Gigamon®

GigaVUE V Series Applications 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

GigaVUE V Series Application Guide

This guide describes the list of supported V Series Applications and how to add the V Series Applications to monitoring session and configure it.

Overview of GigaVUE V Series Applications

GigaVUE V Series Node is a virtual machine running in the customer's infrastructure which processes and distributes network traffic. It plays the same role as an HC Series appliance in a physical deployment, running many of the same GigaSMART applications and feeding data to tools in a similar manner. Because GigaVUE V Series nodes reside in a virtual environment, inbound and outbound traffic is tunneled (because there are no physical device ports).

GigaVUE V Series Applications run on GigaVUE V Series Nodes. All these applications use Volume- Based License. Refer to Volume-Based License for more detailed information.

You can use these applications to optimize the traffic sent from your instances to the monitoring tools. GigaVUE Cloud Suite supports the following applications:

- Application Intelligence
- De-duplication
- GENEVE Decapsulation
- Header Stripping
- Load Balancing
- Masking
- SSL Decrypt
- PCAPng Application
- 5G-Service Based Interface Application
- 5G-Cloud Application
- Slicing

Refer to the Supported V Series Applications table for more information on the platforms in which these applications will be supported.

Supported V Series Applications

The following table summarizes GigaSMART feature support across GigaVUE Cloud Suite platforms, covering packet operations, tunnel handling, application intelligence, and 5G capabilities.

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Masking	✓	✓	✓	✓	✓	✓	✓
Slicing	✓	✓	✓	✓	✓	✓	✓
De-duplication	✓	✓	✓	✓	✓	✓	✓
Application Metadata Exporter	✓	✓	✓	✓	✓ (Only when deploying GigaVUE V Series Node using Third party Orchestration)	✓	✓
L2GRE Tunnel Encapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite	✓	✗	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Deployment Guide.							
VXLAN Tunnel Encapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Decapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓	✓
VXLAN Tunnel Decapsulati	✓	✓	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
on Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.							
ERSPAN Tunnel Decapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓	✓
UDPGRE Tunnel Decapsulation Refer to *Create Ingress and Egress*	✓	✗	✓	✓	✓	✓	✗

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Tunnels section on the retrospective GigaVUE Cloud Suite Deployment Guide.							
GENEVE Decapsulation	✓	×	×	×	✓	×	×
Header Stripping	✓	✓	✓	✓	✓	✓	✓
Adaptive Packet Filtering (APF) without RegEx	✓	✓	✓	✓	✓	✓	✓
Application Session Filtering (ASF)	✓	✓	✓	✓	✓	✓	✓
Application Filtering Intelligence	✓	✓	✓	✓	✓	✓	✓
Application Metadata Intelligence	✓	✓	✓	✓	✓	✓	✓
GigaSMART NetFlow Generation	✓	✓	✓	✓	✓	✓	✓
Application Visualization	✓	✓	✓	✓	✓	✓	✓
Load	✓	✓	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Balancing							
SSL Decrypt	✓	✓	✓	✓	×	✓	✓
5G-Service Based Interface Application	×	×	✓	✓	✓	✓	×
5G-Cloud Application	×	×	✓	✓	×	✓	×
Secure Tunnels Encapsulation	×	✓	×	✓	✓	✓	✓
Secure Tunnels Decapsulation	×	✓	×	✓	✓	✓	✓
GRE-In-UDP Tunnel Decapsulation	×	×	✓	✓	×	✓	×

Application Intelligence

Application Intelligence provides a comprehensive solution that:

- identifies the applications contributing to the network traffic.
- isolates preferred application-specific traffic and directs it to the appropriate tools.
- exports relevant application metadata for further analytics and analysis.

Application Intelligence provides the following capabilities for virtual nodes:

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter

Points to Note for Application Intelligence

Point to note when configuring Application Intelligence:

1. For a monitoring domain, the following application can be configured only once, and all these applications must be configured in a single monitoring session.
   a. Application Visualization
   b. Application Filtering
   c. Application Metadata
2. For GigaVUE V Series Node version lesser than 6.3.00, Application Visualization, Application Filtering, Application Metadata, and Application Metadata Exporter (AMX) applications are not supported in the Monitoring Session.

3. When undeploying and redeploying the Monitoring session which has the Application Intelligence application, ensure to follow the steps given below:
   a. 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.
   b. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.
   c. Add the Application Intelligence applications.
   d. Modify the Number of Flows as per the below table:

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16GB RAM)	200k
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	200k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16GB RAM)	200k

      - 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..
      - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.

   e. Click **Deploy**.
4. After adding the above-listed applications and deploying the Monitoring Session, you cannot edit the Number of flows and Fast Mode. For more detailed information on Number of flows and Fast Mode, refer to Number of Flows and Fast Mode.
5. Once the Number of flows is added in any of the above-listed applications, the same value is applied to all the above-listed applications configured in that Monitoring Session. You cannot change it.
6. Once Fast Mode is enabled in any of the above-listed applications, then it is enabled for all the above-listed applications configured in that Monitoring Session. You cannot change it.

7. You can also configure Application Intelligence with Precryption, prefiltering, and secure tunnels. Refer to Precryption, Prefiltering, and Secure Tunnels topics in the respective cloud deployment guides for more detailed information on how to configure these features.
8. Small Form Factor for VMware ESXi is not supported when using applications like Application Visualization, Application Metadata, Application Filtering. Refer to *Configure GigaVUE V Series Nodes for VMware ESXi* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)more detailed information on how to deploy GigaVUE V Series Node, where you select the Form Factor.

Application Visualization

Application Visualization identifies and monitors all applications contributing to the network traffic and reports on the total applications and the total bandwidth they consume over a select period. Application Visualization allows you to identify more than 3,200 applications. It displays the traffic statistics in bytes and packets.

Refer to the following topics for more detailed information on how to configure the application and view the statistics:

- Configure Application Visualization for Virtual Environment
- View Application Statistics for Application Visualization
- Configure Filtering and Metadata Export for Selected Applications in Application Visualization

Configure Application Visualization for Virtual Environment

Application Visualization can be configured in the **Edit Monitoring Session** Canvas Page. To add an Application Visualization application to the canvas, follow the steps given below:

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

view appears.

3. In the Application quick view, enter or select the following details:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter a name for the application.</td></tr>
<tr><td>Description</td><td>Enter the description.</td></tr>
<tr><td>Export Interval</td><td>The time interval in seconds at which the export must be done. The export interval is set to 300 seconds. It cannot be modified.</td></tr>
<tr><td colspan="2">Advanced Settings</td></tr>
<tr><td>Number of Flows</td><td>The number of flows supported by the application.
Refer to the following table for the maximum number of flows supported for VMware, AWS, Nutanix, and Azure platforms.
<table>
<tr><th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr>
<tr><td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
<tr><td>AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr>
<tr><td></td><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr>
<tr><td>Azure</td><td>Large (Standard_D8s_V4)</td><td>500k</td></tr>
<tr><td></td><td>Medium (Standard_D4s_v4)</td><td>100k</td></tr>
<tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</table>

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..
If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.
</td></tr>
<tr><td>Monitoring</td><td>You can use this option, enable or disable the Application Visualization application functionality.</td></tr>
<tr><td>Fast Mode</td><td>Enable the Fast Mode option for performance (less CPU cycles and less memory utilization) improvement. When the Fast Mode is enabled, some or all of the attributes of the applications will be disabled. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and limitations of the Fast Mode.
Note: This option is disabled for NetVUE Base Bundle License.</td></tr>
</table>

4. Click **Save**.

View Application Statistics for Application Visualization

To view the application Statistics for the Application Visualization application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the statistics page:
   a. **Total Traffic**: Displays the total traffic of the network. Use the drop-down menus to change the parameters. You can use the **Select Tags** filter option to filter the traffic related to the selected application tags.
   b. **Total Applications** : You can view all the applications and their bandwidth in the network. You can also perform filtering and exporting metadata for selected applications. Refer to Configure Filtering and Metadata Export for Selected Applications in Application Visualization for more detailed information on how to perform filtering and exporting metadata for selected applications.
   c. **Top 10 Applications**: Click on the drop-down menu that displays **All** and select the **Top 10** . Displays the Top 10 applications running in the network based on the metrics.
   d. **Top 10 Application Families**: You can view a graphical representation of top 10 applications running in the network based on the metrics. When you hover over the Pie-chart, GigaVUE-FM shows the application families in the network.

   You can view the statistics for past hour, past 24 hours, or past 7 days. GigaVUE-FM also allows you to view statistics for a particular period by selecting the date and time. The selected data and time must be with in the past 7 days.

   GigaVUE-FM takes more than five minutes to display the application statistics since the export interval is fixed at five minutes. For the first fifteen minutes after creating the solution, if GigaVUE-FM receives traffic, it will show real-time data. If there is no traffic during this time, it will take at least eleven minutes to display the statistics once traffic is received.

Configure Filtering and Metadata Export for Selected Applications in Application Visualization

This section describes how to perform filtering and exporting metadata for selected applications when configuring Application Visualization. Refer to the following steps for more detailed information:

- Filter Traffic for Selected Applications
- Export Metadata for Selected Applications

Filter Traffic for Selected Applications

1. Click the Application Visualization application in the Monitoring Session Canvas page and select **Details**. The Application quick view appears.
2. Click on **STATISTICS** tab.
3. Click on the drop-down menu that displays **Top 10** and select the **All** .
4. Select the applications for which you want to filter traffic.

   > **NOTE:** Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.

5. Click **Actions > Filter Selected Applications**. The **Filter Selected Applications** dialog box opens.
6. In the **Filter Selected Applications** dialog box, Select the existing Application Filtering map or New Map from the **Send to Map** drop-down menu.
   - **New Map:**Select this option if you wish to create a new application filtering map, to filter the traffic from the applications.
   - **Existing map:** Select this option if you have already configured an application filtering map and you wish to send the traffic for filtering to that map.
7. Under the **Applications** section, choose the traffic as pass or drop for the selected applications.
8. Click **Send to Map**.

> **NOTE:** If the **New Map** option is selected from the **Send to Map** drop-down menu. Then, the map quick view appears. Refer to step 3, 4, 5, 6, and 7 in Configure Application Filtering Intelligence for Virtual Environmentsection for more detailed instructions on how to configure Application Filtering.

Export Metadata for Selected Applications

1. Click the Application Visualization application and select **Details**. The Application quick view appears.
2. Click on **STATISTICS** tab.
3. Click on the drop-down menu that displays **Top 10** and select the **All** .
4. Select the applications for which you want to export metadata.

   > **NOTE:** Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.

5. Click **Actions > Export Metadata for Selected Applications**. The **Export Metadata for Selected Applications** dialog box opens.
6. In the **Export Metadata for Selected Applications** dialog box, Select the existing Application Metadata application or New Exporter from the **Send to Exporter** drop-down menu.
   - **New Application Metadata:**Select this option if you wish to create a new application metadata, to export metadata from the applications.
   - **Existing Application Metadata Application:** Select this option if you have already configured an Application Metadata Intelligence application and you wish to send the traffic for exporting metadata from the applications.
7. Click **Export**.

NOTE: If the **New Application Metadata** option is selected from the **Send to Exporters** drop-down menu. Then, the application quick view appears. Refer to steps 3 and 4 in Configure Application Metadata Intelligence for Virtual Environment sectionConfigure Application Filtering Intelligence for Virtual Environmentfor more detailed instructions on how to configure Application Metadata application.

User Defined Application

This feature allows you to identify unclassified TCP, UDP, HTTP, and HTTPS applications and extract their application name and ID.

Refer to the following topic for more detailed information:

- Supported Protocols and Attributes
- Mindata
- Supported RegExp Syntax
- Limitations
- Create Rules for User Defined Application

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regex patterns, refer Supported RegExp Syntax

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Reque	Partially	Client	REGEXP	\/fupload\/(create_file|new_

		st URI	Normalized URL (path + request)	to Server Only		slice|upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http:\/\/gigamon.com\/
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\/football\/.*
	cts-cookie	Cookie (Raw)	Raw value of	Client to	REGEXP	.*tEstCoOkie.*

			the HTTP Cookie header line	Server Only		
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
http2	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file|new_slice|upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http:\/\/gigamon.com\/
ssl	common_name	Domain Name	Domain name from Client Hello message or the certificate		REGEXP	(.*\.)?gigamon\.com

	stc-subject_alt_name	Subject Alt Name (s)	List of host names which belong to the same certificate	Server to Client Only	REGEXP	(.*\.)?gigamon\.com
rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http:\/\/www.music.tv\/recorded\/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a packet, excluding the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata
	port	Server	Server		UINT16	80-4350

		Port	(listen) port number		RANGE as REGEXP String	
sip	user_ agent	User Agent	Software used	Both, Client to Server or Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Messa ge Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Messa ge Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addres s	IP address of the server		IPV4 as REGEXP String	62.132.12.30\/24
	dscp	DSCP Value	DSCP from Differen tia ted Service (DS) Field in IP		UINT8 as REGEXP String	33

			header			
	resolv_ name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Addres s	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a 4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Different ia ted Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it

( ) [ ]	Groups a series of expressions together Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
| [<start>-<end>]	Separates values contained in ( ). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog | cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_ number>	Matches for a direct binary with octal input
\x<hexadecimal-number>\x	Matches for a direct binary with hexadecimal input
\[<character-set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per GigaVUE-FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Create Rules for User Defined Application

To create a new application:

You can create rules for User Defined Application in two ways:

1. Go to **Inventory > Resouces > User-defined Applications**. Refer to User Defined Applications section in GigaVUEGigaVUE Fabric Management Guide for details.
2. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**. Follow the steps listed below:
   a. Select a Monitoring Session from the list view. Navigate to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas page appears.
   b. In the canvas, click on the  icon on the left side of the page to view the traffic processing elements.

c. Select **User Defined Applications** under **Options** menu.

d. Enable the **User-defined Applications** toggle button.

e. Click **New Application**. The New Application page appears.

f. Enter the **User-Defined Application Name**.

g. Enter **Priority**. The value must be between 1 and 120.

> **NOTE:** The lowest value has the highest priority.

h. In the Rules dialog box, select the following details:

- Choose the **Protocol** from the list of protocols.
- Choose the **Attributes** from the list of attributes.
- Choose the **Values** from the list of values.

Using the **Actions** Button, you can perform the following actions:

i. Click **Save**.

To add the created applications to the Monitoring Session:

1. In the **User Defined Applications** tab, click Add Application button.
2. Select the applications that must be added.
3. Click **Done**.

After creating rules for User defined Applications, you can add it to Application Filtering when configuring the applications. Refer to Add Application section for more detailed information on how to add User defined Application when configuring Application Filtering.

Application Filtering Intelligence

Application Filtering Intelligence allows filtering of traffic based on the application (such as YouTube, Netflix, Sophos, or Facebook) or application family (such as antivirus, web, erp, or instant-messaging) or application tags. Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.

Refer to the following topics for more detailed information and step-by-step instructions on how to configure Application Filtering Intelligence application and view the staistics:

- Configure Application Filtering Intelligence for Virtual Environment
- View Application Statistics for Application Filtering

Configure Application Filtering Intelligence for Virtual Environment

Application Filtering Intelligence (AFI) can be configured in the Monitoring Session Canvas. To add Application Filtering application to the canvas, follow the steps given below:

1. Drag and drop **New Map** from **New** to the graphical workspace.
2. Click the application and select **Details**. The Application quick view appears.
3. Enable **Application Filtering** in the **GENERAL** tab.

4. In the Application quick view, enter or select the following details in the **GENERAL** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Filtering Settings	
Bidirectional	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Buffer	This option is enabled by default.
Buffer Count Before	Number of packets that should be buffered until the flow is identified. If the flow is not identified even after reaching the maximum number of packets buffered, then all the subsequent packets of this session will be dropped.
Protocol	Select the Protocol. The packet matching the selected protocol will be filtered. The default value is TCP-UDP.
Packet Count	Enable or Disable Packet Count. Packet Count is disabled by default.
Number of packets **Note**: This field appears only when Packet Count field is enabled.	Specifies the number of packets to forward to the tool port for each session match. After the packet count is reached, subsequent packets for the session are dropped. The packet count includes the packet that triggered the creation of the session. The default is disable, which means that all packets will be forwarded to the tool port. The range is from 2 to 100.
Session Fields	
Session Field	The Packet fields to be considered for creating the Session / traffic flow (Session key fields)
Action	Add or Remove 'VlanId' Packet field for creating the session / traffic flow.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td colspan="2">Advanced Settings</td></tr>
<tr><td>Number of Flows</td><td>The number of flows supported by the application.
Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.
<table>
<tr><th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr>
<tr><td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
<tr><td>AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr>
<tr><td></td><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr>
<tr><td>Azure</td><td>Large (Standard_D8s_V4)</td><td>500k</td></tr>
<tr><td></td><td>Medium (Standard_D4s_v4)</td><td>100k</td></tr>
<tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</table>

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..
If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.
</td></tr>
<tr><td>Fast Mode</td><td>Enable the Fast Mode option for performance (less CPU cycles and less memory utilization) improvement. When the Fast Mode is enabled, some or all of the attributes of the applications will be disabled. You can view the list of attributes/applications available in the fast mode by navigating to the app editor under AMI feature in the GigaVUE-FM. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and Limitations of the Fast Mode.</td></tr>
</table>

5. Click the **RULESETS** 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. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions.

   Enter the following details for each of the Rule Set created:

Parameter	Description
Priority	A 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.
AE ID	Application Endpoint ID will be used as source or destination object for creating or connecting links
Actions	Using this option, you can perform the following functions: • **New Ruleset**- Use to add a new Rule Set. **Note**: A maximum of 5 Rule Sets can be created. • **New Rule**- Use to add a New Rule **Note**: A maximum of 25 Rules can be created per rule set. • **Delete this Ruleset**- Use to delete the Ruleset
RULES	
Rule	Use the toggle button to **Pass** or **Drop** the traffic through the map.

Parameter	Description
Condition	Select any one of the conditions from the drop-down menu and search or select the attributes. Use the + and - buttons to add or remove a condition with a Rule. Click ... and select **Add Condition** to add more conditions. **Note**: A maximum of 4 conditions can be created per Rule.
APPLICATION FILTERING Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select a Type. The available options are: • **Application Family:** Each application is mapped only mapped to one Application Family ▪ Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. ▪ In the Traffic Action column, select **Pass** or **Drop** to pass or drop the traffic. You can also use **Pass All** or **Drop All** to allow or drop the traffic for all the applications. • **Application Tag:** Each application can be mapped to one or more Application Tags. ▪ Select an **Application Tag** and the **Applications** that needs to be filtered from the traffic. ▪ In the Traffic Action column, select **Pass** or **Drop** to pass or drop the traffic. You can also use **Pass All** or **Drop All** to allow or drop the traffic for all the applications. **User Defined Applications**: To configure User Defined Applications for AFI, follow the steps given below. **a.** Enable **User Defined Applications** toggle button in the **Options** page. Refer to User Defined Application topic for more detailed information on what is user defined applications and how to configure it. **b.** In this **Add Application** dialog box, select **User Defined Applications** from the **Application Family** list.

6. To pass or drop any remaining traffic in the network, enter the priority and AE ID in the default rule set available. Select **Pass** or **Drop** option for **Any Remaining Traffic** field.
7. Click the **THRESHOLDS** tab. For more details on how to create and apply threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

8. To reuse the configuration, click **Add to Library**. Save the application filtering configurations using one of the following ways:
   a. Select an existing group from the **Select Group** list or create a **New Group** with a name.
   b. Enter a description in the **Description** field, and click **Save**.
   c. The saved map can be found in the **Map Library** in the **Edit Monitoring Session** Canvas Page.
9. Click **Save**.

