc.cluster.local
GCB_CNTLR_REST_SVC_PORT	The GCB Controller REST service port number. This must be opened on your GigaVUE-FM to allow inbound traffic to Kubernetes.

2. Using the YAML file, Kubernetes automatically downloads and deploys the defined GCB HTTP Pods.

Deploy GCB HTTP Service and Pods using Helm Chart

Follow the instructions below to deploy GCB HTTP Service and Pods in your Kubernetes environment using Helm Chart:

NOTE: Contact Technical Support or Contact Sales for the GCB images and Helm Charts (**gcb-cntlr-<version>.tgz** and **gcb-http-<version>.tgz**).

1. On your Kubernetes orchestrator, extract the received GCB HTTP (service and Pod) **.tgz** package.
   ```
   $ tar -xvf gcb-http-<version>.tgz
   ```
2. After extraction, navigate to the gcb-http folder and edit the **values.yaml** file as per your environment. Refer to Deploy GCB HTTP Service and Deploy GCB HTTP Pods for detailed information.
3. From the extracted gcb-http folder, install the GCB HTTP Helm Chart using the following command:
   ```
   $ helm install <Name for the GCB HTTP> <Extracted folder path>
   ```
   Example: **$ helm install gcb-http gcb-http/**
4. Using the Helm file, Kubernetes creates the GCB HTTP Service, automatically downloads the defined GCB HTTP Pods and deploys it to the Kubernetes worker node.

Configure GCB for Service Mesh and HTTPS/2 Support with Metadata through GigaVUE-FM

In this topic, you learn how to configure GCBthrough GigaVUE-FM GUI.

For details, refer to the following section:

- Launch GigaVUE-FM
- Create Metadata Field Names
- Create Monitoring Domain
- Configure Service Identification
- Configure Traffic Policy

Launch GigaVUE-FM

To deploy,

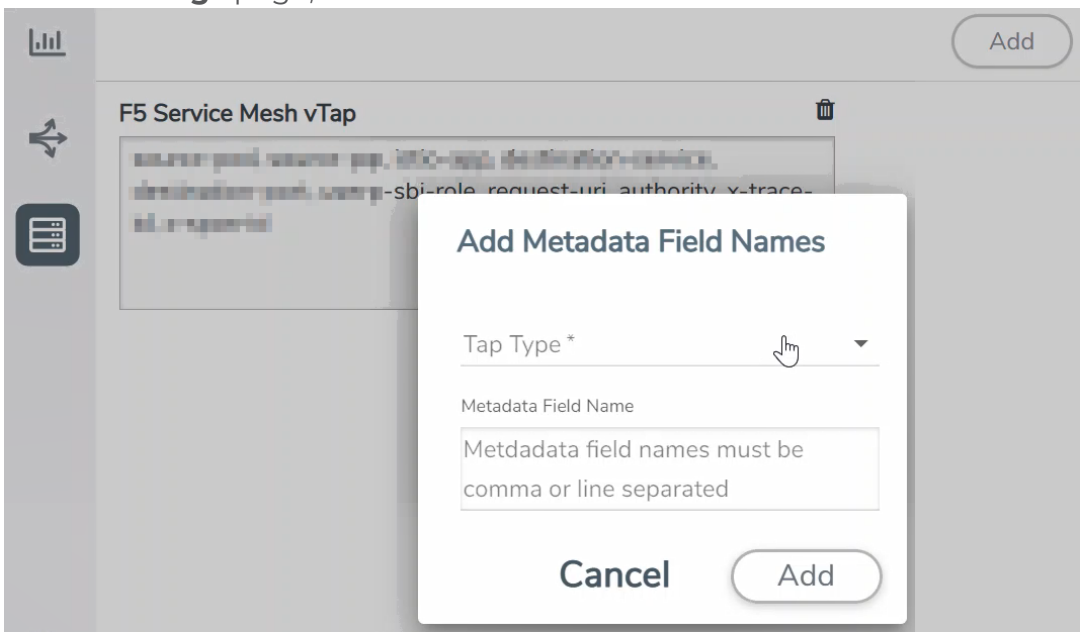
1. Download the latest GigaVUE-FM image files from Gigamon Customer Portal.
2. Upload and launch GigaVUE-FM on your OpenStack environment.

   For assistance,Contact Technical Support of Gigamon or refer to the *GigaVUE Cloud Suite Deployment Guide - OpenStack* for more information on GigaVUE V Series configuration on OpenStack environment.

Create Metadata Field Names

To create metadata field names in GigaVUE-FM.

1. In GigaVUE-FM, on the left navigation pane, select **Inventory > CONTAINER > Gigamon Containerized Broker > Settings**. The **Settings** page appears.
2. In the **Settings** page, select **Add**. The **Add Metadata Field Names** wizard appears.



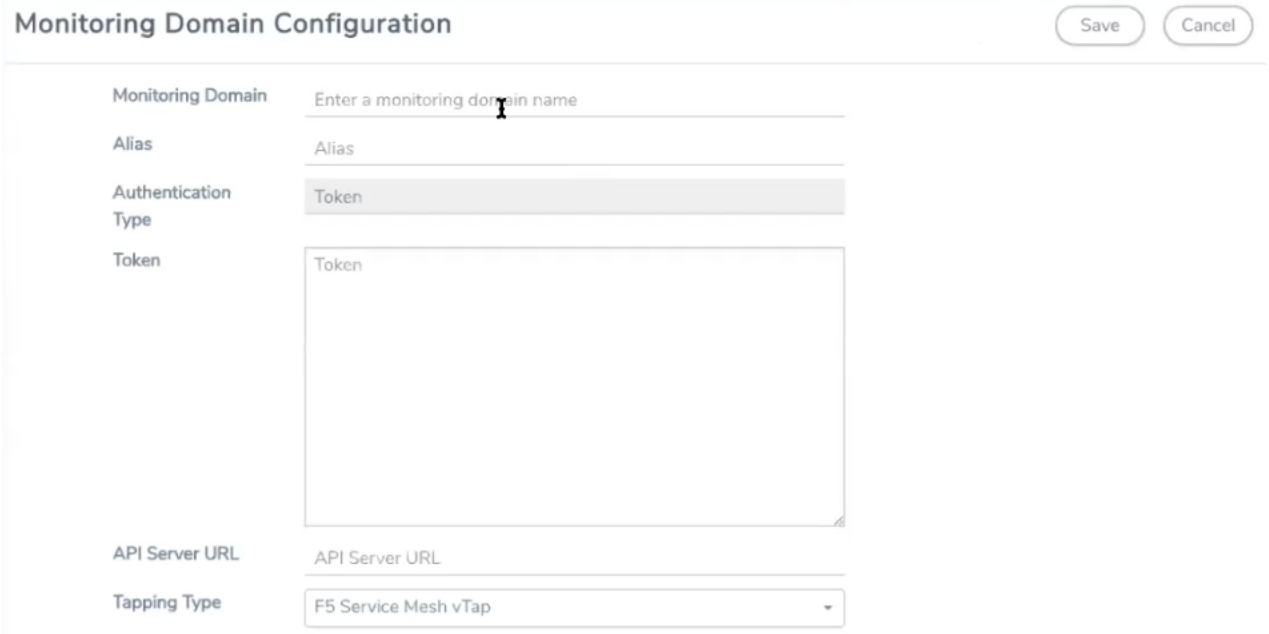
3. Select the **Tap type** as **F5 Service Mesh vTAP** and enter the **Metadata Field Names**.
4. Select **Add**. The newly added metadata field names appear on the **Settings** page.

Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM,

1. In GigaVUE-FM, on the left navigation pane, select **Inventory > CONTAINER > Gigamon Containerized Broker > Monitoring Domain**. The **Monitoring Domain** page appears.

2. On the Monitoring Domain page, select **New**. The Monitoring Domain Configuration wizard appears.



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

Fields	Description
Monitoring Domain	Enter a name for the monitoring domain
Alias	Enter a name for the GCB connection
Authentication Type	Select Token as the authentication type
API Server URL	Enter the URL of the API server
Tapping Type	Select **F5 Service Mesh vTap** as the Tapping Type

4. Select **Save** to create a monitoring domain.

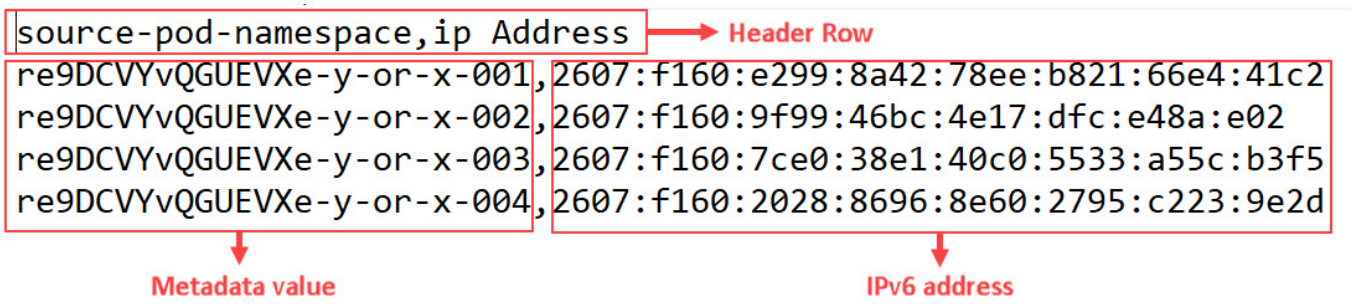
Configure Service Identification

In the Service mesh and HTTP/s supported platform, the GCB receives packets to be monitored in the form of HTTPS/2 requests. On receiving the HTTPS/2 request from Pcapper, GCB applies the rules configured in GigaVUE-FM and forwards the filtered traffic to GigaVUE V Series Nodes deployed on the OpenStack platform through L2GRE or VXLAN tunnels.

In a Kubernetes environment, the IP addresses associated with pods and services are temporary and can change regularly. For the external tools, these changing IP addresses are difficult to consistently correlate incoming data to the services and the sources related to

that data. The same IP addresses may also exist in multiple Kubernetes clusters adding difficulty in identifying the true source of the monitored traffic. To correlate these temporary and same IP addresses, the GigaVUE-FM and GCB use information supplied in the .csv text files to map the temporary IP addresses to IPv6 addresses that the external tools can consistently use.

The CSV file must contain a header row with two columns. The first column is for the Metadata value and the second column is for the IPv6 address. The metadata value specified in the header row and the values in the first column of the CSV file must match theMetadata Field Names.



NOTE: The length of the metadata value in first column of the non-header row must be less than or equal to 255 and the number of non-header entries (rows) must be less than **4096**. Service ID feature will not work if metadata fields for Service ID mapping are greater than 255 bytes.

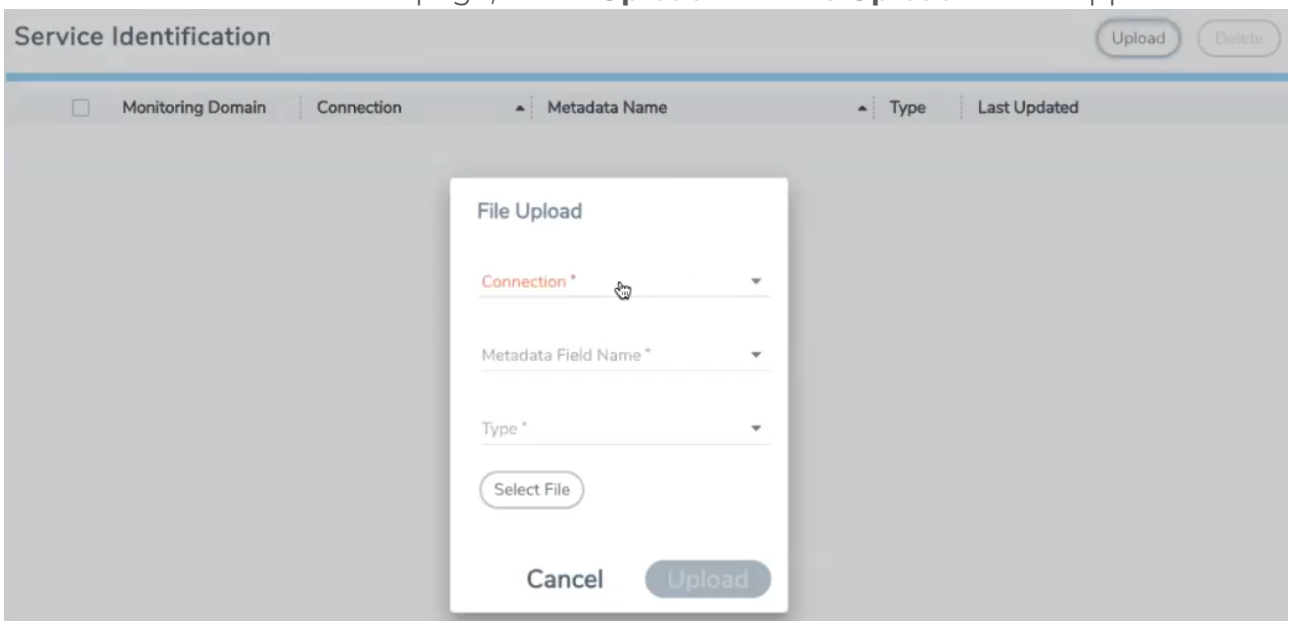
The Service Mesh and HTTPS/2 supported platform must provide the following CSV files:

- a **src-ip-mapping.csv** file to translate the temporary source IP (IPv4) address to an external IPv6 address.
- a **dest-ip-mapping.csv** file to translate the temporary destination IP (IPv4) address to an external IPv6 address.

To upload the mapping CSV files to GigaVUE-FM,

1. After creating a Monitoring Domain, in GigaVUE-FM, from the left navigation pane, select **Inventory > CONTAINER > Gigamon Containerized Broker > Service Identification**. The **Service Identification** page appears.

2. In the Service Identification page, select **Upload**. The **File Upload** wizard appears.



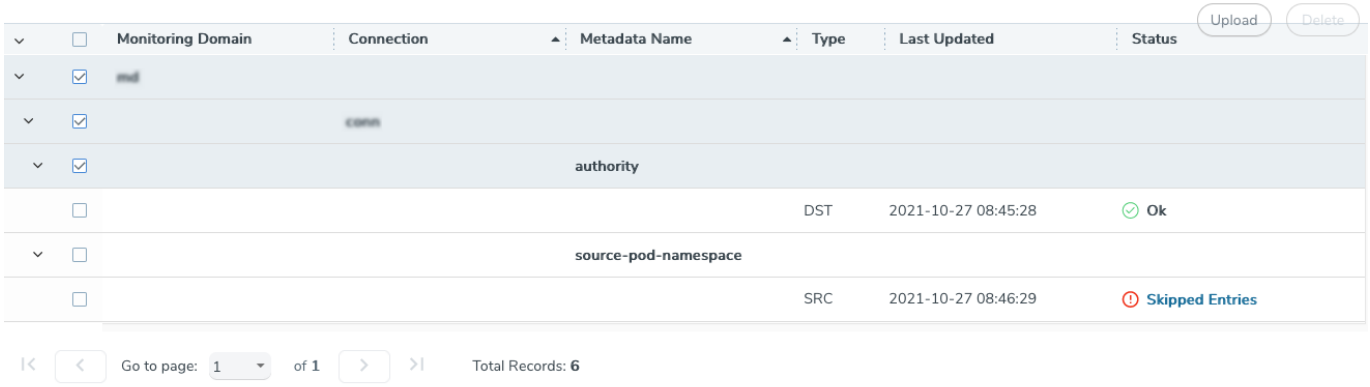
3. Enter or select the required information as described in the following table:

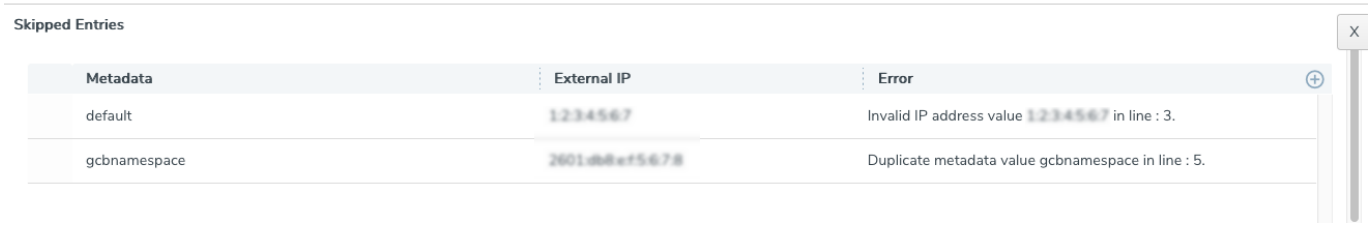
Fields	Description
Connection	Select an existing monitoring domain
Metadata Field Name	Select a Metadata field to search in the CSV file. • If the value for the metadata field matches the content of the received packets, then GCB use the mapping tables to convert the ephemeral IPv4 addresses to external IPv6 addresses and replaces the incoming IPv4 header with an IPv6 header, before forwarding the packets to the Tools or V Series nodes. • If the value for the metadata field doesn't match the content of the received packets, then the GCB forwards the packets without translation.
Type	Select an IP address type from the following: • SRC - Source IP • DST - Destination IP
Select (CSV) File	Select an IP mapping CSV file to upload to GigaVUE-FM.

4. Select **Upload** to upload the selected CSV file for the monitoring domain.

NOTE: You must upload a source and a destination IP mapping CSV file for the IP translation.

Once the CSV file is uploaded successfully, GigaVUE-FM displays the status of the uploaded file. If no error is found in the meta-data, then the status is displayed as **Ok**. However, when an error happens, in the meta data or processing, then the error message is displayed under the **Status** column. Select the error message to get detailed information about the error.





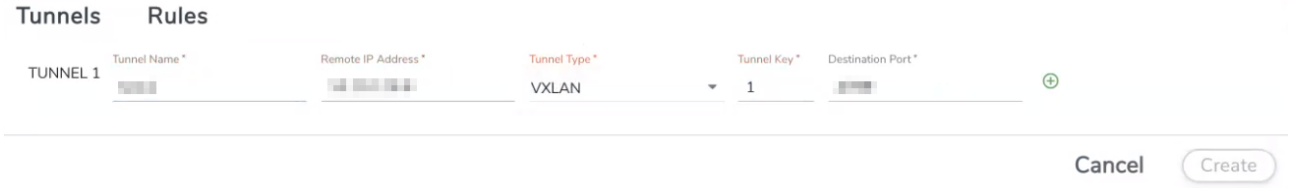
Types of Error messages:

1. **Skipped Entries**: This error message is displayed:
   - If the metadata value is blank or more than 127 characters.
   - If the IP address is invalid.
   - If there are more than 4096 entries in the file excluding the header. In this case, only the first 4096 entries will be sent to GCB and the rest would be skipped.
   - If the uploaded CSV file contains two or more identical entries, or two or more entries with the same meta data values. In this case only the first entry will be sent to GCB and the rest would be skipped.
2. **GCB**: This error message is displayed due to processing errors or a failure.