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

When using the Application Filtering application, you can either use a single tunnel, to tunnel all the filtered traffic from the application or use a separate tunnel for each rule configured.

View Application Statistics for Application Filtering

To view the application Statistics for the Application filtering application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the Application Filtering application statistics page:
   a. Rules - Displays the rules created in this application.
   b. Pass App (Bytes) - Displays the packet that pass through the applications selected.
   c. Drop App (Bytes) - Displays the packets that are dropped by the applications selected.
   d. Pass Rule (Bytes) - Displays the packet that pass through the rule sets configured.
   e. Drop Rule (Bytes) - Displays the packets that are dropped by the rule sets configured.

Application Metadata Intelligence

Application Metadata Intelligence allows you to export metadata from applications that are detected in the network traffic. The records can be exported to a collector either in IPFIX or CEF format through the IP interface or the management interface. You can also use the application metadata attributes for purposes other than security, such as to determine the network or application health, to track the long-lived sessions seen in the network, and so on.

Application Metadata Intelligence generates more than 5000 attributes for more than 3200 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

Application Metadata Intelligence (AMI) is enabled to multi-collect protocols with more than one metadata attribute of the same type. The multi-collect feature supports additional protocols such as DNS, GTP,GTPV2, DHCP, HTTP, HTTPS, SSL, HTTP_PROXY, HTTP2, KERBEROS5, and DHCP6.

The generated metadata is exported in IPFIX (IP Flow Information Export) format and CEF (Common Even Format) to security analytics and forensics tools thereby providing greater visibility to enforce corporate compliance.

The output from the Application Metadata Intelligence in CEF format can also be converted to JSON format using Application Metadata Exporter (AMX) application. To learn more about AMX application refer to Application Intelligence—Application Metadata Exporter

Refer to following topics for more detailed information and step-by-step instructions on how to configure Application Metadata Intelligence and view the statistics:

- Configure Application Metadata Intelligence for Virtual Environment
- View Application Statistics for Application Metadata

You can convert the output from the Application Metadata Intelligence (AMI) which is in CEF format into JSON format and send it to the cloud tools and Kafka. Refer toApplication Metadata Exporter for detailed information on AMX and how to configure it..

Configure Application Metadata Intelligence for Virtual Environment

Application Metadata Intelligence (AMI) can be configured in the Monitoring Session Canvas. To add Application Metadata Intelligence application to the canvas, follow the steps given below:

NOTE: Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.

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

view appears.

3. In the Application quick view, enter or select the following details in the **General** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Metadata Settings	
Flow Direction	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Multi Collect	• **Enable**: Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. Multi Collect is enabled by default, when a new cache is created. Multi Collect is enabled, when upgraded from an older release. • **Disable**: Disables the multi-collect of attributes within a given Metadata Store cache. This option is disabled by default. **Note**: Do not enable this option if you are going to export the Application Metadata using the AMX application. There can be only one attribute in a JSON object, therefore Multi-collect is not supported when configuring the AMX application.
Data Link	If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
Observation ID	Enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
Enable DPI Packet limit	This field is used to restrict the number of packets in a particular session to be sent to the DPI engine instead of sending all the packets in order to improve the AMI performance. The value must range between 20 - 50 as the first 20 to 50 packets contains the most significant attributes.
Advanced Settings	
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr>
<tr><td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
<tr><td>AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr>
<tr><td></td><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr>
<tr><td>Azure</td><td>Large (Standard_D8s_V4)</td><td>500k</td></tr>
<tr><td></td><td>Medium (Standard_D4s_v4)</td><td>100k</td></tr>
<tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</table>

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..
If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.

</td></tr>
<tr><td>Fast Mode</td><td>Enable the Fast Mode option for performance (less CPU cycles and less memory utilization) improvement. When the Fast Mode is enabled, some or all of the attributes of the applications will be disabled. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and Limitations of the Fast Mode.</td></tr>
<tr><td>Aggregate Round-trip Time</td><td>Enable this option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.
<table>
<tr><th>Protocol</th><th>Arrtibute</th></tr>
<tr><td>http</td><td>rtt</td></tr>
<tr><td>icmp</td><td>rtt</td></tr>
<tr><td>icmp6</td><td>rtt</td></tr>
<tr><td>ssh</td><td>rtt</td></tr>
<tr><td>tcp</td><td>rtt</td></tr>
<tr><td>tcp</td><td>rtt_app</td></tr>
</table>
</td></tr>
</table>

Parameter	Description	
	telnet	rtt
	wsp	connect_rtt
	wsp	query_rtt

4. In the Application quick view, enter or select the following details in the **Exporters** tab:

Parameter	Description
Exporter Name	Enter a name for the Exporter.
Actions	Using this option, you can perform the following functions: • **Add Exporter** - Use to add a new Exporter to this Application Metadata Intelligence Application. A maximum of 5 exporters can be added. • **Save as New Template** - Use to save the current configuration as a new custom tool template. • **Delete this Exporter** - Use to delete the Exporter.
Template	Use to select the tool template. Refer to *Tool Templates*section in GigaVUE Fabric Management Guide for more information on tool templates and how to create custom tool templates.
Export Params	Select any one of the following options: • **Application Name** - Exports Application Name Attribute in AMI records. Enable this option to export Application Name attribute with network attributes • **Application Family** - Exports Application Family Attribute in AMI records. Enable this option to export Application Family attribute with network attributes • **Application Tags** - Exports Application Tag Attribute in AMI records. Enable this option to export Application Tag attribute with network attributes
Format	Select NetFlow or CEF
NetFlow: Select this option to use NetFlow	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool. **Note**: It is recommended to select **Cohesive** from the drop-down menu, as NetFlow exports network and transport parameters only.
Enable Maximum Packet Length	Enable this option to edit the interface MTU value.
Maximum Packet Length (This option appears only when Enable Maximum Packet Length option is enabled)	Using this field, you can configure the maximum length of the packet that can be exported. Enter this value less than or equal to egress interface MTU value to avoid fragmentation. The value can range between 1280 and 9001.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
Version	Select the NetFlow version. The supported versions are V5, V9, IPFIX (V10).
Template Refresh Interval	Enter the time interval at which the template must be refreshed in

Parameter	Description
	seconds
CEF: Select this option to use CEF	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
APPLICATION & ATTRIBUTES: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFlow V5, V9, NetFlow IPFIX(V10), or CEF when the flow direction is Uni-Directional in the above **Template** drop-down menu.) **NOTE:** When you edit application attributes during an AMI deployment with background traffic, you may experience minor data loss until the update completes.	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select a Type. The available options are: • **Application Family:** Each application is mapped only mapped to one Application Family ▪ Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the **Attribute** column. You can select the required attributes. • **Application Tag:** Each application can be mapped to one or more Application Tags. ▪ Select an **Application Tag** and the **Applications** that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the **Attribute** column. You can select the required attributes.
NETWORK & TRANSPORT PARAMETERS: Select the Network and the transport packet attributes with the respective parameters	
Data Link	Select any one of the parameters such as Source MAC address, Destination MAC Address and VLAN.
Interface	Select any one of the parameter such as Input Physical, Output Physical and Input Name.
IP	Select the parameter as Version if required.
IPv4	Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.

Parameter	Description
IPv6	Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
Transport	Select the required attributes. By default, Source Port, Destination Port are enabled.
Counter	Select the Bytes, and Packets.
Timestamp	Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
Flow	Select the parameter as End Reason if required.
GTP-U	Select the required parameters such as QFI and TEID.
Outer IPv4	Select any one of the parameter such as Source or Destination.
Outer IPv6	Select any one of the parameter such as Source or Destination.

NOTE: In the exporter record, the generator ID represents the hostname of the GigaVUE V Series Node. Any changes to the hostname after deploying the Monitoring Domain with the AMI application will not be reflected in the exporter record.

5. Click **Save**.

After configuring the Application Metadata application, follow the below steps to create an egress tunnel:

1. In the canvas page, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. Enter the **Alias**, **Description** and select **UDP** as **Type**.

   NOTE: When using Application Metadata, if you create a tunnel to send the output to the tools, select UDP as the tunnel type.
   You can either use a single tunnel to export all metadata from the application or configure separate tunnels for each exporter.
3. Enter the **MTU** value.
4. **L4 Destination IP Address** - Enter the IP address of the tool port. If using Application Metadata Exporter (AMX), enter the data subnet IP address of the V Series Node where AMX application is deployed. Refer to Application Metadata Exporter for details.
5. **Source L4 Port** - The 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.
6. **Destination L4 Port** - The 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. The destination port must match the AMX ingestor port number to ensure seamless data forwarding from AMI to AMX.

> **NOTE:** If the export format is CEF, the default value for L4 destination port is 514. If the export format is NetFlow, the default value for L4 destination port is 2055.

To deploy the configured Application Metadata Intelligence application, follow the below steps:

1. On the Monitoring Session canvas page, click **Deploy** from the **Actions** menu to deploy the Monitoring Session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on the V Series Node.
2. You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab. 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.
   - 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 or Instances.

After adding the Application Metadata application and deploying Monitoring Session, you cannot change the **Aggregate Round Trip time** option.

> **NOTE:** To configure Application Metadata Intelligence in physical environment, refer to Create an Application Intelligence Session in Physical Environment.

View Application Statistics for Application Metadata

To view the application Statistics for the Application Metadata application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the Application Metadata application statistics page:
   a. Exporter Name - Displays the exporters created for this application.
   b. Format - Displays the format as NetFlow or CEF, for the individual exporters.
   c. Packet Sent/ Sec - Displays the count of packets sent per second for each exporter.

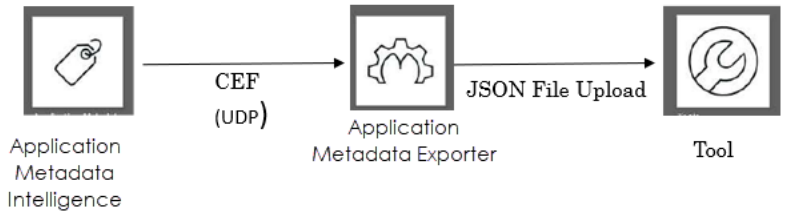
Application Metadata Exporter

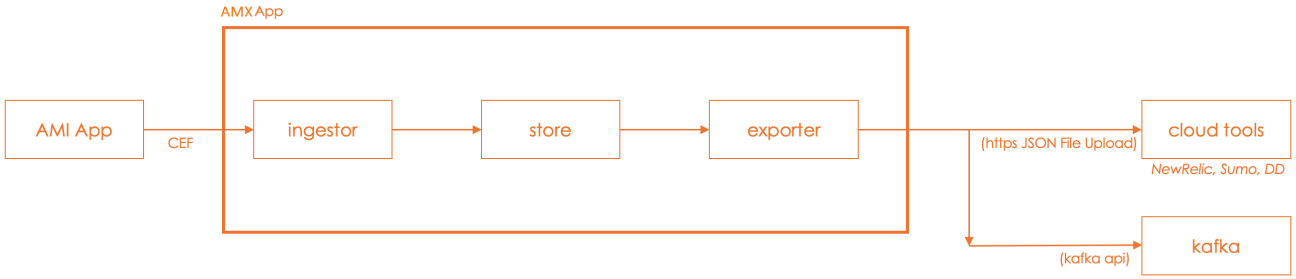
Refer to the following topics for more detailed information on the various ways to configure AMX:

- Export AMI output by AMX
- Export NetFlow/IPFIX from third-party sources or AMI using the NetFlow Integrator in AMX
- Export of 3G/4G/5G Control Plane Metadata by AMX
- Export of GigaVUE Enriched Metadata for Mobile Networks by AMX
- Export of GigaVUE Enriched Metadata for Cloud Workloads by AMX

Export AMI output by AMX

Application Metadata Exporter(AMX) application converts the output from the Application Metadata Intelligence (AMI) in CEF format into JSON format and sends it to the cloud tools and Kafka Consumers.





The AMX application can be deployed only on a GigaVUE V Series Node and connected to Application Metadata Intelligence running on a physical node or a virtual machine. GigaVUE-FM manages the AMX application and the AMI.

Export NetFlow/IPFIX from third-party sources or AMI using the NetFlow Integrator in AMX

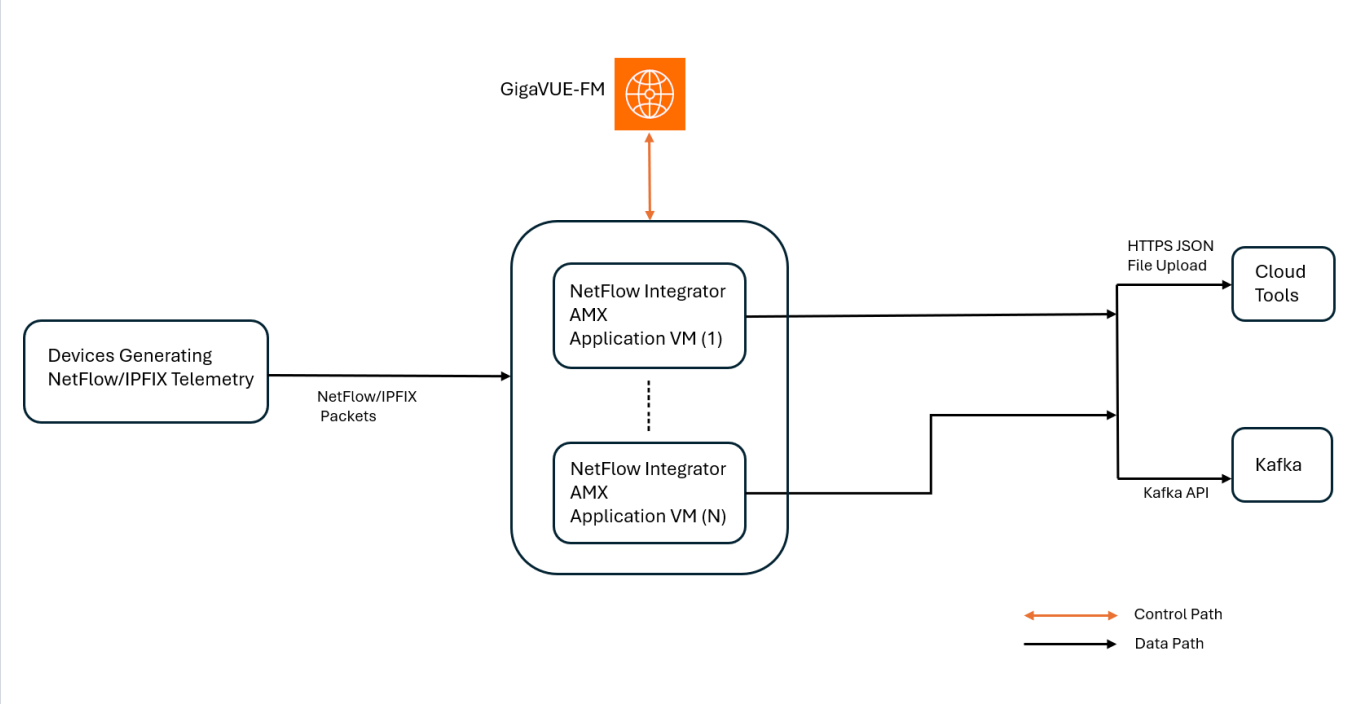
The AMX application with NetFlow Integrator functionality supports ingesting NetFlow/IPFIX flow records from various sources and devices, such as firewalls, routers, and switches. These packets are parsed and converted into a standardized JSON format and exported over

HTTPS or Kafka to the external tools.

Since the AMI application also generates the NetFlow/IPFIX flow records, with the NetFlow Integrator functionality added to AMX, AMX can export the AMI NetFlow/IPFIX as JSON to the tools.

Integrating NetFlow/IPFIX flow records into the AMX application provides a consolidated view of network traffic and NetFlow insights by exporting them as separate JSONs to the tools. This integration provides a unified source of network traffic data and NetFlow/IPFIX insights in standard JSON format, compatible with most Network Performance Monitoring (NPM) tools.

The diagram below illustrates how the AMX application ingests, processes, and exports network traffic data collected from various devices. GigaVUE-FM acts as the central control system for AMX.



Supported Platforms

- VMware ESXi
- VMware NSX-T

License Requirement

NetFlow Integrator functionality will be disabled by default and requires a valid SecureVUE Plus VBL license to enable it

Rules and Notes

- The recommended deployment method for NetFlow Integrator functionality is Third Party Orchestration.
- Only the elements specified in the mapping file will be included in the JSON output. Editing or customizing the mapping file is not supported. Refer to Supported Element Types for NetFlow Integrator Element Mapping.
- The NetFlow/IPFIX ingestor type does not support Metadata Enrichment. Refer to Configure Application Metadata Exporter Application.
- An AMX application cannot be configured to ingest both CEF and NetFlow/IPFIX formats at the same time.
- A maximum of 12 NetFlow/IPFIX type ingestors can be configured per deployment.
- A single instance of AMX processes traffic in line with the published performance KPIs. Additional instances should be deployed if traffic volume exceeds these thresholds to ensure stable and efficient performance. For details regarding performance KPIs, Contact Technical Support.
- The memory and CPU requirements for a single AMX instance are as follows:
  - CPU : 40 cores
  - Disk : 128 GB
  - Memory : 64 GB

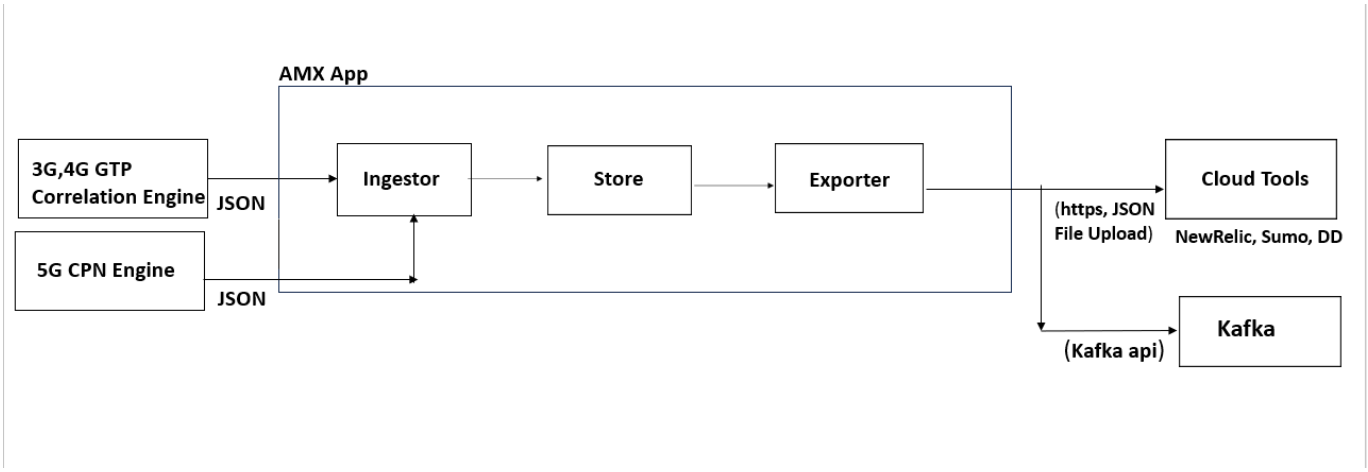
To know more about the configuration of NetFlow Integrator functionality, supported element types, and related statistics details, refer to the following sections:

- Configure Application Metadata Exporter Application
- Supported Element Types for NetFlow Integrator Element Mapping
- View Application Statistics for Application Metadata Exporter

Export of 3G/4G/5G Control Plane Metadata by AMX

The AMX application can also export the 3G/4G control plane metadata received from the GTP Correlation engine and 5G control plane metadata received from the 5G CPN engine to the cloud tools and Kafka in Flat JSON format.