Configure Traffic Policy

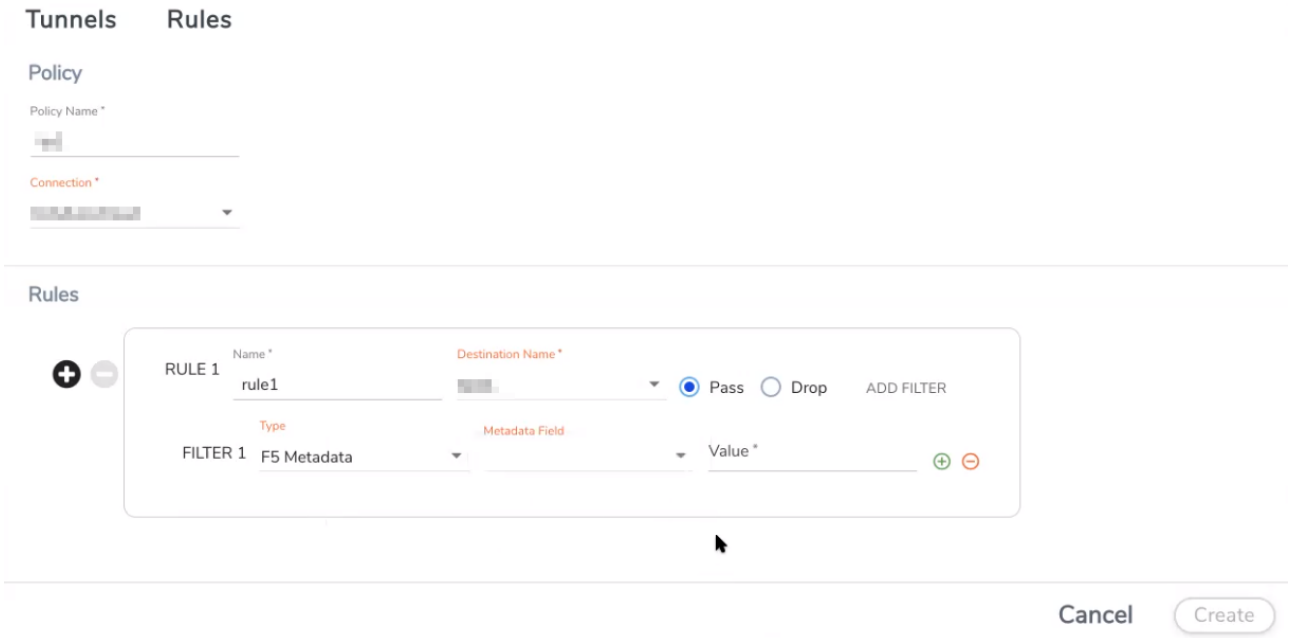
To create a Traffic Policy in GigaVUE-FM:

1. From the GigaVUE-FM left navigation pane, select **Traffic > CONTAINER > Gigamon Containerized Broker**. The **Traffic Policy** page appears.
2. In the **Traffic Policy** page, click **Create**. The Create Tunnels and Rules wizard appears.
3. In the **Tunnels** tab, enter or select the required information as described in the following table:



Fields	Description
Tunnel Name	Enter a name for the Tunnel.
Remote IP Address	Enter an IP Address for the Tunnel.
Tunnel Type	Select L2GRE or VXLAN as the tunnel type.
Tunnel Key	Enter a value for the tunnel key.
Destination Port	If the tunnel type is VXLAN, enter the tunnel destination port number.

4. Switch to **Rules** tab, and enter or select the required information as described in the following table:



Fields	Description
Policy	
Policy Name	Enter a name for the policy.
Connection	Select a connection for the policy.
Rules	
Name	Enter a name for the Rule.
Destination Name	Select a tunnel destination.
Pass/Drop	Select Pass to allow the packets or select Drop to block the packets based on the filters.
Click **ADD FILTER** to add filters for the rule.	
Type	Select the type as F5 Metadata.
Metadata Field	Select a Metadata field name.
Filter value	Enter a value for the filter type.

5. Click **Create** and this new Traffic Policy deploys itself in the GCB.

The Traffic Policy processes the Pcapper traffic and forwards the traffic to the tunnel destination IP address.

Configure GCB Settings

You can configure the following settings in GigaVUE-FM:

- GCB General Settings
- GCB Individual Settings
- GCB Group Settings

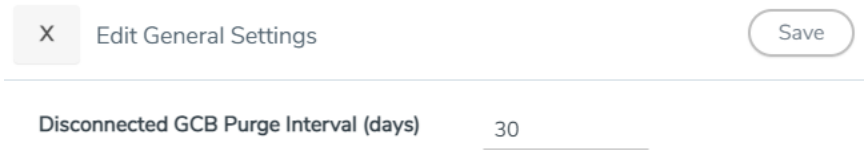
GCB General Settings

In the GCB General Settings, you can specify the purge interval to automatically remove the GCBs that are disconnected for a long duration.

> **NOTE:** GigaVUE-FM generates an alarm for the disconnected GCB when the GCB heartbeats are not received for more than 15 minutes. For details, refer to the "Alarms" topic in the *GigaVUE Administration Guide* .

To view or edit the GCB general settings,

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Gigamon Containerized Broker > Settings**. The **Settings** page appears.
2. From the **Settings** page, on the **General** section, select **Edit**. The **Edit General Settings** quick view appears.



3. Enter the number of days to retain the disconnected GCB. After this duration, the disconnected GCBis removed.
4. Select **Save**. The General Settings is updated.

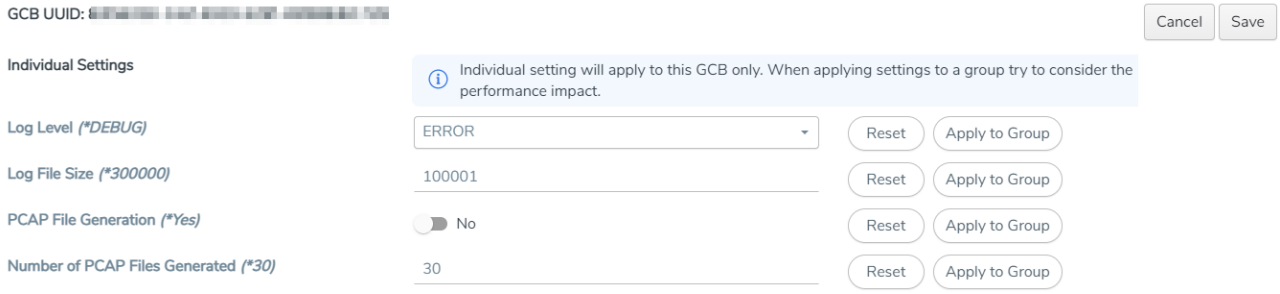
GCB Individual Settings

GCB Log Level Settings

In GigaVUE-FM, you can control the level of logs created at each individual GCBfor troubleshooting. The regular GCB log file name format is **gcb_http2.log**.

To view or edit the GCB log level settings,

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Gigamon Containerized Broker > Settings**. The **Settings** page appears.
2. From the **Settings** page, select a GCB to view or edit the GCB log configuration.
3. Select **Edit** to edit the required GCB log values in the **Individual Settings** section.



Field	Description
Log Level	Select one of the following: • DEBUG: fine-grained log information for application debugging • INFO: coarse-grained log information for highlighting application progress • WARN: Log information of potentially harmful situations • ERROR: Log information of the error events that allows the application to run continuously • FATAL: Log information of very severe error events that presumably lead the application to abort.
Log File Size	Enter a value for the number of lines in the GCB log file.
PCAP File Generation	Select **Yes** to generate the PCAP file and select **No** to continue without the PCAP file.
Number of PCAP Files Generated	Enter a value for the number of PCAP files to be generated and stored on the GCB.

On one of the above fields,

- Select **Reset** to reset the value to default.
- Select **Apply to Group** to apply the value to all the members of the group

GCB Transaction Logging Settings

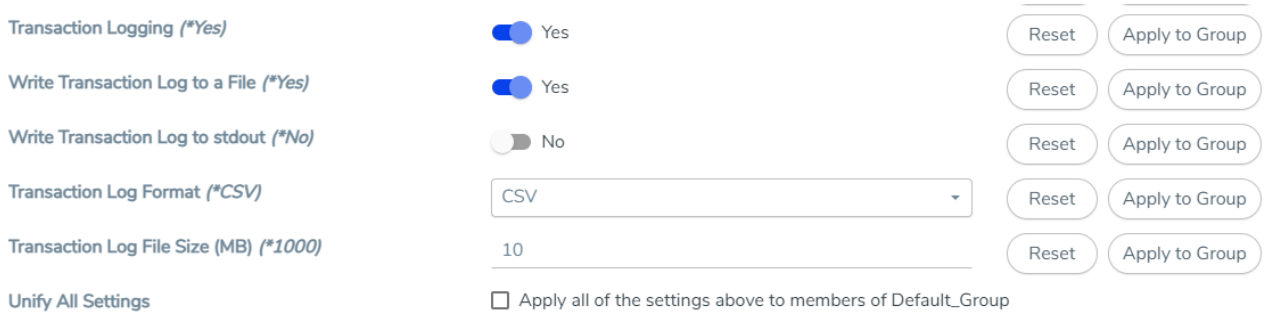
The GCB considers an HTTPS POST message from Pcapper to GCB as a transaction. The Transaction Logging feature collects data from the transaction to aid in troubleshooting problems such as dropped packets, or no traffic at tools. For each transaction, GCB creates a transaction record. The transaction record is logged to a transaction log file in the GCB pod or into the Kubernetes logging stdout stream.

The transaction log consists of various items like transaction index, transaction time, source, and destination details extracted from the data sources like GCB system time, Pcapper metadata field, and Pcapper transaction. Each pod can have a maximum of ten log files.

The GCB transaction log file name format is **gcb_trans_<YYYY-MM-DD_hh-mm-ss>.<csv | json>**, and the file is located on each GCB Pod in the **/pod-data** directory.

To view or edit the transaction log settings,

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Gigamon Containerized Broker > Settings**. The **Settings** page appears.
2. From the **Settings** page, select a GCB to view or edit the GCB transaction log settings.
3. Select **Edit** to edit the required GCB transaction log values in the **Individual Settings** section.



Field	Description
Transaction Logging	Select **Yes** to enable the transaction logs generation or select **No** to disable the transaction logs generation.
Write Transaction Log to a File	Select **Yes** to save the generated transaction logs to a file on your GCB HTTPS Pods or select **No** to continue without saving the logs to a file.
Write Transaction Log to stdout	Select **Yes** to save the generated transaction logs to your Kubernetes logging standard output stream or select **No** to continue without saving the logs to your Kubernetes stdout. Refer to Kubernetes Logging Architecture for detailed information on Kubernetes stdout.
Transaction Log Format	Select **CSV** or **JSON** as the transaction log file format.
Transaction Log File Size (MB)	Enter a value between 1 MB to 4095 MB for the transaction log file size. A new log file is created whenever the log file reaches the specified file size.
Unify All Settings	Enable the Unify All Settings option to apply all the log settings to the members of the group.

On one of the above fields,

- Select **Reset** to reset the value to default.
- Select **Apply to Group** to apply the value to all the members of the group

GCB Group Settings

GCB Group settings allow you to configure group settings such as packet reordering settings to multiple GCBs present in a group. It allows you to create a group consisting of multiple GCBs with the same settings. You can change one or more group settings for a GCB group, and the changes are applied to all the GCBs in the group. You can create many GCB groups. Make sure to provide different names to all the groups.

GCB Packet Reordering Settings

When the GCB receives HTTPS POST request from Pcapper, it extracts the headers, metadata, and packets from the message. After extraction, GCB applies the traffic policy and service identification and forwards packets to the destination.