The AMX application can be deployed only on a GigaVUE V Series Node and can be connected to a GTP Correlation / 5G CPN engine running on a physical node.



Export of GigaVUE Enriched Metadata for Mobile Networks by AMX

The metadata enrichment enhances service provider analytics, by generating metadata on 5G/4G/3G network traffic. The AMX correlates the user plane metadata produced by AMI with the control plane metadata produced by the GTP/5G correlation mobility application to produce an enriched metadata feed for the mobile networks. This data feed helps with use cases like service personalization, planning, and many others by containing information about the

- Subscriber Session
- Over the Top Application
- Handset Type
- Location
- Flow throughput calculation attributes - DL, UL bytes, and time stamps.
- Application Protocol
- Core Network Information
- User Tunnel Information

Export of GigaVUE Enriched Metadata for Mobile Networks is supported only for GigaVUE V Series Node deployed using Third Party Orchestration on VMware ESXi.

Additionally, you can also deploy GigaVUE V Series Node using KVM hypervisor for deploying Application Metadata Exporter (AMX) application on GigaVUE-FM Hardware Appliance.

For deployment instructions, refer to:

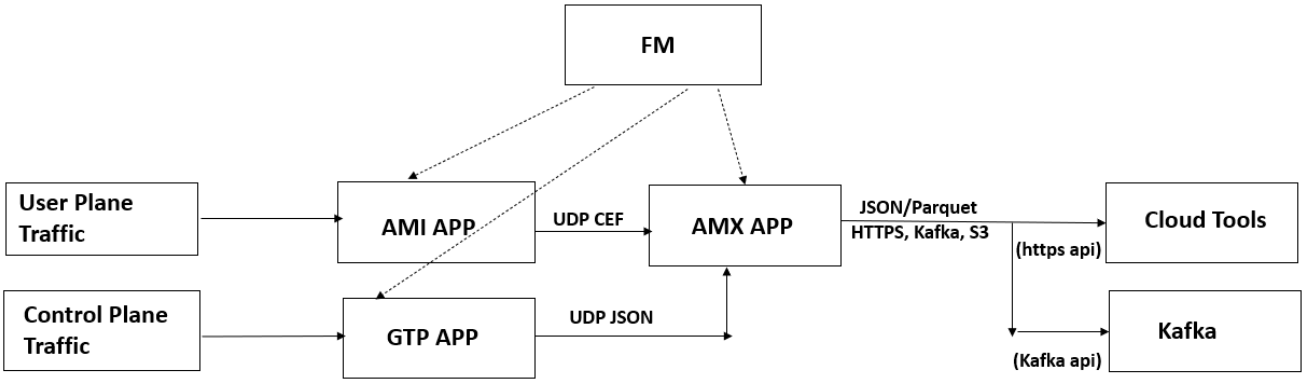
- Configure GigaVUE Fabric Components using VMware ESXi
- Configure GigaVUE V Series Nodes using KVM for AMX Deployment

User Plane and Control Plane traffic from the following devices are supported for exporting GigaVUE Enriched Metadata for Mobile Networks:

- GigaVUE-HC3
- GigaVUE-HC1-Plus

> **NOTE:** For GigaVUE-HC1-Plus, the AMI application must be configured on the built-in engine to efficiently handle higher traffic loads. The plug-in engine can be used for the Control Plane traffic.

For information on Control Plane Metadata, refer to Control Plane Metadata.



Export of GigaVUE Enriched Metadata for Cloud Workloads by AMX

Required License: SecureVUE Plus License

GigaVUE Enriched Metadata for Cloud Workloads provides comprehensive situational awareness to address security and performance pain points in a timely manner. It enriches application metadata from N/S and lateral traffic with key host environment details that allow you to find critical information as follows:

- The location of the workloads hosted and their virtual network.
- The operational environment to which the workloads belong.
- The instance types used, images, and tags that the workload contains.
- The host name, the security associations like security group name, IAM instance profile name.

Export of GigaVUE Enriched Metadata for Cloud Workloads (Virtual Machines)

Export of GigaVUE® Enriched Metadata (GEM) for Cloud Workloads is supported on the following cloud platforms:

- AWS
- Azure
- VMware (ESXi and NSX-T)

This functionality works by using the inventory API which is queried in the following intervals.

- VMware: 300 sec
- AWS: 30 sec
- Azure: 60 sec

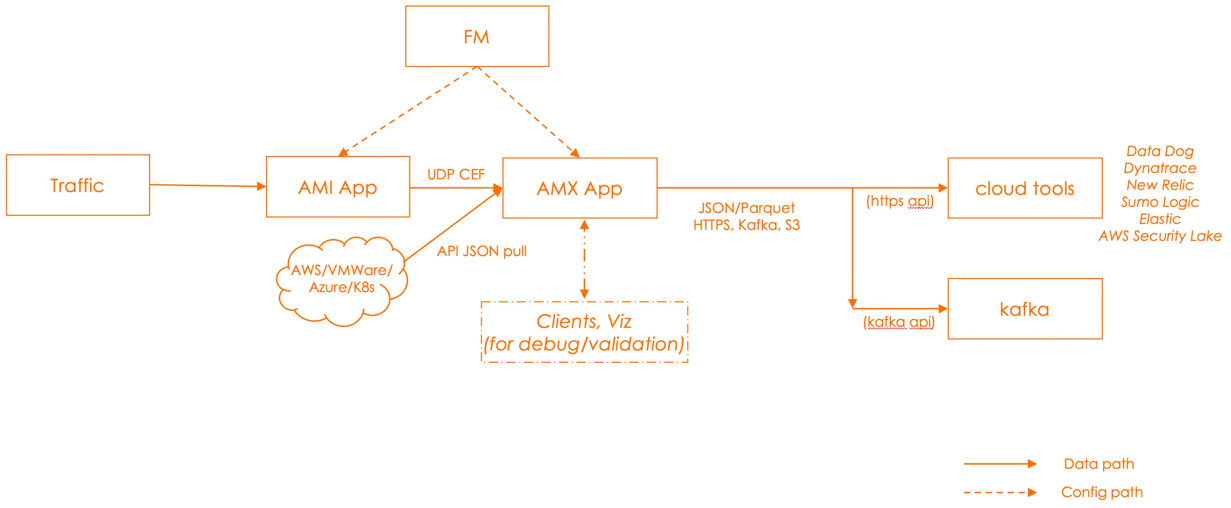
The default inventory query interval should suffice in most cases, however the interval can be customized in extreme situations. Please contact Gigamon Support for assistance.

In addition to the fixed intervals of polling the inventory, you can subscribe to the following optional services to get automatic updates from the workloads.

- AWS- Requires setup of SQS in AWS and event subscription settings to access it.
- Azure - Requires setup of Storage Queue and Events Subscription and settings to access it.
- VMware - No additional configuration is required as the dynamic updates are supported by default.

Refer to Prerequisites for Export of GigaVUE Enriched Metadata for Cloud Workloads for more detailed information.

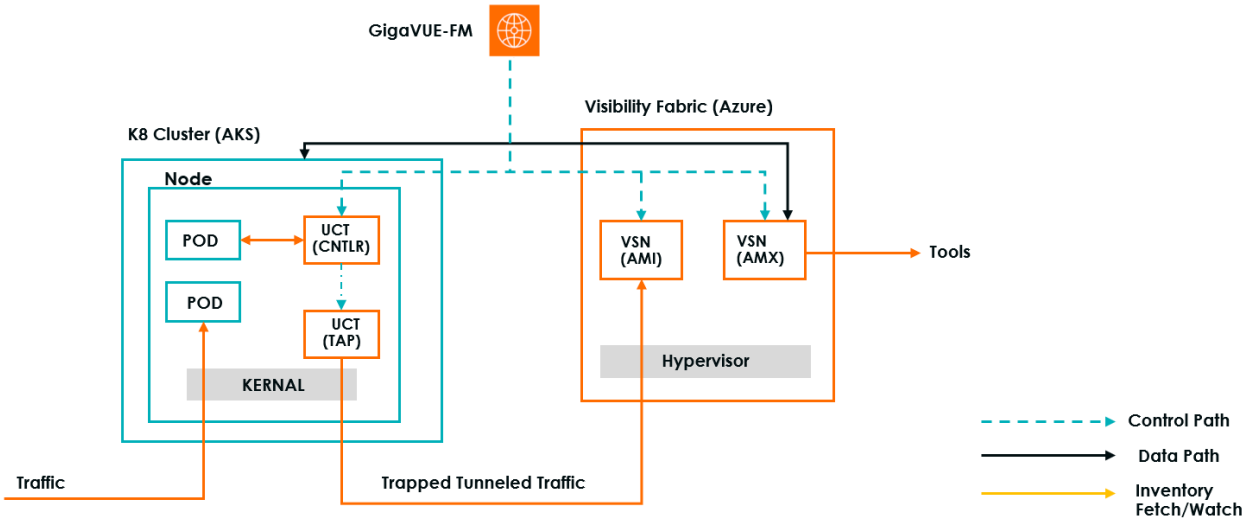
AMX application performs the enrichment every 10 seconds. It picks the flow records, which are 15 seconds or older, to allow any delays in fetching the inventory details, and uses the IP address of the endpoints to enrich the records based on the selected attributes. Refer to the following figure for a high-level illustration of the solution. The solution can be deployed using GigaVUE-FM or Third Party Orchestration.



The enrichment supported depends on the type of platform. Refer to Attributes for GigaVUE Enriched Metadata for Cloud Workloads for more details.

Export of GigaVUE Enriched Metadata for Cloud Workloads Kubernetes containers - Azure Kubernetes Service (AKS)

This feature enables the enrichment of flow records with Kubernetes inventory data, unlocking deeper visibility and advanced use cases for containerized environments. In the current Kubernetes visibility solution for AKS, UCT-TAP ships tapped traffic (both east-west and north-south) to the AMI node deployed in Azure. The AMI node then forwards metadata to the AMX node, also deployed in Azure. With the new enhancement, the AMX node enriches the AMI metadata using Kubernetes inventory details fetched directly from the AKS cluster.



GigaVUE-FM queries the Kubernetes inventory every 300 seconds, which is the default interval for monitoring events between inventory fetches. The default inventory query interval should suffice in most cases; however the interval can be customized in extreme situations. Please contact Gigamon Support for assistance.

NOTE: In addition to sending regular queries every 300 seconds, GigaVUE-FM enables a watch mechanism that updates AMX with every event—create, delete, and modify.

For Kubernetes environments, GigaVUE-FM uses a controller with access to the Kubernetes API. The controller subscribes to cluster events and pushes updates in near real-time. No built-in optional services are required.

Refer to Prerequisites for Export of GigaVUE Enriched Metadata for Cloud Workloads for more detailed information.

Refer to the following topics for more detailed information and configuration:

- AMX Application Deployment Options
- Prerequisites for Application Metadata Exporter
- Rules and Notes
- Configure Application Metadata Exporter Application
- View Application Statistics for Application Metadata Exporter
- Attributes for GigaVUE Enriched Metadata for Mobile Networks.
- Attributes for GigaVUE Enriched Metadata for Cloud Workloads

AMX Application Deployment Options

The output from the Application Metadata Intelligence or GTP Correlation Engine is sent to the AMX application, which exports it to the tools in the required formats. AMX application is always deployed in GigaVUE V Series Node. The GigaSMART application sending data to the AMX application can be on hardware or the GigaVUE V Series Node. Based on where the GigaSMART applications are, there can be four deployment methods:

NOTE: For exporting GigaVUE Enriched Metadata for Cloud Workloads, AMI should be deployed in GigaVUE V Series Nodes.

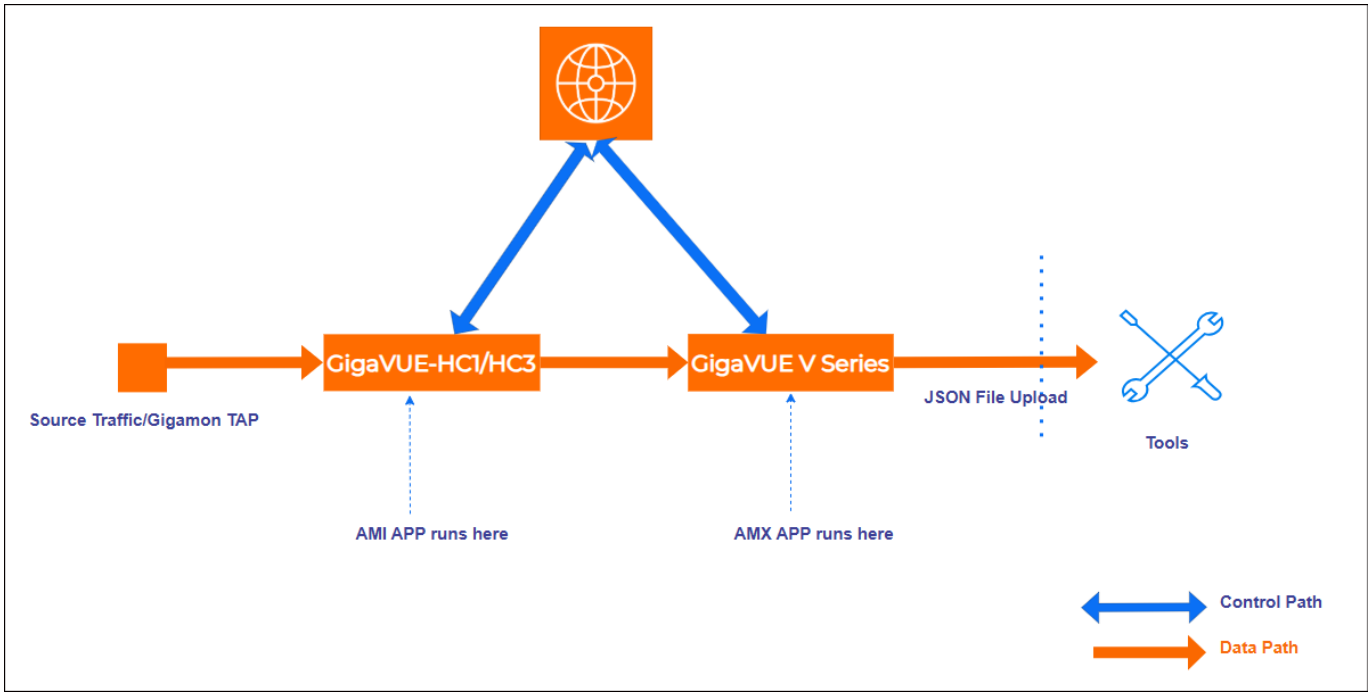
- On-Premises
    - Hardware (AMI)
    - Hardware (Control Plane Metadata)
    - Virtual (VMware)
- Public Cloud

On-Premises

Hardware (AMI)

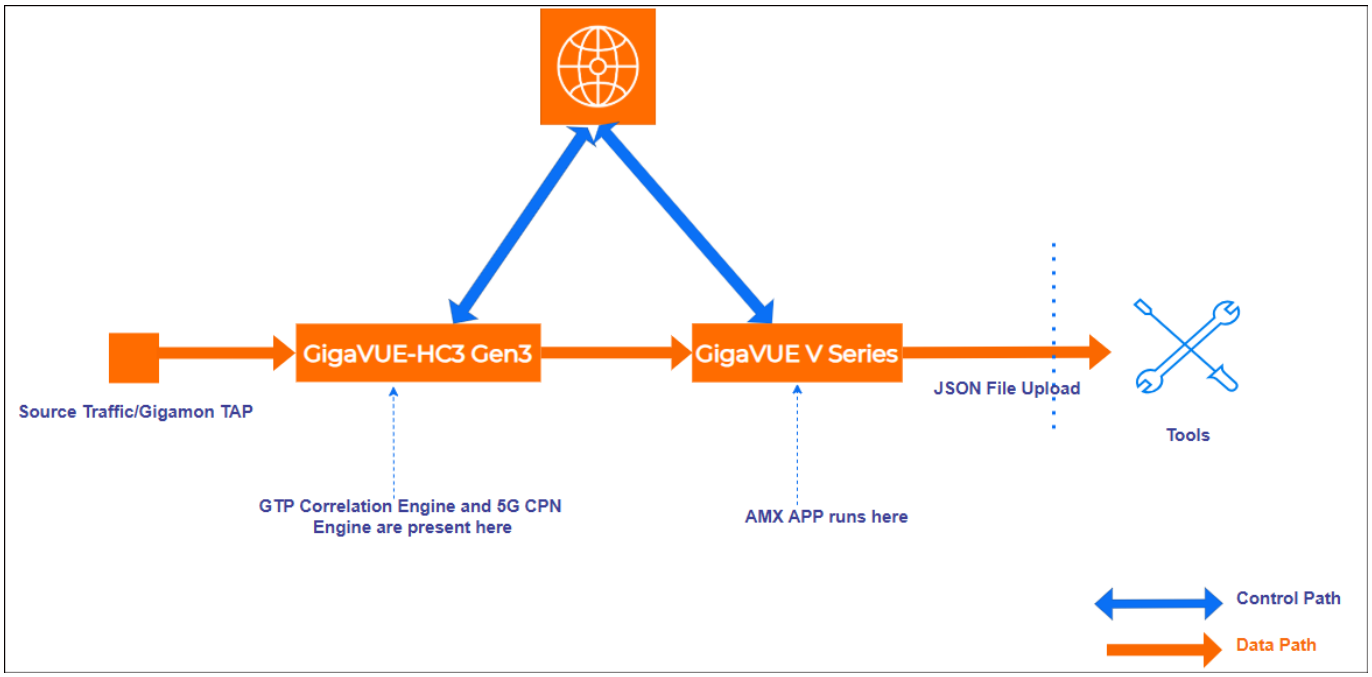
In hardware deployments, the Application Metadata Intelligence (AMI) runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi. The output from the AMI in CEF format is sent to the AMX application in GigaVUE V Series Node. The performance of the device and the application is managed by GigaVUE-FM. The following devices support the integration of AMX application:

- GigaVUE-HC1
- GigaVUE-HC3
- GigaVUE-HC1-Plus



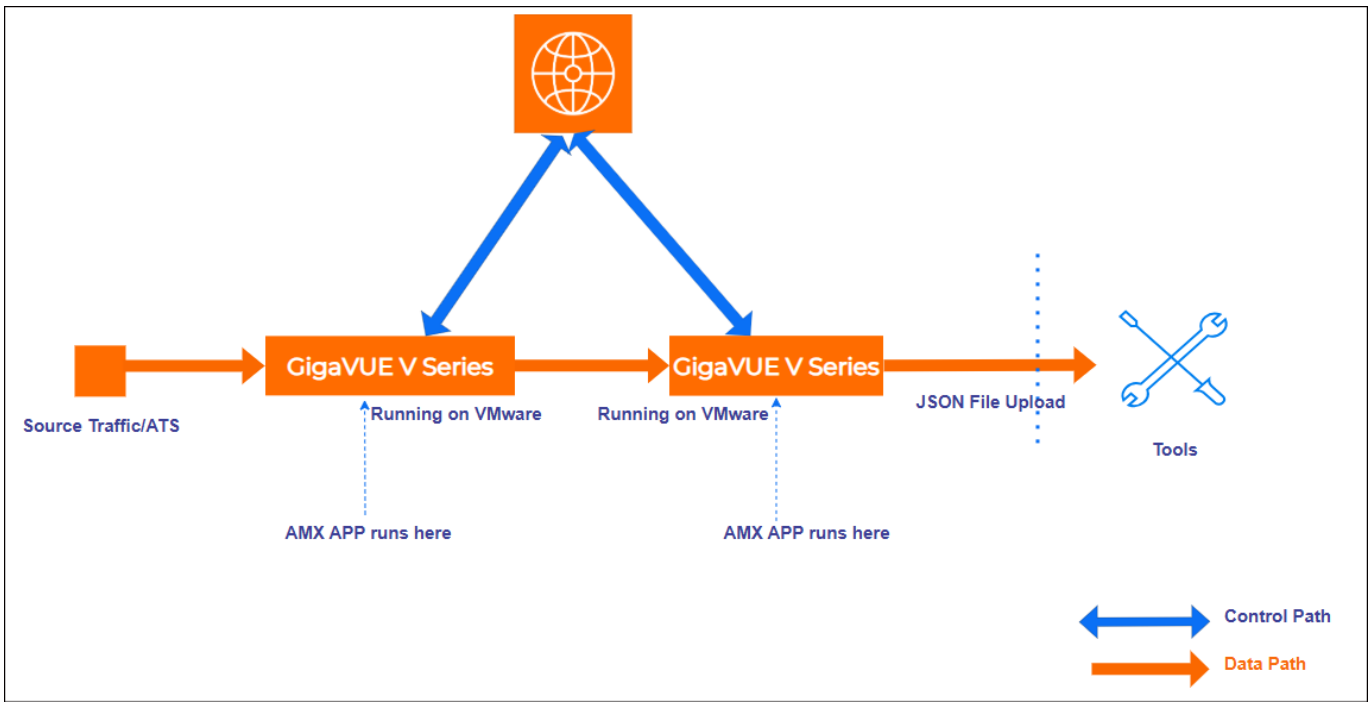
Hardware (Control Plane Metadata)

In hardware deployments, the GTP Correlation Engine runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi. The output from the GTP Correlation Engine in Flat JSON format is sent to the AMX application in GigaVUE V Series Node. The performance of the device and the application is managed by GigaVUE-FM. The GigaVUE-HC3 Gen3 devices support the integration of AMX application.