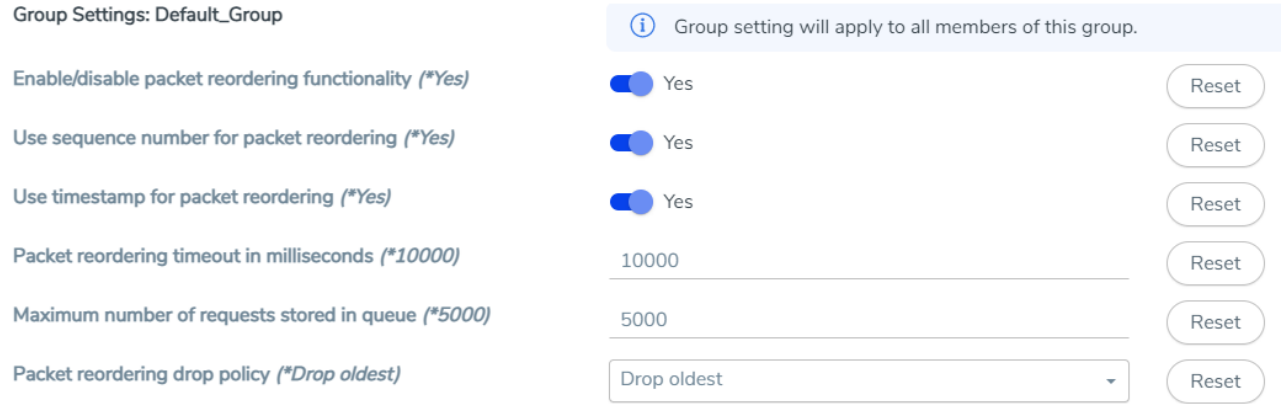
In some cases, a single request may not have the complete transaction, or the request may have packets that are out of order. The GCB packet reordering functionality fixes these out of order packets and makes a complete transaction for tool effectiveness. When the GCB receives a request from Pcapper, GCB checks for complete transaction using a combination of metadata fields and the flow of the extracted messages.

GCB stores the request in a queue with a time stamp and waits until the transaction is complete. When the queue reaches the maximum storage limit, then GCB drops the oldest or the most recent request based on the selected policy.

To view or edit the GCB packet reordering settings,

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Gigamon Containerized Broker > Settings**. The **Settings** page appears.
2. From the **Settings** page, select a GCB to view or edit the GCB packet reordering settings.

3. Select **Edit** to edit the required GCB packet reordering values in the **Group Settings** section.



Field	Description
Enable/disable packet reordering functionality	Select **Yes** to enable the packet reordering functionality or select **No** to disable the packet reordering functionality.
Use sequence number for packet reordering	Select **Yes** to use sequencing numbers for packet reordering or select **No** to reorder packets based on timestamps.
Use timestamp for packet reordering	Select **Yes** to use time stamps for packet reordering or select **No** to continue without using time stamps for the packet reordering.
Packet reordering timeout in milliseconds	Enter a value between 10000 to 3600000 milliseconds for the packet reordering timeout. Packet reordering timeout in the duration, the GCB waits for the pending packets to complete the transaction, and after this timeout, all the related packets are dropped.
Maximum number of requests stored in queue	Enter a value between 1000 to 100000 requests for the maximum number of requests that can be stored in the queue.
Packet reordering drop policy	Select **Drop most recent** to drop the most recent packets when the queue is overloaded or select **Drop oldest** to drop the old packets when the queue is overloaded.

GCB for Cloud Object Storage

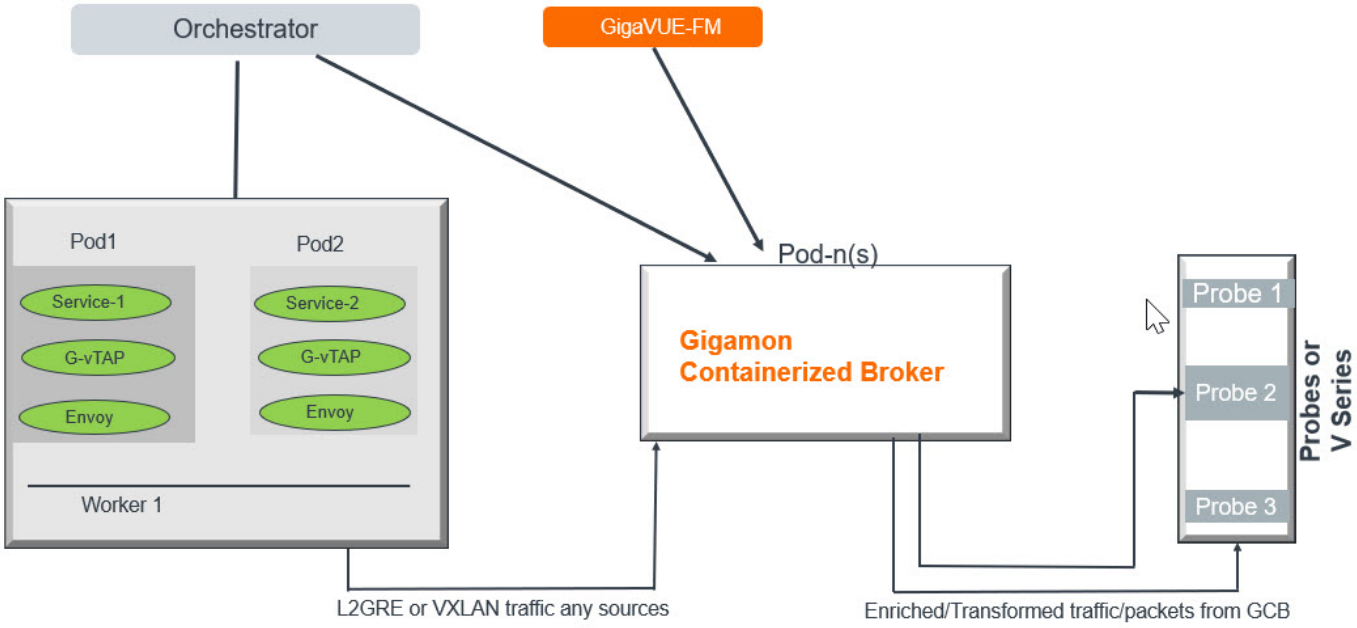
This chapter provides an overview of Gigamon Containerized Broker for cloud object storage and describes how to install and deploy UCT Containers in your Pods.