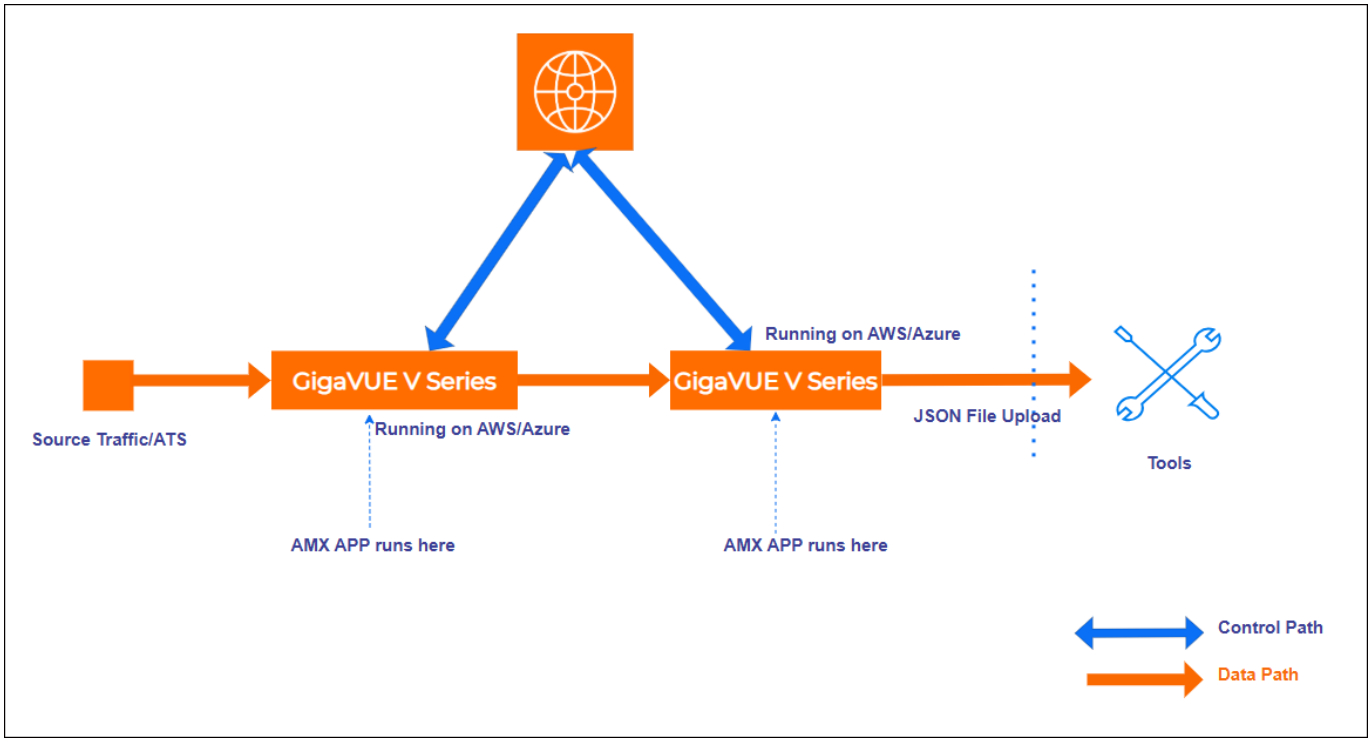
Private Cloud (VMware)

In the Private Cloud environment, the application is supported only on VMware and can be deployed in the VMware as shown in the diagram.



Public Cloud

In the Public Cloud environment, the application is supported on AWS and Azure platforms, and can be deployed as shown in the diagram:



Prerequisites for Application Metadata Exporter

Prerequisites for AWS

Prerequisites to follow when creating a monitoring domain and deploying a GigaVUE V Series Node in AWS:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer to Create a Monitoring Domain.
- Select **Instance type** with three or more NICs. Select one subnet to receive the mirrored GRE or VXLAN tunnel traffic and one other for tools subnet. Refer Configure GigaVUE Fabric Components in GigaVUE-FM for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, the Volume Size field appears on the **AWS Fabric Launch Configuration** page. Enter the Volume Size as 80GB.

Prerequisites for Azure

Prerequisites to follow when creating a monitoring domain and deploying GigaVUE V Series node in Azure:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer *Create Monitoring Domain* section in the respective GigaVUE Cloud Suite Deployment Guide for more detailed information on how to create a monitoring domain.
- Select **Size** with three or more NICs. Select one subnet to receive the mirrored GRE or VXLAN tunnel traffic and one other for tools subnet. Refer to Configure GigaVUE Fabric Components in GigaVUE-FM for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, the **Disk Size** field appears on the **Azure Fabric Launch Configuration** page. Enter the Disk Size as 80GB.

Prerequisites for VMware

Prerequisites to follow when creating a monitoring domain and deploying GigaVUE V Series Node in VMware:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer Create Monitoring Domain for VMware ESXi section in *GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)* for more detailed information on how to create a monitoring domain and deploy GigaVUE V Series Nodes.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, select the **Form Factor** field as 80GB on the **VMware Configuration** page. Refer to *Configure GigaVUE Fabric Components using VMware ESXi* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more detailed information on how to deploy GigaVUE V Series Node.
- When uploading the OVF files for GigaVUE V Series Node deployment using third party orchestration, ensure to select the OVF files with 80GB disk space. Refer to the following topics for more detailed information.
  - Deploying GigaVUE V Series Node using Third Party Orchestration (VMware ESXi): *Configure GigaVUE Fabric Components using VMware ESXi* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
  - Deploying GigaVUE V Series Node using Third Party Orchestration (VMware vCenter): *Configure GigaVUE Fabric Components using VMware vCenter* in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration.

Prerequisites for Third Party Orchestration

Prerequisites to follow when creating a monitoring domain and deploying a GigaVUE V Series Node in Third Party Orchestration:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer to Create a Monitoring Domain.
- Select **Instance type** with three or more NICs. Select one subnet to receive the mirrored GRE or VXLAN tunnel traffic and one other for tools subnet. Refer Deploy Fabric Components using Generic Mode for more detailed information on how to deploy a GigaVUE V Series Node.

- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, enter the Volume Size, Disk Size, or Form Factor as 80 GB, depending on the selected platform.

Prerequisites for Export of GigaVUE Enriched Metadata for Cloud Workloads

This section provides the detailed steps that need to be performed in each platform for exporting the enriched metadata from cloud workloads.

AWS:

The following section describes how to setup IAM roles with least privileges for exporting GigaVUE Enriched Metadata for Cloud Workloads:

1. Create two IAM roles.
   - First one is for AMX instance that gets launched to let it access assume role (sts) service. (AMXEC2Role)
   - Second one is with **ec2ReadOnlyAccess** permission. (AMXToAssumeRole)
2. Map the instance role to an assume role that has AmazonEC2ReadOnlyAccess permissions.
   a. Copy arn name of the AMXEC2Role.
   b. Click **AMXToAssumeRole > Trust Relationships > Edit Trust Policy**.
   c. Click **Add a principal**.
   d. Select IAM role as Principal Type. Paste the AMXEC2Role arn that was copied. This is the critical step of mapping two IAM roles.
   e. Click **Add principal > Update Policy**
3. Add the arn of AMXToAssumeRole in AMX ingestion configuration options.
   a. Copy the arn and add as aws_assume_role_arn in AWS ingestion configuration.
   b. If aws_assume_role_arn is configured, there is no need to provide token and keys.
4. (optional) Create an SQS queue. Refer to Create a queue using the Amazon SQS console in AWS documentation for more detailed information.
5. (optional) Create an EventBridge Rule. In the **Select Target** field, select the SQS queue created in the previous step. Refer to Creating rules that react to events in Amazon EventBridge in AWS documentation for more detailed information.
6. (optional) Add SQS URL in AMX ingestion configuration options.

   Copy the url and add as aws_sqs_url in AWS ingestion configuration.

Azure:

The following instructions need to be configured in Azure for exporting enriched metadata from Azure workloads:

1. Create a Storage Account under the Resource Group. Refer to Create an Azure storage account in Azure documentation for more detailed information.
2. Create a Storage Queue under the Storage Account. Refer to Quickstart: Create a queue and add a message with the Azure portal in Azure Documentation for more detailed information.
3. Under the Storage Account > Access Control (IAM). Select "Storage Queue Data Contributor" and select your ID to add the IAM role. Refer to Assign Azure roles using the Azure portal for more detailed information on how to assign roles.
4. (optional) Create an Event subscription. Refer to Create an event subscription section in Azure documentation.
5. In the Storage queue, switch the **Authentication method** to **Access key**.

The following section describes how to setup IAM permissions in Azure for exporting GigaVUE Enriched Metadata for Cloud Workloads:

Register an application and assign a role to the application with the following set of minimum IAM permissions. Refer to Register an application with Microsoft Entra ID and create a service principal and Assign a role to the application in the Azure documentation for more detailed information.

Minimum IAM permission required:

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/publicIPAddresses/read
Microsoft.Network/networkSecurityGroups/read
Microsoft.Compute/virtualMachineScaleSets/read
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/images/read
Microsoft.Network/networkInterfaces/read
Microsoft.Resources/subscriptions/read
Microsoft.Resources/subscriptions/resourceGroups/read
```

VMware:

The following are the prerequisites required:

- URL - The URL of VMware vCenter.
- Username - Username of the VMware vCenter
- Password - vCenter password used to connect to the vCenter

- Self Signed Certificate
  - True - When self signed certificate = true, use the default certificate.
  - False - When self signed certificate = false, a PKI certificate must be used. Refer to Replace the Default Certificate with a Custom Certificate Using the vSphere Client section in VMware documentation for more detailed information on how to replace the default certificate with a custom certificate.

    NOTE: The default CA trust store is supported based on the Ubuntu version 22.04.4. The default trust store cannot be updated to include internal CA certificates.

- Ensure that the VM tools are installed on the ESXi hosts that are being monitored to fetch the properties of the virtual machines.
- The minimum role required for exporting GigaVUE Enriched Metadata from VMware is **Read Only Role**. Refer to vCenter Server System Roles section in VMware documentation for more detailed information.

Kubernetes (AKS)

The following are the prerequisites required:

1. GEM for Kubernetes requires configuring an Ingestor in GigaVUE-FM to set up the source for Kubernetes containers. You must upload the k8s_kubeconfig file during the initial setup. GigaVUE-FM does not allow viewing or editing the uploaded file. However, you can upload a new file to overwrite the existing one.
2. Each ingestor must have a separate k8s_kubeconfig file. If you need to configure multiple clusters, create a dedicated k8s_kubeconfig file and a corresponding Ingestor for each cluster. You can configure up to four Ingestors.
3. Ensure that the user credentials specified in the kubeconfig file have the following sufficient read permissions to access the required Kubernetes resources.
   - Pods
   - Nodes
   - Namespace
   - Endpoints
   - Services
4. If DNS/FQDN is not configured, map the cluster name (as specified in the server field of the kubeconfig file) to a valid IP address in the /etc/hosts file.

Rules and Notes

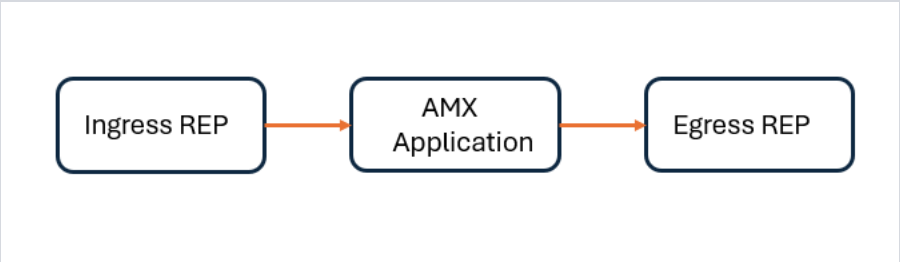
- The GigaVUE V Series Node deployed must be entirely dedicated to the AMX application, it cannot have other applications in it.

- The monitoring session can only have Raw End Point (REP), it cannot have other applications, maps, or tunnels when using the AMX application. Refer to *Create Raw Endpoint*section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more detailed information on how to add a REP to the monitoring session and how to configure it.
- When using this application for production usage, it is recommended to use large size Virtual Machines.
- If you reload the GigaVUE V Series Node after configuring the AMX application, then the Ingestor in the AMX application fails.
- When using GigaVUE Enriched Metadata for Cloud Workloads, if duplicate IP address is assigned to workloads, the metadata received from the most recently queried workload will be enriched. Hence, it is not recommended to use the feature in environments that are prone to have duplicate IP addresses.
- When using GigaVUE Enriched Metadata for Cloud Workloads, endpoints and the GigaVUE V Series Node running AMI and AMX should be co-located in the same cloud platform.

Configure Application Metadata Exporter Application

In GigaVUE-FM, you must do the following to configure the Application Metadata Exporter application in the Monitoring Session.

S.No	Steps	Refer to
1	Create an ingress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (VMware NSX-T) Create Raw Endpoint (AWS) Create Raw Endpoint (Azure) Create Raw Endpoint (Third Party Orchestration)
2	Create a link between the ingress REP and Application Metadata Exporter application	N/A
3	Create an egress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (VMware NSX-T) Create Raw Endpoint (AWS) Create Raw Endpoint (Azure) Create Raw Endpoint (Third Party Orchestration)
4	Create a link between the Application Metadata Exporter application and egress REP	N/A



To add AMX application:

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

   Notes:

   - Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.
   - You can use the Third-Party Orchestration method when deploying fabric components—such as the AMX V Series Node—on your own.
   - When deploying AMX using the Third-Party Orchestration method, Monitoring Session must also be configured in the same work flow. To deploy through Third Party Orchestration, go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**.
   - Before deploying AMX, ensure to change the **Traffic Acquisition Method** to **Customer Orchestrated Source** in the Monitoring Domain. Refer to Create Monitoring Domain.

2. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
3. In the canvas, click the icon on the left side of the page to view the traffic processing elements. Drag and drop **AMX** from **APPLICATIONS** to the graphical workspace. The application quick view appears.
4. Enter the **Alias** for the application.

5. In the **Ingestor** section, enter or select the following details. Click ⊕ to add another ingestor to add multiple inputs to the AMX application and click ⊖ to remove an existing ingestor.

Fields	Description
Name	Enter name for the Ingestor.
Port	Enter the port number to which the Application Metadata or the NetFlow/IPFIX or the Control Plane metadata must be ingested.
Type	Select any one of the following: AMI - Select this option if the input is AMI. Mobility Control Plane - Select this option if the input is Control Plane Metadata. NetFlow/IPFIX - Select this option if the input type is NetFlow/IPFIX. **Note**: If your selected ingestor type is NetFlow/IPFIX, Metadata Enrichment will be disabled by default. NetFlow/IPFIX input type is not supported for Metadata Enrichment.

6. Enter or select the following details in the **Metadata Enrichment** section:

> You can use the **Actions** button to add multiple Metadata Enrichment. Keep in mind the following when configuring multiple Metadata Enrichment:
>
> - You can only configure either Mobility or Workload enrichment
> - You can only configure one Metadata enrichment with either **Mobility** or **Workload** as the **Type**
> - You can only configure a maximum of 5 Metadata enrichment with **Others** as the **Type**.

Fields	Description
Enrichment Name	Enter a unique name for each enrichment.
Enable	Use this option to enable the enrichment.
Type	Select the type from the drop-down menu. o Mobility o Workload o Others
Mobility	
Attribute Fields	Select the attributes from the list. You can use the **Select All** option to select all the available attributes. Refer to Attributes for GigaVUE Enriched Metadata for Mobile Networks. for more detailed information on the list of available attributes and their description.
Workload	
Platforms	Select the platform in which your Workload Virtual Machines are present. • VMware vCenter • AWS • Azure • Kubernetes
Attribute Fields	Select the attributes from the list. You can use the **Select All** option to select all the available attributes. Refer to Attributes for GigaVUE Enriched Metadata for Cloud Workloadsfor more detailed information on the list of available attributes and their description. **Advanced Options** The advanced options allow you to configure additional details like interval and delay. Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**.
Source Information	Enter the details of the source. **Name**: Enter a unique name for each Source Information. The name should be unique across the ingestor and the source information.

Fields	Description
	Key: The default keys for each platform are listed as follows. Click **+** to add more keys. **AWS**: Refer to Manage access keys for IAM users section in AWS documentation for more detailed information on how to create an access key ID and a secret access key. ▪ aws_access_key_id ▪ aws_secret_access_key ▪ aws_region **Azure**: Refer to Register a Microsoft Entra app and create a service principal section in Azure documentation for more detailed information on how to configure client ID, client secret, tenant ID, and subscription ID in Azure. ▪ azure_client_id ▪ azure_client_secret ▪ azure_tenant_id ▪ azure_subscription_id **VMware**: ▪ url - The URL of VMware vCenter. ▪ username - Username of the VMware vCenter ▪ password - vCenter password used to connect to the vCenter ▪ self_signed_certificate **Kubernetes**: ▪ Upload **kubeconfig** YAML file from your local. Refer to Kubernetes (AKS) for Prerequisites details. **Value**: Enter the value for the keys. This field is editable after saving the changes. **Secure Keys**: Use this option to mask the value. After saving the changes, **Secure Keys** and **Key** fields are disabled and the value is masked. Click ⊕ to add another Source Information and click ⊖ to remove a Source Information. You can add multiple Source Information if your workloads are across different vCenters, AWS Accounts, or Azure Subscriptions. You can create an individual Source Information for each of the vCenters, AWS Accounts, or Azure Subscriptions.
Others: Use this setting to perform custom mapping for advanced use cases. For details contact Gigamon Support.	
Attribute Fields	Click **Add** and enter the attribute.
Settings	Click **Add** and enter the details.

7. Enter or select the following details in **Cloud Tools Export** section:

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Endpoint	Enter the endpoint URL where the cloud tool instance is installed and the ports are configured. Enable **Secure Endpoint** option to hide the API keys from the URL. Example: • Normal Endpoint: http://examples.com/mykey/key123 • Masked Endpoint: http://examples.com/mykey/****
Headers	Enter the custom header value of the cloud tool instance. Example: Add Content-Type: application/json in a separate header field. Ensure that the **Secure Keys** option is enabled.
Type	Select any one of the following: **AMI** - Select this option to export AMI. **Mobility Control**- Select this option to export control plane metadata. **AMI Enriched** - Select this option to export enriched metadata for cloud workloads. **NetFlow/IPFIX** - Select this option to export NetFlow/IPFIX packets to tools such as HTTPS or Kafka.
Account ID	Enter the account ID number of the selected Cloud Tool.
API Key	Enter the API key of the Cloud Tool.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Cloud Tool. Both IPv4 and IPv6 are supported. This field is optional.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Format	The default output format is JSON.
Zip	Enable the box to compress the output file. **Note**: Enable this field when using New Relic as the cloud tool.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Cloud Tool. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 20000 and the minimum is 10, however 1000 is the default value.

Fields	Description
Backoff Reset Window	With a non-zero value, the exporter keeps trying to reach the tool as many times as the retry. The default setting is 0, and the Backoff Reset Window is disabled at this value.
Request Timeout	This is the time exporter waits for a response back from the tool. The default value is 10 seconds.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**. **Note**: Refer to the deployment guides of the respective cloud tools for configuring the Key and Value.

8. Enter or select the following details in the **Kafka Exports** section:

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select any one of the following: AMI - Select this option to export AMI. Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata. NetFlow/IPFIX - Select this option to export NetFlow/IPFIX ingestor types.
Brokers	The URL that contains the Kafka cluster endpoints. Click ⊕ to add another broker and click ⊖ to remove an existing broker.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Kafka Broker. Both IPv4 and IPv6 are supported. This field is optional.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Format	The default output format is JSON.
Zip	Enable the box to compress the output file.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Kafka. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 20000 and the minimum is 10, however 1000 is the default value.

Fields	Description
Backoff Reset Window	With a non-zero value, the exporter keeps trying to reach the tool as many times as the retry. The default setting is 0, and the Backoff Reset Window is disabled at this value.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**.
Producer Configurations	Click **Add** to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN • sasl.username=username • sasl.password=password

9. Click **Save** to deploy the Monitoring Session. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to deploy the Monitoring Session.
10. Click **Deploy** from the **Actions** menu 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.

Switching to outer_ip for Mobility Enrichment

In 5G Control Plane (CP) records, only the lower 64 bits of the inner IP address are captured. To overcome this limitation, you can switch to outer_ip. Follow the steps below based on your configuration:

If AMX is already configured and the Monitoring Session is deployed:

1. Undeploy the Monitoring Session in GigaVUE-FM.
2. Create a new .yaml file in the GigaVUE V Series Node: vi /etc/amx_settings.yaml
3. Modify the enrichment mode:
```
# Default mobility enrichment mode: inner_ip (default) or outer_ip
mobility_outer_ip_version: <Enter version as v6 or v4>
mobility_enrichment_mode: outer_ip
```
4. Deploy the Monitoring Session.

During Initial AMX Configuration:

1. Create a new .yaml file in the GigaVUE V Series Node: vi /etc/amx_settings.yaml
2. Modify the enrichment mode:

```
# Default mobility enrichment mode: inner_ip (default) or outer_ip
mobility_outer_ip_version: <Enter version as v6 or v4>
mobility_enrichment_mode: outer_ip
```

3. Save the file and proceed with the deployment.

Application Monitoring Options

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab. Refer to View Application Statistics for Application Metadata Exporter for more detailed information.

View Application Statistics for Application Metadata Exporter

To view the application Statistics for the Application Metadata Exporter application, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**. The **Monitoring Sessions** Overview page appears.
2. Navigate to the **TRAFFIC PROCESSING** tab. In the canvas page, click the ⋮ menu button on the **AMX** application and select **Details**. The Application quick view appears.
3. Click on **STATISTICS** tab.
4. To view the statistics of a particular GigaVUE V Series Nodes, select the required GigaVUE V Series Node from the **V Series Nodes** drop-down menu.
5. Select the IP address of the GigaVUE V Series Node from the **V Series Node IP** drop-down menu to view the **Ingestor** and **Attributes Enrichment** statistics.

6. You can view the following in the Application Metadata Exporter application statistics page:
    a. **Exporter - Statistics to monitor exports from AMX**
        i. Name - Displays the name of exporters created for this application.
        ii. Exported Entries - Displays the number of entries available in the files that will be uploaded from AMX to the cloud tool or the Kafka consumers.
        iii. Average File Size - Displays the average size of the file.
        iv. File Uploads - Displays the number of file uploaded from the AMX to the cloud tool or the Kafka consumers.
        v. File Upload Errors - Displays the number of times the file was not uploaded to the cloud tools or Kafka consumers due to errors.

b. **Ingestor - Statistics to monitor ingestion**

i. Name - Displays the name of the ingestor created for this application.

ii. Packets Received - Displays the packets received from the AMI to AMX ingestor.

iii. Packets Dropped - Displays the packets dropped when the traffic passes from AMI to AMX ingestor.

iv. Octets Received - Displays the octets received from the AMI to AMX ingestor.

v. Octets Dropped - Displays the octets dropped when the traffic passes from AMI to AMX ingestor.

vi. Records Added - Displays the number of workload information pulled from the workload environment.

vii. Records Dropped - Displays the number of the workload details that were dropped from the workload environment.

viii. Request Success - Displays if the workload information was fetched from the cloud environment. The default interval at which the AMX fetches the workload information is 60 seconds.

ix. Request Authentication Errors - Displays if the workload information was not fetched from the cloud environment due to any authentication errors like wrong password.

x. Request Timedout Errors - Displays if the workload information was not fetched from the cloud environment even after the default interval of 60 seconds.

xi. Request Errors - Displays when the workload information could not be fetched from the cloud environment due to issues other than authentication failures or timeout conditions.

xii. Decode Success - Displays number of successful decoding operations performed by a system when processing NETFLOW/IPFIX packets.

xiii. Decode Fail - Displays the number of failed attempts to decode NETFLOW/IPFIX packets.

xiv. Elements Skipped - Displays number of data elements that were not processed or were omitted during the NETFLOW/IPFIX ingestion process.

c. **Attributes Enrichment**

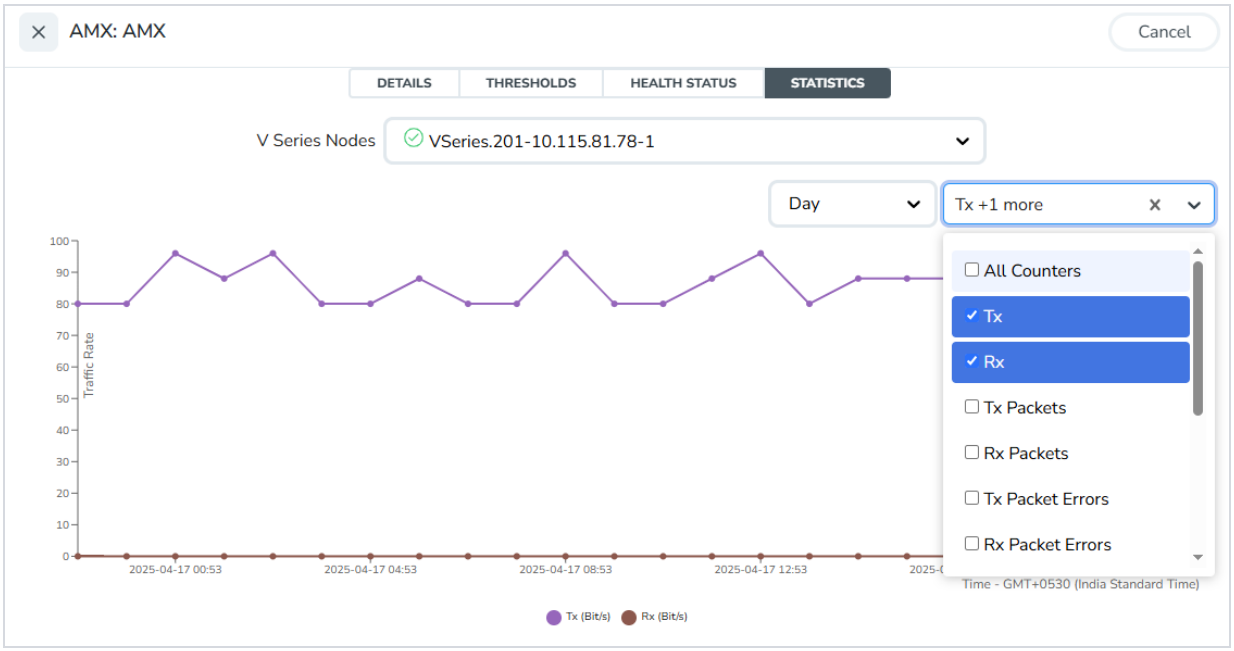
i. Name - Displays the name of the Metadata enrichment.

ii. One Min Percent - Displays the percentage of the traffic that is enriched from the last 1 minute.

iii. Five Min Percent - Displays the percentage of the traffic that is being enriched from the last 5 minutes.

iv. Ten Min Percent - Displays the percentage of the traffic that is being enriched from the last 10 minutes.

The below image shows the statistical details for general AMX application.

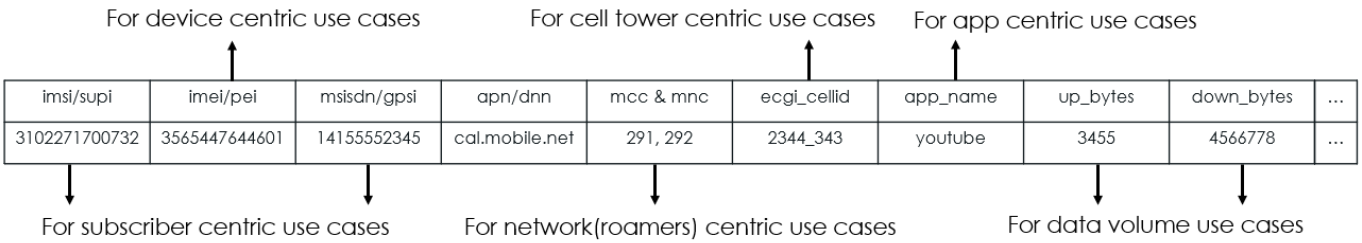


Attributes for GigaVUE Enriched Metadata for Mobile Networks.

This section describes the various attributes available within GigaVUE Enriched Metadata for Mobile Networks.

Each flow will generate only one record per export interval; however, in this section, the attributes are separated into the following categories:

- Control Plane Attributes
- User Plane Attributes



Control Plane Attributes

The control plane attributes are generated based on network signaling message transactions with successful responses. These include signaling transactions for session establishment, modification, deletion, and others. These attributes are used for enriching the user plane metadata with the corresponding control plane subscriber, device, and location information.

Attribute	Description
imsi	International Mobile Subscriber Identity. A 3GPP-defined unique private identifier for a mobile user on a 4G network.
imei	International Mobile Equipment Identity. A 3GPP-defined unique identifier for a mobile device on a 4G network.
msisdn	Mobile Station Integrated Services Digital Network. A 3GPP-defined identifier for a mobile device on a 4G network.
supi	Subscription Permanent Identifier. A 3GPP-defined unique identifier for a mobile user on a 5G network.
gpsi	Generic Public Subscription Identifier. A 3GPP-defined public identifier for a mobile user on a 5G network.
pei	Permanent Equipment identifier. A 3GPP-defined unique identifier for a mobile device on a 5G network.
ctrl_tun_ access_ ipv4_addr	Control Plane Access Tunnel IPv4 Address. MME identifier for S11, SGW identifier for S5/S8-C, AMF identifier for N11 and SGSN for Gn, GP
ctrl_tun_ access_ ipv6_addr	Control Plane Access Tunnel IPv6 Address. MME identifier for S11, SGW identifier for S5/S8-C, AMF identifier for N11 and SGSN for Gn, GP
ctrl_tun_ access_teid	Control Plane Access Tunnel Endpoint Identifier
ctrl_tun_ core_ipv4_ addr	Control Plane Core Tunnel IPv4 Address. SGW identifier for S11, PGW identifier for S5/S8-C, SMF identifier for N11 and GGSN for Gn,Gp
ctrl_tun_ core_ipv6_ addr	Control Plane Core Tunnel IPv6 Address. SGW identifier for S11, PGW identifier for S5/S8-C, SMF identifier for N11 and GGSN for Gn,Gp
ctrl_tun_ core_teid	Control Plane Core Tunnel Endpoint Identifier

user_tun_up_link_ipv4_addr	User Plane Uplink Tunnel IPv4 Address. Identifier of the SGW/UPF that receives the uplink user plane data from the eNodeB/gNodeB
user_tun_up_link_ipv6_addr	User Plane Uplink Tunnel IPv6 Address. Identifier of the SGW/UPF that receives the uplink user plane data from the eNodeB/gNodeB
user_tun_up_link_teid	User Plane Uplink Tunnel Endpoint Identifier
user_tun_down_link_ipv4_addr	User Plane Downlink Tunnel IPv4 Address. Identifier of the eNodeB/gNodeB that receives the uplink user plane data from the SGW/UPF
user_tun_down_link_ipv6_addr	User Plane Downlink Tunnel IPv6 Address. Identifier of the eNodeB/gNodeB that receives the uplink user plane data from the SGW/UPF
user_tun_down_link_teid	User Plane Downlink Tunnel Endpoint Identifier
if_name	3GPP Control Plane Interface Name
name	Name of the event on the 3GPP control plane interface
cause_code	Outcome of the event on the 3GPP control plane interface. Mostly set to 16 to indicate a successful event
sm_context_ref	Session Management Context
ebi	EPS(Evolved Packet System) Bearer ID
lbi	Linked Bearer Identity
pdu_session_id	PDU(Packet Data Unit) Session ID
apn	Access Point Name
dnn	Data Network Name
ue_ipv4_addr	User Equipment IPv4 Address
ue_ipv6_addr	User Equipment IPv6 Address
ue_ipv4v6_addr	User Equipment IPv4v6 Address
ue_non_ip_addr	User Equipment non-IP Address
ue_addr_type	User Equipment IP address type (IPv4 or IPv6)
qci	QoS Class Identifier
qfi	QoS Flow Identifier
five_qi	5G QoS Identifier

cgi_mcc	Mobile Country Code from Cell Global Identity
cgi_mnc	Mobile Network Code from Cell Global Identity
cgi_lac	Local Area Code from Cell Global Identity
cgi_cell_id	Cell Identification from Cell Global Identity
sai_mcc	Mobile Country Code from Service Area Identifier
sai_mnc	Mobile Network Code from Service Area Identifier
sai_lac	Local Area Code from Service Area Identifier
sai_sac	Service Area Code from Service Area Identifier
tai_mcc	Mobile Country Code from Tracking Area Identity
tai_mnc	Mobile Network Code from Tracking Area Identity
tai_tac	Tracking Area Code from Tracking Area Identity
ecgi_mcc	Mobile Country Code from E-UTRAN Cell Global Identifier
ecgi_mnc	Mobile Network Code from E-UTRAN Cell Global Identifier
ecgi_cell_id	Cell Identification from E-UTRAN Cell Global Identifier
lai_mcc	Mobile Country Code from Location Area Identity
lai_mnc	Mobile Network Code from Location Area Identity
lai_lac	Local Area Code from Location Area Identity
enode_id_mcc	Mobile Country Code from Evolved Node
enode_id_mnc	Mobile Network Code from Evolved Node
macro_enode_id	Evolved Node ID
ncgi_mcc	Mobile Country Code from NR Cell Global Identity
ncgi_mnc	Mobile Network Code from NR Cell Global Identity
ncgi_nr_cell_id	Cell Identification from NR Cell Global Identity
rat_type	Type of Radio Access Technology
snssai_sst	Slice/Service Type from Single Network Slice Selection Assistance Information
snssai_sd	Slice Differentiator id from Single Network Slice Selection Assistance Information

User Plane Attributes

The user plane attributes are generated by Application Metadata Intelligence (AMI), and include information such as IP addresses, protocols, timestamps, and byte/packet counters. These attributes are generated from the network flows and do not require DPI capabilities. The attributes for the mobile network traffic are generated for the inner IP flow by bypassing the outer headers

Attribute	Description
ts	Timestamp of the metadata generated in UTC
vendor	Identifying Gigamon as the vendor providing the metadata
version	Version number of the GigaSMART software release from the AMI application
generator	Identifies the Gigamon device that generates the user plane metadata. For example - HC3
src_ip	Source IPv4 address of the inner flow
dst_ip	Destination IPv4 address of the inner flow
src_mac	Source MAC address of the inner flow
dst_mac	Destination MAC address of the inner flow
mpls	MPLS Label if the flow has the MPLS header
protocol	Layer 4 protocol of the inner flow
src_port	Layer 4 protocol source port of the inner flow
dst_port	Layer 4 protocol destination port of the inner flow
device_inbound_ interface	Traffic receiving port on the Gigamon device example HC3
tcp-sport	Source TCP port
tcp_dport	Destination TCP port
udp_sport	Source UDP port
udp_dport	Destination UDP port
src_bytes	Source bytes from client to server in the flow including the outer and the inner IP header
dst_bytes	Destination bytes from client to server in the flow including the outer and the inner IP header
src_inner_bytes	Source bytes from the client to the server in the flow with the inner IP header (without the outer header)
dst_inner_bytes	Destination bytes from the server to the client in the flow with the inner IP header (without the outer header)
src_packets	Source packets from client to server in the flow including the header
dst_packets	Destination packets from client to server in the flow including header
total_bytes	Total bytes is sum of source and destination bytes
total_packets	Total packets is sum of source and destination packets
id	Unique flow id assigned to a flow
ingress_vlan_id	Vlan id in the packet received for the flow
src_ipv6	Source IPv6 address of the inner flow
dst_ipv6	Destination IPv6 address of the inner flow
ip_version	IP version v4, v6
ip_cos_id	QOS value in the IPv4 header
ip_dscp	DSCP value in the IPv4 header

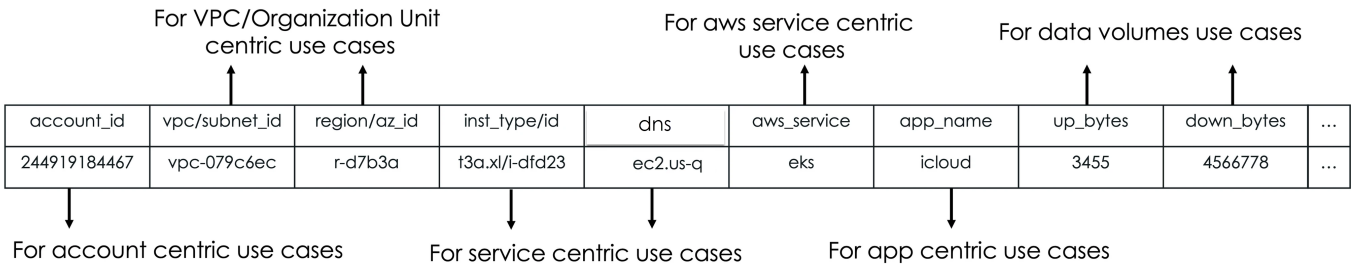
ip_ttl	Time to live in the IPv4 header
ip6hop_limit	Hop limit in the IPv6 header
flow_labelv6	flow label in the IPv6 header
ip6_ds	DSCP value in the IPv6 header
tcp_flags	TCP flag in the TCP header
gre_key	Generic routing encapsulation header key in the GRE header
ip_hdr_len	IPv4 header length
ip_frag_flags	IPv4 fragmentation flags
ipv6frag_flags	IPv6 fragmentation flags
ip_frag_id	IPv4 fragment id
ipv6frag_id	IPv6 fragment id
ip_frag_offset	IPv4 fragment offset
ipv6frag_offset	IPv6 fragment offset
ipv4opt	IPv4 options
ip_precendence_id	IPv4 precedence id
ip6precendence_id	IPv6 precedence id
ip_tot_len	IPv4 total length
ip6tot_len	IPv6 total length
ipv6hdr_len	IPv6 header length
payload_len_id	Payload length for the flow excluding the L3 IPv4 header
next_hdr_v6	Layer 4 protocol
icmp_type_v4	ICMP message type IPv4
icmp_code_v4	ICMP response code IPv4
icmp_code_v6	ICMP response code IPv6
icmp_type_v6	ICMP message type IPv6
tcp_ack_id	TCP ack id
tcp_hdr_len	TCP header length
tcp_seq_no	TCP sequence number
tcp_urgent_ptr	TCP urgent pointer
tcp_win_size	TCP window size
udp_msg_len	UDP message length
ip6traffic_class	IPv6 traffic class same as QoS in IPv4
flow_start_usec	Inner flow start time in microseconds in UTC
flow_end_usec	Inner flow end time in microseconds in UTC
flow_start_sec	Inner flow start time in seconds in UTC
flow_end_sec	Inner flow end time in seconds in UTC
start_time	Inner flow start time in milliseconds in UTC
end_time	Inner flow end time in milliseconds in UTC

egress_intf_id	egress IP interface-id for the Gigamon device sending the metadata
sys_up_time_first	Difference between the flow start time and the gigaSMART uptime in milliseconds
sys_up_time_last	Difference between the flow end time and the gigaSMART uptime in milliseconds
end_reason	Inner flow end reason – TCP ack, reset, inactive, etc
tcpflagsyn	TCP flag SYN from TCP header
tcpflagsynack	TCP flag SYNACK from TCP header
tcpflagfin	TCP flag FIN (finish)from TCP header
tcpflagrst	TCP flag RST (reset) from TCP header
Labels	Labels are added to the metadata by configuration in AMX. There can be multiple labels configured and added. Each label is configured as a key and a string value.
Labels configured in the JSON example in the section below	
label_event_type	Label identifying the vendor generating the event in the AMX exporter
label_deployment	Label identifying the deployment address of the AMX exporter
label_traffic	Label identifying the traffic region where the AMX is deployed
MSS	Maximum payload size a TCP segment can carry without the headers. The MSS value is exported at the beginning of a flow. Its exported only when bidirectional flows are configured.
aggr-window-size	The actual TCP window size minimum, mean, and maximum values, calculated separately for both sender and receiver packets.