Topics:

Architecture of GCB for Cloud Object Storage

GCB with GigaVUE-FM deployment

With GCB in its own Pod, you can choose an orchestrator (other than GigaVUE-FM) like K8S to spin up/down the GCB pods.



During GCB initialization, the GCB Controller tries to connect with the GigaVUE-FM IP that you provided in the YAML file.

- GigaVUE-FM has a server certificate and GCB has a client certificate, so that GigaVUE-FM and GCB can identify the connection and traffic flow.
- GigaVUE-FM does not control the GCB spin up/down. The GCB parameter definition and deployment is performed through Kubernetes orchestrator and not by GigaVUE-FM.

Get Started with GCB for Cloud Object Storage

This section describes how to initiate GCB deployment with the required licenses and network requisites.

Refer to the following sections for details:

- Components of GCB for Cloud Object Storage
- License Information

- Network Requirements

Components of GCB for Cloud Object Storage

The Gigamon Containerized Broker for cloud object storage works with the following components:

- **GigaVUE-FM fabric manager** A web-based interface that provides centralized visibility, management, and orchestration of both physical and virtual traffic that flows through GCB.
- **UCT Container** A traffic acquisition component that receives mirrored traffic from network infrastructure. It uses overlays like VXLAN to send the traffic to Gigamon Containerized Broker.
- **GCB Controller** Manages the registration and deregistration of GCB with GigaVUE-FM. It also collects and sends traffic statistics from both the GCB and UCT Container to GigaVUE-FM.
- **GCB S3** Refers to the storage service component of GCB that collects the mirrored packets from GCB Controller, converts to PCAP file and uploads it into Amazon S3.

License Information

Points to Note:

- All theUCT Container instances connected to GCB periodically report the statistics to GCB.
- Then, the GCB periodically reports the collective statistics of UCT Containers and its own statistics to GigaVUE-FM for Volume-Based Licensing.
- GigaVUE-FM adds the required licensing tags into the OpenSearch.

In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon's accounting purpose.

GigaVUE-FM:

- Tracks the total amount of data that various licensed applications process.
- Provides visibility into the actual amount of data, each licensed application is using on each node.
- Tracks the overuse if any.

Network Requirements

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, Gigamon Containerized Broker, and UCT Containers in your project, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

We recommend to create a separate security group for each component using the rules and port numbers.

Direction	Type	Protocol	Port	CIDR	Purpose
Gigamon Containerized Broker deployed inside EKS worker node					
Inbound	HTTPS	TCP	443	Any IP address	Allows GCB Controller to communicate with GigaVUE-FM.

Configure GCB for Cloud Object Storage

This topic describes how to configure GCB in your environment.

For details, refer to the following:

- Launch GigaVUE-FM
- Launch Gigamon Containerized Broker
- Store Traffic Data in S3 Bucket

Launch GigaVUE-FM

You can download the latest GigaVUE-FM image files from Gigamon Customer Portal. After fetching the image, upload and launch GigaVUE-FM inside or outside your VPC. For assistance,Contact Technical Support of Gigamon.

Launch Gigamon Containerized Broker

Follow these instructions to deploy GCB in your node:

1. In your Kubernetes orchestrator, enter the GCB Controller and GCB S3 image name, commands and the required information in a YAML file.
   Sample data to enter into your YAML file:

```
image: gigamon/gcb-s3:<version>
- command:
- gcb-s3
- <pkt_filter_type(ip|tcp|udp)>
- <i_iface: eth0, eth1>
- <s3_bucket_name>(Ex: gcb_s3_bucket)
- <s3_region>(Ex: us-east-2>)
- <AWS Account-ID>
- <max_pkt_per_pcap>
- <idle_timeout (in sec)>
- <stats_active (0/1)>
- <gcm port>
- <stats_interval(in sec)>
- <filtering rule>
- <gcb vxlan port>

image: gigamon/gcb-cntlr:<version>
- command:
- /gcb-cntlr
- <GigaVUE-FM IP>
- <PORT ID for GCB controller to communicate with GigaVUE-FM>
```

2. Using the YAML file, Kubernetes automatically downloads the defined GCB Controller and GCB S3. Then, both are deployed in a new Pod.
3. Connect the deployed UCT Containers to the GCB installed in the same node.
4. Register GCB with the GigaVUE-FM launched inside or outside your VPC.

Once the GCB is registered with GigaVUE-FM, the GCB starts to collect the traffic from the UCT Containers and periodically sends the heartbeats and statistics to GigaVUE-FM. For more information on GCB and GigaVUE-FM interaction, refer to GCB and GigaVUE-FM Interaction

Store Traffic Data in S3 Bucket

By default, the traffic information from GCB is saved into Amazon S3 bucket. All the parameters of the S3 bucket are defined in the yaml files.

The following are the S3 bucket parameters defined in yaml file:

Parameter	Description
s3_bucket_name	Name of the Amazon S3 bucket
s3_region	AWS region (Example: us-east-2>)
AWS Account-ID	ID of AWS user account
max_pkt_per_pcap	Maximum packets required to create a PCAP file
idle_timeout (in sec)	Idle time limit to create PCAP file without waiting to collect the maximum packets defined.

Follow the instructions below to store the traffic data from GCB to your Amazon S3 bucket.

1. Save the traffic data from the GCB as a PCAP file with the Server-Side Encryption technology.
2. Transfer and save the encrypted PCAP files to your Amazon S3 bucket.

NOTE: Naming convention of the PCAP file and the folder in S3 bucket are as follows:

- PCAP file name: **<AWS Accout ID>_pod_<Pod IP>_YYYY_MM_DD_HH_mm_ss_<milliseconds>.pcap**
- S3 folder name: **[S3 bucket name]/account_id/MM-DD-YYYY/[file-name]/**

Configure GCB for Cloud Object Storage

This topic describes how to configure GCB in your environment.

For details, refer to the following:

- Launch GigaVUE-FM
- Launch Gigamon Containerized Broker
- Store Traffic Data in S3 Bucket

Launch GigaVUE-FM

You can download the latest GigaVUE-FM image files from Gigamon Customer Portal. After fetching the image, upload and launch GigaVUE-FM inside or outside your VPC. For assistance,Contact Technical Support of Gigamon.