zero-window	This captures TCP zero window event statistics for both sender and receiver, indicating when the TCP receive buffer is full and data transmission is temporarily paused due to flow control.

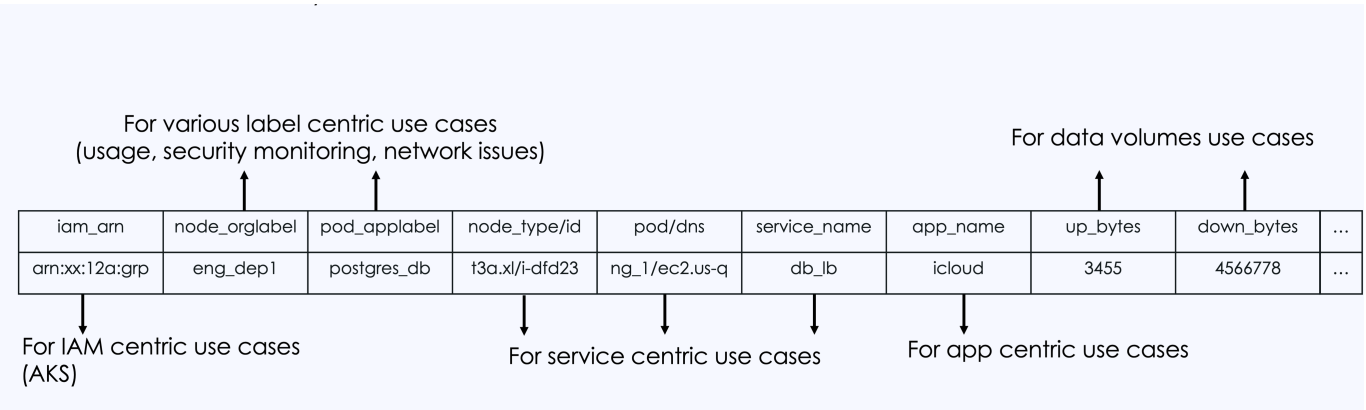
Attributes for GigaVUE Enriched Metadata for Cloud Workloads

This section describes the various attributes available within GigaVUE Enriched Metadata for Cloud Workloads for the following platforms:

- AWS
- Azure
- VMware vCenter



- Kubernetes



The following table defines the purpose and scope of each referenced dataset, detailing configuration, resource, and operational parameters across AWS, Azure, and Kubernetes environments to support multi-cloud infrastructure documentation.

AWS

Attribute	Description	Source	Destination
aws_ instance_id	ID of the EC2 instance	✓	✓
aws_ instance_ type	Type of EC2 instance	✓	✓
aws_ availability_ zone	Availability Zone of the EC2 instance	✓	✓
aws_image_ id	ID of the base image use for EC2 instance	✓	✓
aws_private_ dns_name	Private DNS hostname name assigned to the EC2 instance	✓	✓
aws_private_ ip	Private IPv4 address assigned to the EC2 instance	✓	✓
aws_public_ dns_name	Public DNS name assigned to the EC2 instance	✓	✓
aws_public_ ip	Public IPv4 address assigned to the EC2 instance	✓	✓
aws_ instance_ state	Current state of the EC2 instance	✓	✓
aws_subnet_ id	ID of the subnet in which the EC2 instance is running	✓	✓
aws_vpc_id	ID of the VPC in which the EC2 instance is running	✓	✓
aws_iam_	Amazon Resource Name (ARN) of the IAM instance profile	✓	✓

instance_ profile_arn			
aws_iam_ instance_ profile_id	ID of the IAM instance profile	✓	✓
aws_ security_ group_name	Security group name assigned for the EC2 instance	✓	✓
aws_ security_ group_id	Security group ID assigned for the EC2 instance	✓	✓
aws_ network_if_id	ID of the network interface	✓	✓
aws_ network_if_ attach_id	ID of the network interface attachment	✓	✓
aws_tags	Tags assigned to the EC2 instance in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
aws_flat_tags	Tags assigned to the EC2 instance extracted to top level keys and values	✓	✓
aws_owner_ id	ID of the AWS account that created the network interface	✓	✓
workload_ platform	Platform Name - AWS	✓	✓

Azure

Attribute	Description	Source	Destination
azure_ subscription_id	Subscription ID of the Azure account that created the VM	✓	✓
azure_ resource_ group	Resource Group of the VM	✓	✓
azure_vm_id	Complete path of the Azure VM. This includes subscription	✓	✓
azure_ instance_id	Instance ID of the Azure VM	✓	✓
azure_ instance_type	Instance type of the Azure VM	✓	✓
azure_ availability_ zone	Availability zone of the Azure VM	✓	✓
azure_image_ id	Image ID of the Azure VM	✓	✓
azure_private_	Private DNS name assigned to the VM instance	✓	✓

dns_name			
azure_private_ip	Private IP address assigned to the VM instance	✓	✓
azure_public_dns_name	Public DNS name assigned to the VM instance	✓	✓
azure_public_ip	Public IP address assigned to the VM instance	✓	✓
azure_instance_state	Current state of the VM instance	✓	✓
azure_subnet_id	Subnet ID of the VM instance	✓	✓
azure_vnet_id	ID of the VNET in which the VM instance is running	✓	✓
azure_network_if_id	ID of the network interface	✓	✓
azure_network_if_attach_id	ID of the network interface attachment	✓	✓
azure_tags	Tags assigned to the VM instance in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
azure_flat_tags	Tags assigned to the VM instance extracted to top level keys and values	✓	✓
azure_owner_id	Owner of the VM instance	✓	✓
azure_location	Resource Location	✓	✓
azure_scaleset_name	Scale set name	✓	✓
azure_scaleset_mode	Scale set orchestration mode	✓	✓
workload_platform	Platform Name - Azure	✓	✓

VMware vCenter

Attribute	Description	Source	Destination
vmware_vm_name	Name of the guest VM	✓	✓
vmware_vm_network	Network name of the guest VM	✓	✓
vmware_vm_status	Current status of the guest VM	✓	✓
vmware_vm_tags	Tags assigned to the guest VM in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
vmware_vm_flat_tags	Tags assigned to the guest VM extracted to top level keys and values	✓	✓

vmware_vm_os_family_name	OS type of the guest VM (eg: Linux)	✓	✓
vmware_vm_os_distro_name	OS distribution name of the guest VM	✓	✓
vmware_vm_os_distro_version	OS distribution version of the guest VM	✓	✓
vmware_vm_os_distro_pretty_name	OS distribution pretty name of the guest VM	✓	✓
vmware_vm_dns_host_name	Host DNS name of the guest VM	✓	✓
vmware_vm_dns_host_domain_name	Host DNS domain name of the guest VM	✓	✓
vmware_host_name	Host name of the guest VM	✓	✓
vmware_host_ip	Host IP address of the guest VM	✓	✓
vmware_datacenter_name	Datacenter name of the guest VM	✓	✓
vmware_cluster_name	Cluster name of the guest VM	✓	✓
vmware_vcenter_name	vCenter name of the guest VM	✓	✓
workload_platform	Platform Name - VMware	✓	✓

Kubernetes

Attribute	Description	Source	Destination
k8s_cluster_name	Name identifying the Kubernetes cluster	✓	✗
k8s_cluster_version	Version of Kubernetes running on the cluster	✓	✗
k8s_cluster_status	Operational state of the Kubernetes cluster	✓	✗
k8s_node_name	Identifier for the node within the cluster	✓	✗
k8s_node_internal_ip	Internal IP address assigned to the node	✓	✗
k8s_node_external_ip	External IP address of the node	✓	✗
k8s_node_os_version	Operating system version installed on the node	✓	✗
k8s_node_os_image	Name of the OS image used by the node	✓	✗
k8s_node_kernel_version	Kernel version of the node	✓	✗
k8s_node_cri_version	Version of the container runtime interface used on the node	✓	✗
k8s_node_status	Health and availability status of the node	✓	✗

k8s_node_labels	Node labels parsed into key-value pairs for metadata enrichment	✓	✗
k8s_pod_name	Name assigned to the Kubernetes pod	✓	✗
k8s_pod_labels	Pod labels parsed into key-value pairs for metadata enrichment	✓	✗
k8s_pod_namespace	Namespace in which the pod is deployed	✓	✗
k8s_pod_status	Operational state of the pod	✓	✗
k8s_pod_ip	IP address assigned to the pod	✓	✗
k8s_service_name	Name of the Kubernetes service	✓	✗
k8s_service_type	Type of service	✓	✗
k8s_container_name	Name of the container running inside the pod	✓	✗
k8s_container_image	Image used to create the container	✓	✗
k8s_container_port	Container port details	✓	✗
k8s_cluster_name	Name identifying the Kubernetes cluster	✗	✓
k8s_cluster_version	Version of Kubernetes running on the cluster	✗	✓
k8s_cluster_status	Operational state of the Kubernetes cluster	✗	✓
k8s_node_name	Identifier for the node within the cluster	✗	✓
k8s_node_internal_ip	Internal IP address assigned to the node	✗	✓
k8s_node_external_ip	External IP address of the node	✗	✓
k8s_node_os_version	Operating system version installed on the node	✗	✓
k8s_node_os_image	Name of the OS image used by the node	✗	✓
k8s_node_kernel_version	Kernel version of the node's operating system	✗	✓
k8s_node_cri_version	Version of the container runtime interface used on the node	✗	✓
k8s_node_status	Health and availability status of the node	✗	✓
k8s_node_labels	Node labels parsed into key-value pairs for metadata enrichment	✗	✓
k8s_pod_name	Name assigned to the Kubernetes pod	✗	✓
k8s_pod_labels	Pod labels parsed into key-value pairs for metadata enrichment	✗	✓

k8s_pod_namespace	Namespace in which the pod is deployed	✗	✓
k8s_pod_status	Operational state of the pod	✗	✓
k8s_pod_ip	IP address assigned to the pod	✗	✓
k8s_service_name	Name of the Kubernetes service	✗	✓
k8s_service_type	Type of service	✗	✓
k8s_container_name	Name of the container running inside the pod	✗	✓
k8s_container_image	Docker image used to create the container	✗	✓
k8s_container_port	Container port details	✗	✓

Supported Element Types for NetFlow Integrator Element Mapping

This section outlines the element types (v5, v9, and v10) supported by the AMX application for element mapping from the ingest NetFlow/IPFIX flow records to JSON on the following platforms. These elements are predefined and cannot be configured:

- VMware ESXi
- VMware NSX-T

Elements	Description	Supported for NetFlow v5	Supported for NetFlow v9	Supported for NetFlow v10/IPFIX
type	Type of flow message	✓	✓	✓
sampler_address	Address of the device that generated the packet	✓	✓	✓
sampling_rate	Sampling rate of the flow	✓	✓	✓
export_time_ns	Export time in Nano seconds	✓	✓	✓
time_received_ns	Timestamp in nanoseconds of when the message was received	✓	✓	✓
sequence_num	Sequence number of the flow packet	✓	✓	✓
source_id	An identifier that uniquely identifies the flow source. For IPFIX it refers to the observation domain ID.	✗	✓	✓
etype	Ethernet type (0x86dd for IPv6...)	✓	✓	✓
src_addr	Source address (IP) • NetFlow v5 - IPv4 only • NetFlow v9 - IPV4_SRC_ADDR(8), IPV6_SRC_ADDR(27)	✓	✓	✓

[1]The numbers within the enclosed brackets represent the element ID in IPFIX/NetFlow v10 and the field type ID in NetFlow v9.

	• NetFlow v10/IPFIX - sourceIPv4Address(8), sourceIPv6Address(27)			
dst_addr	Destination address (IP) • NetFlow v5 - IPv4 only • NetFlow v9 - IPV4_DST_ADDR (12), IPV6_ DST_ADDR (28) • NetFlow v10/IPFIX - destinationIPv4Address(12), destinationIPv6Address(28)	✓	✓	✓
ip_tos	IP Type of Service • NetFlow v5 – tos • NetFlow v9 - SRC_TOS (5) • NetFlow v10/IPFIX - ipClassOfService (5)	✓	✓	✓
ip_dscp	Differentiated Services Code Point • ipDiffServCodePoint (195)	✗	✓	✓
ip_ precedence	The value of the IP Precedence • ipPrecedence (196)	✗	✓	✓
proto	Protocol (UDP, TCP, ICMP...) • NetFlow v5 – proto • NetFlow v9 - PROTOCOL (4) • NetFlow v10/IPFIX - protocolIdentifier (4)	✓	✓	✓
ip_ttl_max	Maximum TTL value observed for packets of the flow • NetFlow v9 - MAX_TTL (53) • NetFlow v10/IPFIX - maximumTTL (53)	✗	✓	✓
src_port	Source port (when UDP/TCP/SCTP) • NetFlow v5 – srcport • NetFlow v9 - L4_SRC_PORT (7) • NetFlow v10/IPFIX - sourceTransportPort (7)	✓	✓	✓
dst_port	Destination port (when UDP/TCP/SCTP) • NetFlow v5 – dstport • NetFlow v9 - L4_DST_PORT (11) • NetFlow v10/IPFIX - destinationTransportPort (11)	✓	✓	✓
bytes	Number of bytes in a flow • NetFlow v5 – dOctets • NetFlow v9 - IN_BYTES (1), OUT_BYTES (23) • NetFlow v10/IPFIX - octetDeltaCount (1), postOctetDeltaCount (23)	✓	✓	✓
packets	Number of packets in a flow • NetFlow v5 – dPkts • NetFlow v9 - IN_PKTS (2), OUT_PKTS (24)	✓	✓	✓

	• NetFlow v10/IPFIX - packetDeltaCount (2), postPacketDeltaCount (24)			
bytes_total	Running byte counter for a permanent flow • NetFlow v9 - IN_PERMANENT_BYTES (85) • NetFlow v10/IPFIX - octetTotalCount(85)	✖	✓	✓
packets_total	Running packet counter for a permanent flow • NetFlow v9 - IN_PERMANENT_PKTS (86) • NetFlow v10/IPFIX - packetTotalCount(86)	✖	✓	✓
flow_ direction	Flow direction • NetFlow v9 - DIRECTION (61) • NetFlow v10/IPFIX - flowDirection(61)	✖	✓	✓
in_if	Input interface • NetFlow v5 – input • NetFlow v9 - INPUT_SNMP (10) • NetFlow v10/IPFIX - ingressInterface (10)	✓	✓	✓
out_if	Output interface • NetFlow v5 – output • NetFlow v9 - OUTPUT_SNMP (14) • NetFlow v10/IPFIX - egressInterface (14)	✓	✓	✓
time_flow_ start_ns	Time the flow started in nanoseconds. Refer to Important Notes. • NetFlow v5 – System uptime and first • NetFlow v9 - System uptime and FIRST_ SWITCHED (22) • NetFlow v10 - flowStartXXX (150, 152, 154, 156)	✓	✓	✓
time_flow_ end_ns	Time the flow ended in nanoseconds. Refer to Important Notes. • NetFlow v5 – System uptime and last • NetFlow v9 - System uptime and LAST_ SWITCHED (21) • NetFlow v10/IPFIX - flowEndXXX (151, 153, 155, 157)	✓	✓	✓
tcp_flags	TCP flags • NetFlow v5 – tcp_flags • NetFlow v9 - TCP_FLAGS (6) • NetFlow v10/IPFIX - tcpControlBits (6)	✓	✓	✓
ip_length_ min	Minimum IP packet length • NetFlow v9 - MIN_PKT_LNGTH (25) • NetFlow v10/IPFIX - minimumIpTotalLength (25)	✖	✓	✓
ip_length_ max	Maximum IP packet length • NetFlow v9 - MAX_PKT_LNGTH (26)	✖	✓	✓

	• NetFlow v10/IPFIX - maximumIpTotalLength (26)			
next_hop	Nexthop IP address • NetFlow v5 – nexthop • NetFlow v9 - IPV4_NEXT_HOP (15), IPV6_NEXT_HOP (62) • NetFlow v10/IPFIX - ipNextHopIPv4Address (15), ipNextHopIPv6Address (62)	✓	✓	✓
ipv4_next_hop	Nexthop IPv4 address • NetFlow v9 - IPV4_NEXT_HOP (15) • NetFlow v10/IPFIX - ipNextHopIPv4Address (15)	✗	✓	✓
ipv6_next_hop	Nexthop IPv6 address • NetFlow v9 - IPV6_NEXT_HOP (62) • NetFlow v10/IPFIX - ipNextHopIPv6Address (62)	✗	✓	✓
flow_id	An identifier of a flow that is unique within an Observation Domain • NetFlow v9 - flowId (148) • NetFlow v10/IPFIX - flowId (148)	✗	✓	✓
firewall_event	Indicates a firewall event. Allowed values are listed in the firewall Event registry. • firewallEvent(233)	✗	✓	✓
icmp_type	Type of the ICMP message • NetFlow v9 - ICMP_TYPE (32) • NetFlow v10/IPFIX - icmpTypeXXX (176, 178), icmpTypeCodeXXX (32, 139)	✗	✓	✓
icmp_code	Code of the ICMP message • NetFlow v9 - ICMP_TYPE (32) • NetFlow v10/IPFIX - icmpCodeXXX (177, 179) icmpTypeCodeXXX (32, 139)	✗	✓	✓
flow_end_reason	The reason for flow termination. Values are listed in the flowEndReason registry.	✗	✓	✓
application_id	Specifies an Application ID • NetFlow v9 - APPLICATION TAG (95) • NetFlow v10/IPFIX - applicationId (95)	✗	✓	✓
application_description	Specifies the description of an application • NetFlow v9 - APPLICATION DESCRIPTION (94) • NetFlow v10/IPFIX - applicationDescription (94)	✗	✓	✓

application_name	Specifies the name of an application • NetFlow v9 - APPLICATION NAME (96) • NetFlow v10/IPFIX - applicationName (96)	✖	✓	✓
tcp_window_size	The window field in the TCP header • tcpWindowsSize (186)	✖	✓	✓
viptela_vpn_id	Private enterprise number for vIPtela Inc. (41916)	✖	✖	✓

Important Notes

- **NetFlow v9 and v5 Timestamps**:
  - The NetFlow header contains system uptime (in seconds) and an export timestamp.
  - Flow start time is derived using the following formula:
    - Flow_Start = Export Timestamp - System Uptime + First_Switched
  - Flow end time is derived using the following formula:
    - Flow_End = Export Timestamp - System Uptime + Last_Switched
  - The calculated start and end time are converted into nanoseconds.
  - Unsupported attributes such as flow start/end in milliseconds, microseconds, or nanoseconds will be ignored. Instead, the export timestamp is used as both the flow start and end times, which are then converted to nanoseconds.
- **NetFlow v10/IPFIX Timestamps**:
  - NetFlow v10/IPFIX directly incorporates timestamps without the need for system uptime.
  - Even if Flow start and end timestamps are available in seconds, milliseconds, microseconds, or nanoseconds, they are always converted to nanoseconds for output.
- **Missing Flow Start/End Attributes** - For records that do not include flow start or end attributes, AMX automatically assigns both values to the export timestamp.

The image below explains how flow start and end times are calculated using system uptime, export timestamp and flow switch times.