Launch Gigamon Containerized Broker

Follow these instructions to deploy GCB in your node:

1. In your Kubernetes orchestrator, enter the GCB Controller and GCB S3 image name, commands and the required information in a YAML file.
   Sample data to enter into your YAML file:

```
image: gigamon/gcb-s3:<version>
- command:
- gcb-s3
- <pkt_filter_type(ip|tcp|udp)>
- <i_iface: eth0, eth1>
- <s3_bucket_name>(Ex: gcb_s3_bucket)
- <s3_region>(Ex: us-east-2>)
- <AWS Account-ID>
- <max_pkt_per_pcap>
- <idle_timeout (in sec)>
- <stats_active (0/1)>
- <gcm port>
- <stats_interval(in sec)>
- <filtering rule>
- <gcb vxlan port>

image: gigamon/gcb-cntlr:<version>
- command:
- /gcb-cntlr
- <GigaVUE-FM IP>
- <PORT ID for GCB controller to communicate with GigaVUE-FM>
```

2. Using the YAML file, Kubernetes automatically downloads the defined GCB Controller and GCB S3. Then, both are deployed in a new Pod.
3. Connect the deployed UCT Containers to the GCB installed in the same node.
4. Register GCB with the GigaVUE-FM launched inside or outside your VPC.

Once the GCB is registered with GigaVUE-FM, the GCB starts to collect the traffic from the UCT Containers and periodically sends the heartbeats and statistics to GigaVUE-FM. For more information on GCB and GigaVUE-FM interaction, refer to GCB and GigaVUE-FM Interaction

Store Traffic Data in S3 Bucket

By default, the traffic information from GCB is saved into Amazon S3 bucket. All the parameters of the S3 bucket are defined in the yaml files.

The following are the S3 bucket parameters defined in yaml file:

Parameter	Description
s3_bucket_name	Name of the Amazon S3 bucket
s3_region	AWS region (Example: us-east-2>)
AWS Account-ID	ID of AWS user account
max_pkt_per_pcap	Maximum packets required to create a PCAP file
idle_timeout (in sec)	Idle time limit to create PCAP file without waiting to collect the maximum packets defined.

Follow the instructions below to store the traffic data from GCB to your Amazon S3 bucket.

1. Save the traffic data from the GCB as a PCAP file with the Server-Side Encryption technology.
2. Transfer and save the encrypted PCAP files to your Amazon S3 bucket.

NOTE: Naming convention of the PCAP file and the folder in S3 bucket are as follows:

- PCAP file name: **<AWS Accout ID>_pod_<Pod IP>_YYYY_MM_DD_HH_mm_ss_<milliseconds>.pcap**
- S3 folder name: **[S3 bucket name]/account_id/MM-DD-YYYY/[file-name]/**

View GCB statistics in GigaVUE-FM

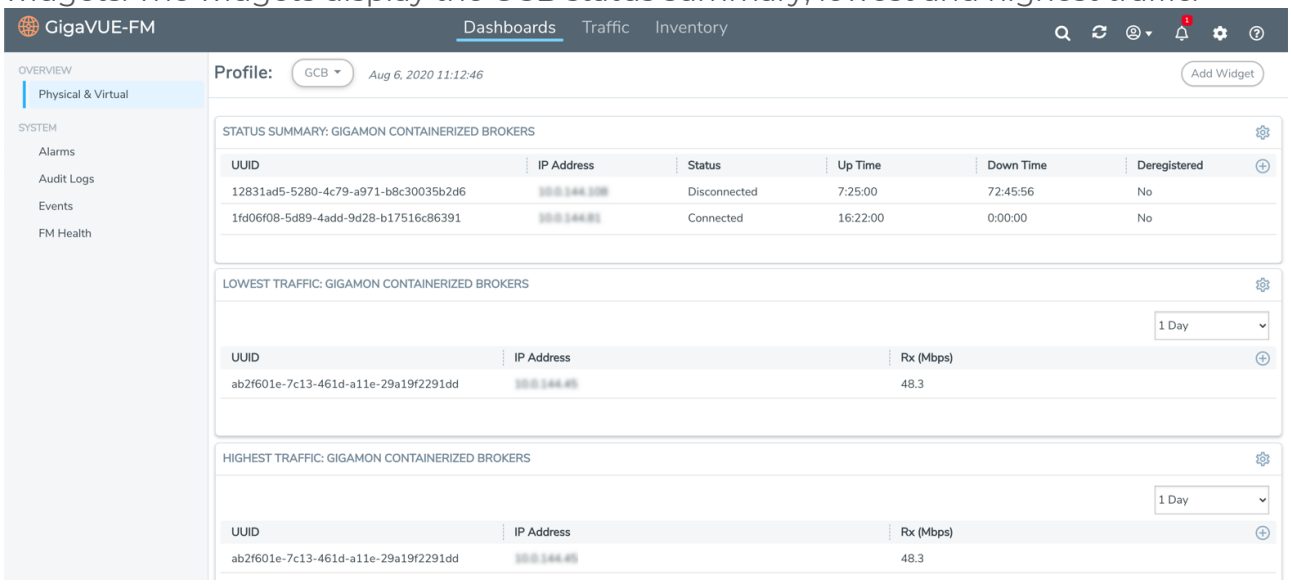
You can view the traffic information of GCB in GigaVUE-FM as the collective traffic from UCT Containers and GCB are periodically transferred to GigaVUE-FM.

GigaVUE-FM dashboard displays the GCB statistics in the following widgets:

- Status Summary
- Lowest Traffic
- Highest Traffic

To view the GCB statistics in GigaVUE-FM,

1. On the top navigation bar, select **Dashboard**.
2. In the left navigation pane of the Dashboard, select **Physical & Virtual**.
3. Select **Add Widget** and select Status Summary, Lowest Traffic, and Highest Traffic widgets. The widgets display the GCB status summary, lowest and highest traffic.



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 6.12 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rackmount, 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-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 6.12 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E 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 Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE 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

GigaVUE Cloud Suite 6.12 Hardware and Software Guides
Universal Cloud TAP - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **Note**: Release Notes are not included in the online documentation. **Note**: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

Documentation Feedback

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

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

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

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

Contact Technical Support

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

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

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to 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 Community site to:

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

The VÜECommunity 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)