```
        Boot - Device boot , uptime init
        FS - First Packet for the flow switched
        LS -  Last Packet for the flow switched
        Export - When the flow is exported
        EXP_TS  -  abs ts at export [present in netflow v9 header]
        UPTIME  - Time since this device is booted [present in netflow v9 header]
        FIRST_SWITCHED - System uptime at which the first packet of this flow was switched
        LAST_SWITCHED - System uptime at which the last packet of this flow was switched



       epoc                          EXP_TS
        |<-------------------------------------------------------------------------->
TIMELINE|_________________|[Boot]_____________|[FS]_____________|[LS]__________|[Export]_____________
        |                 <------------------------------------------------------------>
        |                                        UPTIME
        |                 <-------------------->
                           FIRST_SWITCHED
                          <---------------------------------------->
                                      LAST_SWITCHED


        Flow_Start = EXP_TS - UPTIME + FIRST_SWITCHED
        Flow_End   = EXP_TS - UPTIME + LAST_SWITCHED
```

GigaSMART NetFlow Generation

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

Refer to the following topics for step-by-step instructions on how to configure NetFlow:

- Configure Application Metadata Intelligence for Virtual Environment- For SecureVUE Plus Base Bundle
- Create NetFlow Session for Virtual Environment - For NetVUE Base Bundle

Create NetFlow Session for Virtual Environment

NOTE: This configuration is applicable only when using NetVUE Base Bundle.

To create an NetFlow session, follow these steps:

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

view appears.

3. In the Application quick view, enter or select the following details in the **General** tab:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter a name for the application.</td></tr>
<tr><td>Description</td><td>Enter the description.</td></tr>
<tr><td colspan="2">Application Metadata Settings</td></tr>
<tr><td>Flow Direction</td><td>Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.</td></tr>
<tr><td>Timeout</td><td>Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.</td></tr>
<tr><td>Data Link</td><td>If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the Data Link and enable the VLAN option.</td></tr>
<tr><td>Observation ID</td><td>Enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is 00 01 02 05, and in Decimal is 66053.</td></tr>
<tr><td colspan="2">Advanced Settings</td></tr>
<tr><td>Number of Flows</td><td>The number of flows supported by the application.
Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.
<table>
<tr><th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr>
<tr><td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
<tr><td>AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr>
<tr><td></td><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr>
<tr><td>Azure</td><td>Large (Standard_D8s_V4)</td><td>500k</td></tr>
<tr><td></td><td>Medium (Standard_D4s_v4)</td><td>100k</td></tr>
<tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</table>

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..
If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.
</td></tr>
</table>

NOTE: When using NetVUE Base Bundle, Multi-Collect, Fast Mode, and Aggregate round-trip time fields are disabled.

4. In the Application quick view, enter or select the following details in the **Exporters** tab:

Parameter	Description
Exporter Name	Enter a name for the Exporter.
Actions	Using this option, you can perform the following functions: • **Add Exporter** - Use to add a new Exporter to this Application Metadata Intelligence Application • **Apply Template** - Use to select the tool template.Refer to *Tool Templates*section in GigaVUE Fabric Management Guide for more details on what are tool templates and to create custom tool templates. • **Save as New Template** - Use to save the current configuration as a new custom tool template. • **Delete this Exporter** - Use to delete the Exporter.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow
NetFlow: Select this option to use NetFlow	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
APPLICATION & ATTRIBUTES: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application. (Not applicable when using Netflow V5, V9, Netflow IPFIX(V10), or CEF when the flow direction is Uni-Directional in the above **Template** drop-down menu.)	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select a Type. The available options are: • **Application Family:** Each application is mapped only mapped to one Application Family ▪ Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the **Attribute** column. You can select the required attributes. • **Application Tag:** Each application can be mapped to one or more Application Tags. ▪ Select an **Application Tag** and the **Applications** that needs

Parameter	Description
	to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the **Attribute** column. You can select the required attributes.
NETWORK & TRANSPORT PARAMETERS: Select the Network and the transport packet attributes with the respective parameters	
Data Link	Select any one of the parameters such as Source MAC Address, Destination MAC Address and VLAN.
Interface	Select any one of the parameter such as Input Physical, Output Physical and Input Name.
IP	Select the parameter as Version if required.
IPv4	Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
IPv6	Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
Transport	Select the required attributes. By default, Source Port, Destination Port are enabled.
Counter	Select the Bytes, and Packets.
Timestamp	Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
Flow	Select the parameter as End Reason if required.
GTP-U	Select the required parameters such as QFI and TEID.
Outer IPv4	Select any one of the parameter such as Source or Destination.
Outer IPv6	Select any one of the parameter such as Source or Destination.

5. Click **Save**.

Examples- Configuring Application Intelligence Solution with Other Applications

This sections provides information on how applications like Application Filtering Intelligence, Application Metadata Intelligence and Application Metadata Exporter can be used with other applications in the monitoring session.

Refer to the following topics for more detailed information:

- Slicing and Masking with Application Filtering Intelligence
- De-duplication with Application Metadata Intelligence

Slicing and Masking with Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. You can use the Slicing and Masking application along with Application Filtering application slice, mask, or slice and mask the filtered packets before sending them to the destination tunnel endpoint.

NOTE: When combining Slicing and Masking operations, the offset range of the Masking must be lesser than the offset value entered for the Slicing operation, as the Slicing operation is performed first.

Follow the steps below to configure Application Filtering Intelligence with Masking and Slicing:

1. Drag and drop **New Map / Application Filtering** from **New** to the graphical workspace.
2. Click the map and select **Details**. The Application quick view appears.
3. Configure Application Filtering Intelligence using the steps given inConfigure Application Filtering Intelligence for Virtual Environment
4. Drag and drop **Slicing** from **Applications** to the graphical workspace.
5. Click the application and select **Details**. The Application quick view appears.
6. Configure Slicing application using the steps given in Slicing
7. Drag and drop **Masking** from **Applications** to the graphical workspace.
8. Click the application and select **Details**. The Application quick view appears.
9. Configure Masking application using the steps given in Masking.
10. Drag and drop **New Tunnel** from **New** to the graphical workspace.
11. Click the tunnel and select **Details**. The Application quick view appears.
12. Select the **Type** as L2GRE/VXLAN. Select the Traffic Direction as **Out**. Refer to Create Ingress and Egress Tunnel section in the respective Cloud Deployment guides for step-by-step instructions on how to configure Tunnels.
13. Enter Source L4 Port and Destination L4 Port.
14. After placing the required items in the canvas, hover your mouse on the applications, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

The filtered traffic will be sent to the Slicing application, the sliced traffic will be sent to Masking application and then to the destination tunnel Endpoint.

De-duplication with Application Metadata Intelligence

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output. Using de-duplication with Application Metadata Intelligence lets you eliminate the duplicate packets in the Application Metadata

output, only forwarding a packet once and thus reducing the processing load on your tools.

Follow the steps below to configure Application Metadata Intelligence with De-duplication:

1. Drag and drop **Application Metadata** from **Applications** to the graphical workspace.
2. Click the application and select **Details**. The Application quick view appears.
3. Configure Application Metadata Intelligence using the steps given in Configure Application Metadata Intelligence for Virtual Environment.
4. Drag and drop **dedup** from **Applications** to the graphical workspace.
5. Click the application and select **Details**. The Application quick view appears.
6. Configure de-duplication application using the steps given in De-duplication.
7. Drag and drop **New Tunnel** from **New** to the graphical workspace.
8. Click the tunnel and select **Details**. The Application quick view appears.
9. Select the **Type** as UDP.
10. Enter Source L4 Port, Destination L4 Port, and Destination IP. Refer to Create Ingress and Egress Tunnel section in the respective Cloud Deployment guides for step-by-step instructions on how to configure Tunnels.
11. 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).

The duplicate packets are removed before sending the traffic to AMI. This will reduce the load on Application Metadata application which in turn can avoid exporting the duplicated Metadata to the tool.

De-duplication

De-duplication application targets, identifies, and eliminates duplicate packets, blocking unnecessary duplication and sending optimized flows to your security and network monitoring tools. De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment.

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output. They can also appear when packets are gathered from multiple collection points along a path. The de-duplication application lets you eliminate these packets, only forwarding a packet once and thus reducing the processing load on your tools.

Feature Overview

There are two actions that can be specified for handling the duplicate packets detected:

- drop, which drops the duplicate packets
- count, which counts the duplicate packets, but does not drop them

A time interval can be configured within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination.

For example, if two of the same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates.

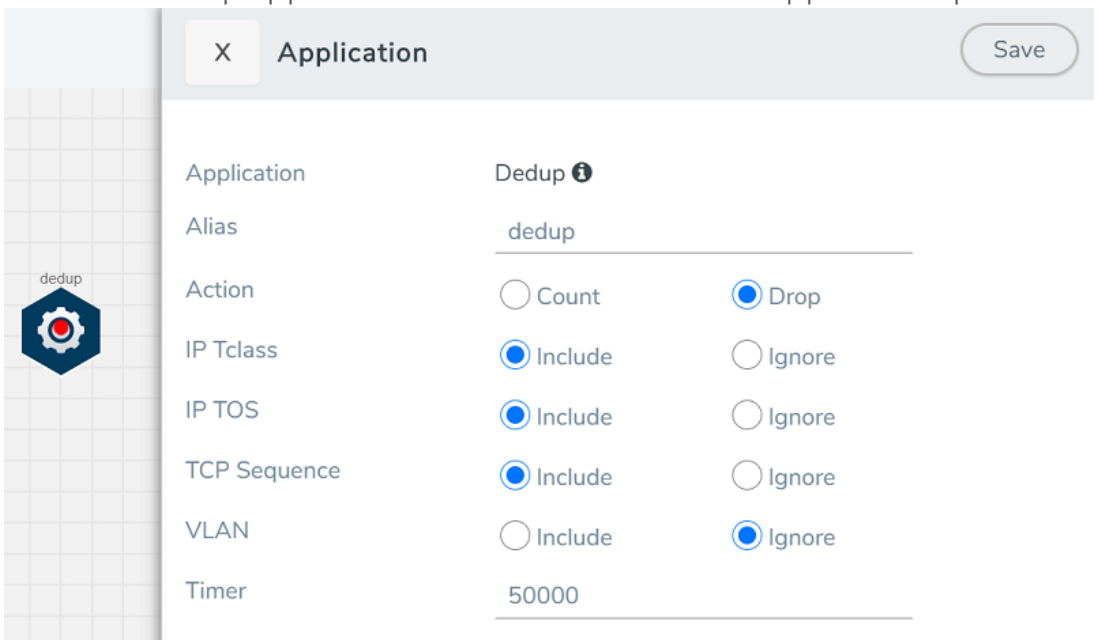
For IPv4 and IPv6 packets, to determine if a packet is considered to be a duplicate, parts of the IP headers (Layer 3 and Layer 4), as well as part of the payload are compared.

For non-IP packets, a packet is considered to be a duplicate if it is identical.

Configure De-duplication Application

To add a de-duplication application:

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



3. In the Application quick view, enter the information as follows:

Parameter	Description
Alias	Enter a name for the application.
Action	Specifies whether duplicate packets are to be counted or dropped as follows: o **Count**– The de-duplication application counts the duplicate packets, but does not drop them. o **Drop**– The de-duplication application drops the duplicate packets. The default is drop.
IP Tclass **IP TOS** **TCP Sequence** **VLAN**	These options are useful when applying de-duplication operations to packets in a NAT environment. Different NAT implementations can change certain packet header fields (for example, the TCP sequence number). If you want to be able to detect duplicates without requiring that these fields match (ToS field, TCP sequence number, VLAN ID), you can disable the corresponding option. o **IP Tclass** – Ignore or include IPv6 traffic class. Use for IPv6. The default is include. o **IP TOS** – Ignore or include the IP ToS bits when detecting duplicates. Use for IPv4. The default is include. o **TCP Sequence** – Ignore or include the TCP Sequence number when detecting duplicates. The default is include. o **VLAN** – Ignore or include the VLAN ID when detecting duplicates. The default is ignore. Include means the field will be included when the application compares packets. Ignore means the field will be ignored when the application compares packets.
Timer <Value: 10-500000 µs>	Configures the time interval within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination. The default is 50,000µs. For example, if two same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates. **NOTE:** Retransmissions are not counted as duplicates.

4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Distributed De-duplication

In distributed de-duplication, when you set up a monitoring session with a de-duplication app, the traffic is first sent to a component which distributes the traffic based on a consistent mechanism to ensure that packets from a particular traffic go to the same de-duplication instance. The packets are shared across the GigaVUE V Series Nodes. The distributed de-duplication more efficient that the existing de-duplication.

NOTE: From version 6.9, Traffic Distribution option is renamed to Distributed De-duplication.

From version 6.5, distributed de-duplication is supported on Azure, AWS, GCP, Nutanix, VMware NSX-T, VMware ESXi, and OpenStack. An enhanced configuration profile for the load balancer will be set by default with no option for modification. The default profile will use source and destination IP addresses, source and destination ports as the configuration for calculating the hash value for traffic distribution.

Important:

1. False traffic health alarms could be raised due to distribution of traffic across GigaVUE V Series Nodes.
2. Statistics are displayed for all the applications. Distributed De-duplication requires additional entities which will be listed in statistics page.

Limitation

- When using distributed de-duplication application, if **Prefer IPv6** option is enabled when configuring GigaVUE V Series Node using GigaVUE-FM, IPv6 tunnel will be created only between GigaVUE V Series Node and UCT-V and the rest of the tunnels created are IPv4 tunnels. Refer to Configure GigaVUE Fabric Components section in the respective cloud deployment guide for more detailed information on how to deploy GigaVUE V Series Node with IPv6 tunnels.

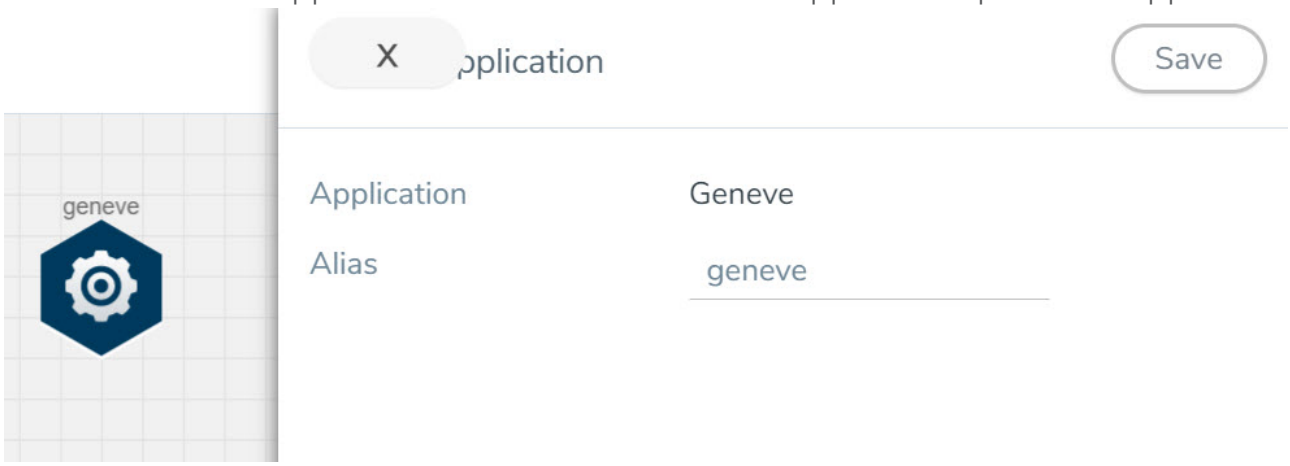
- When using distributed de-duplication application, if **Enable IPv6 Preference** option is enabled when configuring GigaVUE V Series Node using Third Party Orchestration, IPv6 tunnel will be created only between GigaVUE V Series Node and UCT-V and the rest of the tunnels created are IPv4 tunnels. Refer to *Create Monitoring Domain* section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration Guide for more detailed information on how to create a monitoring domain to register GigaVUE fabric components with IPv6 tunnels.

GENEVE Decapsulation

The GENEVE Decapsulation application is used to acquire and strip GENEVE headers. To route the traffic through the third-party network appliances seamlessly, the AWS gateway load balancer with a VPC adds GENEVE header to packets as they are forwarded to a third-party network appliance. Each appliance is expected to terminate the GENEVE tunnel and process the GENEVE encapsulated traffic traffic. When the GigaVUE-FM directs the acquisition of the customer traffic, the packets are encapsulated and forwarded as GENEVE tunnels that are terminated in GigaVUE V Series nodes.

To add a GENEVE application:

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



3. Enter an alias for the GENEVE application.
4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to *Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to *Monitor Cloud Health* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Header Stripping

Header Stripping application efficiently examines the packets for specified headers like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-tag, VXLAN, FM6000Ts, GENEVE, and generic and remove them before sending the packet to the appropriate security and analysis tools. Each packet is examined for the packet forwarding addition, and it also ensures that the headers are removed before sending the packet to the tools. This application is useful when working with tools that either cannot recognize these headers or must engage in additional processing to adjust for them.

Furthermore, the presence of protocols like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-tag, VXLAN, GENEVE, and FM6000Ts in the packet can restrict or limit the ability to apply filtering and flow-based load balancing to the traffic as it is forwarded to specific tools. To address each of these challenges, Header Stripping of these protocols is required.

List of Protocols that are supported for striping:

- GTP
- ISL
- ESPRAN
- MPLS
- MPLS+VLAN
- VLAN
- VN-tag
- VXLAN
- FM6000Ts
- GENEVE
- Generic

Note:

Header Stripping for the GENEVE protocol is currently supported for the following platforms:

- VMware vCenter
- VMware NSX-T
- Nutanix

Limitation

The GENEVE protocols currently supported for header stripping are the Transparent Ethernet Bridge (0x6558), IPv4 (0x0800), and IPv6 (0x86DD).

Configure Header Stripping Application

To configure the Header Stripping application in GigaVUE-FM, follow the steps given below:

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

3. In the application quick view, enter or select the required information as described in the following table:

Field	Description
Alias	Enter the alias name for the application.
Protocol	Select the type of protocol.
VLAN: Use this option to strip the VLAN header from the packets. You can either strip the outer VLAN header or the entire VLAN header. When choosing VLAN as your protocol for stripping, enter the following details:	
VLAN Header	The VLAN Header that should be stripped. The supported minimum value is 0, and the maximum value is 16777215. The default value is 0.
VXLAN: Use this option to strip VXLAN (Virtual eXtensible Local Area Network) headers. You can strip either matching VXLAN headers or all VXLAN headers. When choosing VXLAN as your protocol for stripping, enter the following details:	
VXLAN ID	The VXLAN ID that should be stripped. The default value is outer.
FM6000Ts: Use this option to strip FM6000Ts time stamp headers. Packets entering the application from other devices may contain FM6000 timestamps. FM6000 is an Intel chip used for time stamping. FM6000 has a hardware timestamp in the packet. When choosing FM6000Ts as your protocol for stripping, enter the following details:	
Time Stamp Format	The format of the time stamp you wish to strip. The only supported format for the time stamp is **None**.
ESPRAN: Use this option to strip ERSPAN Type II and Type III headers. When choosing ESPRAN as your protocol for stripping, enter the following details:	
ESPRAN FlowID	Specify an ERSPAN flow ID between 0 to 1023. A flow ID of zero is a wildcard value that matches all flow IDs.
GENEVE: Use this option to strip the GENEVE header from the packets. The default L4 Destination Port value is 6081. To change the default L4 destination port value, follow the steps given below: **1.** Expand the **Custom Port** section. **2.** You can either select an existing template with the port details or provide them directly in the pop-up window. o **Using Template** - If you wish to use an existing template, select the template from the **Template** drop-down menu. To create a new template, refer to Create Custom Port Template. **Note**: You cannot modify an existing template by editing the values directly in the Monitoring Session. However, you can modify the values in the Monitoring Session and save it as a new template. o **Without Template** - You can directly enter your port details in the **L4 Destination Port** field. Click the **Save as New Template** button to save this existing configuration as a template. You can view the newly created template in the **Custom Port Template** page.	

Generic: Using this option to strip any header without worrying about the header level. When choosing generic as your protocol for stripping, enter the following details:	
Ah1	The anchor header (AH1), after which the header to be stripped occurs.
Offset	Based on the selected Offset, enter the following details: • **Offset Range**: If you wish to use offset range as your offset, then enter the following details: a. Offset Range Value: Specify the offset of the header occurrence from the above anchor header. The minimum supported value is one, and the maximum supported value is 1500. b. Header Count: Specify the number of headers the application should remove from the offset. The minimum supported value is one, and the maximum is 32. c. Custom Len: The length (in bytes) of the header that should be stripped. d. Ah2: The next possible standard header that occurs immediately after the header. • **Start / End**: If you wish to use start or end as your offset, then enter the following details: a. Header Count: Specify the number of headers that the application should remove from the offset.. The minimum supported value is one, and the maximum is 32. b. Custom Len: The length (in bytes) of the header that should be stripped. The minimum supported value is one, and the maximum supported value is 1500. c. Ah2: The next possible standard header that occurs immediately after the header.

4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on traffic health monitoring and how to create a threshold template, refer to *Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to *Monitor Cloud Health* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the application statistics in the **STATISTICS** tab.

Create Custom Port Template

GigaVUE-FM enables you to specify custom L4 destination port values when using the Header Stripping application. You can create a template and utilize it to define custom port values when configuring the Header Stripping application.

To create a custom port template for the Header Stripping application:

1. Go to **Inventory > Resources > Custom Port Template**. The **Custom Port Template** page appears.
2. Click **New** to create a new template. The **New Custom Port Template** dialog box appears.
3. Enter a name for the template.
4. Enter valid port numbers between the range 1025 to 65535 in the **L4 Destination Port** field. Enter only comma separated integer values. You can provide a maximum of 10 ports. For example: 1034,1098,1039
5. Click **Save**.

You can view the created template on the **Custom Port Template** page. If a template is associated with a Monitoring Session, you can view the name of the Monitoring Session to which the template is associated in the Affected Entity column.

You can use the **Actions** buttons to perform the following:

- **Edit:** You can use this option to edit a template. If a template is associated with a Monitoring Session, editing it will be reflected in all the Monitoring Sessions associated with that template.
- **Delete:** You can use this option to delete a template. You cannot delete a template associated to a Monitoring Session.

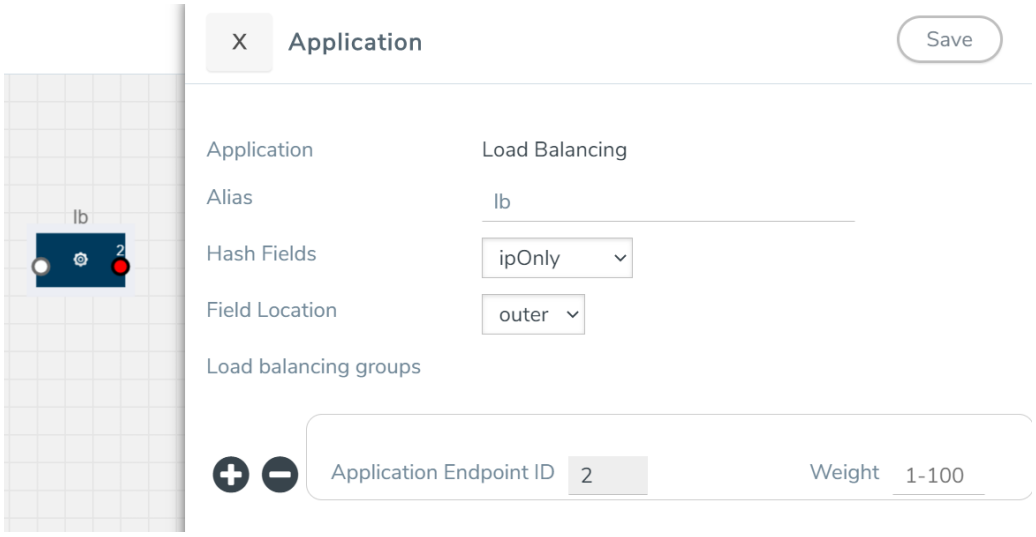
Load Balancing

Load balancing application performs stateless distribution or Enhanced Load Balacing of the packets between different endpoints. Stateless load balancing distributes the processed traffic to multiple tool ports or tunnel endpoints based on hash values generated from predefined protocol fields in the packet.

When Enhanced Load Balancing is enabled and an endpoint fails, the traffic is redistributed for the failed endpoint. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process.

To add a load balancing application:

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



3. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Stateless	Select this option to enable Stateless Load Balancing
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Hash Field	• **ipOnly** : The source IP and destination IP addresses. • **ipAndPort**: The source IP and destination IP addresses, and Layer 4 source port and destination port numbers. • **fiveTupl**e: The source IP and destination IP addresses, source port and destination port numbers, and protocol field in the IP header. • **gtpuTeid**: The GTP-u tunnel identifier (ID). **Note**: There is no inner or outer field location for `GTPU-TEID`. • **greFlowid**: The flow identifier location. **Note**: ▪ The default field location value is outer. ▪ When configuring 5G-Cloud Ericsson SCP Transparent, greFlowid hash field should be selected. Refer to 5G-Cloud Ericsson SCP Support.
Field Location	• **Outer**: The first occurrence of header or field. For example, **IP Only outer** is the first IP header in the packet, which could be IPv4 or IPv6. • **Inner**: The second occurrence of header or field. The supported IP encapsulation types are: IP-in-IP, VXLAN, GTP, GRE, and ERSPAN.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints. Endpoint with higher weight receives more traffic.

4. Click **Save**.

NOTE: When you configure the Load Balancing Application in enhanced mode, you can associate it with only a single enhanced load balancing profile. However, you have the flexibility of changing the association to different profile as needed.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer *to Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to *Monitor Cloud Health* section in the respective GigaVUE Cloud Suite deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Enhanced Load Balancing

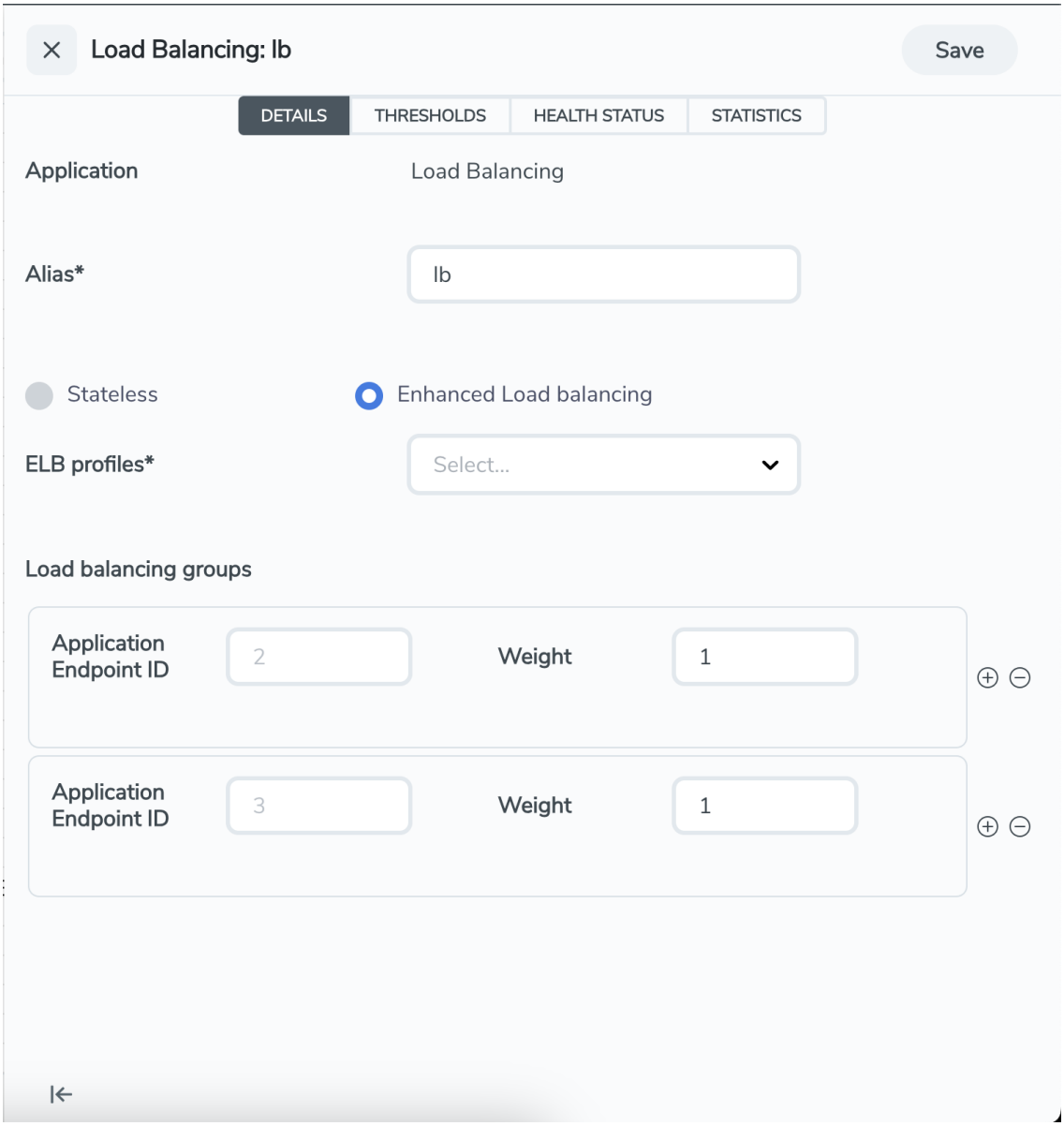
Enhanced Load Balancing redistributes the traffic from a failed endpoint to another endpoint which is a part of the ELB group. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process. Hashing is performed on the packets based on outer and/or inner headers.

To enable to enhanced load balancing application:

1. Create an Enhanced Load Balancing Profile.
   a. In the Monitoring domain page, click Settings, then click **Enhanced Load Balancing**
   b. Click **New** and then create a profile.

Fields	**Values**
Hash fields	The various hash options are ip ip-src ip-dst l4-port l4-portsrc l4-portdst gtputeid
Position	Select either inner/outer location of the hash field to be matched with the incoming packet..
Hash-mask	When the hash-fields ip-src/ip-dst are defined along with the IP, then ip-src/ip-dst hash-mask will overwrite the IP hash mask. For load balancing, you must apply this mask before hashing the IP. The default options and their default values are: IPv4 : 255.255.255.255 IPv6 :FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

2. Go to monitoring session page and
    a. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
    b. Click the load balancing application and select **Details**. The Application quick view appears.



c. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

3. Click **Save**.

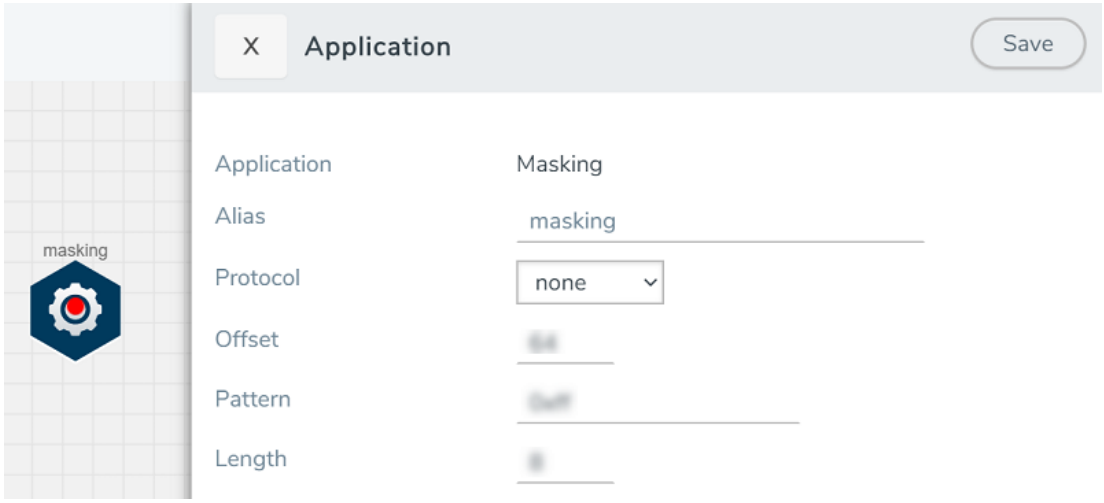
NOTE: When you configure the Load Balancing Application in enhanced mode, you can associate it with only a single enhanced load balancing profile. However, you have the flexibility of changing the association to different profile as needed.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. Masking operations consist of an **offset**, **length**, and **pattern**.

To add a Masking application:

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



3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the application.
Protocol	The following are the protocols that you can select from the protocol drop-down list: o **None** – Mask starting a specified number of bytes from the start of the packet. o **IPV4** – Mask starting a specified number of bytes after the IPv4 header. o **IPV6** – Mask starting a specified number of bytes after the IPv6 header. o **UDP** – Mask starting a specified number of bytes after the UDP header. o **TCP** – Mask starting a specified number of bytes after the TCP header. o **ftp-data**– Identify using TCP port 20. Mask payloads using offset from the TCP header. o **HTTPS** – Identify using TCP port 443. Mask payloads using offset from the TCP header. o **SSH** – Identify using TCP port 22. Mask payloads using offset from the TCP header. o **GTP** – Mask starting a specified number of bytes after the outer GTP header. o **GTP-IPV4** – Mask starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. o **GTP-UDP** – Mask starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. o **GTP-TCP** – Mask starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specifies **where** the application should start masking data with the supplied pattern. You can specify this in terms of either a static offset from the start of the packet or a relative offset from a particular protocol layer. This lets you automatically compensate for variable length headers, specifying a mask target in terms of a particular packet header.
Length	Specifies **how much** of the packet should be masked. The specified one-byte pattern can be repeated to mask from 1-9600 bytes.
Pattern	Specifies **what** pattern the application should use to mask the specified portion of the packet. You can specify a one-byte hex pattern (for example, 0xFF).

4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

SSL Decrypt

License: For information on licensing, refer to the *Volume Based License (VBL)* section of respective GigaVUE Cloud Suite Deployment Guide.

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

SSL encryption secures traffic between a client and a server, such as a Web server. SSL decryption uses keys to decode the traffic between the client and server.

SSL and Transport Layer Security (TLS) protocols consist of a set of messages exchanged between a client and server to set up and tear down the SSL connection between them. To set up the connection, the client and server use the Public Key Infrastructure (PKI) to exchange the bulk encryption keys needed for data transfer.

IMPORTANT: To use SSL Decrypt application in GigaVUE-FM 6.3.00, install new GigaVUE-FM 6.3.00 image. Refer to *GigaVUE-FM Installation and Upgrade Guide* for step-by-step instructions on how to install GigaVUE-FM. SSL Decrypt application does not work if you upgrade from any previous GigaVUE-FM version to GigaVUE-FM 6.3.00.

Keep in mind the following when using SSL Decrypt application:

1. On updating the keys, service, or key maps which are already used in a monitoring session, the monitoring session is dynamically updated, and you need not re-deploy the monitoring session. You can also see if the updated keys, services, or key maps were successfully updated to the monitoring session and the respective GigaVUE V Series Nodes on the **All Events** page. Refer to Overview of Events section in the *GigaVUE Administration Guide* for detailed information on Events.
2. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the key will be removed from the Key Map. If that key is the only available entry in the Key Map, then it will not be removed.
3. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session that is not deployed, then the key will be removed from the Key Map and if that key is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.

4. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the service will be removed from the Key Map. If that service is the only available entry in the Key Map, then it will not be removed.
5. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is not deployed, then the service will be removed from the Key Map and if that service is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.
6. In VMware NSX-T platform, the throughput of SSL Decrypt application is improved to 480 Mbps.

Refer to the following topics for more detailed information:

- Supported Protocols, Algorithms, and Ciphers for SSL Decrypt
- Configure SSL Decrypt

Supported Protocols, Algorithms, and Ciphers for SSL Decrypt

The supported protocols are as follows:

- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

The supported authentication (Au) is as follows:

- RSA

The supported key exchange (Kx) is as follows:

- RSA

The supported encryption algorithms (Enc) are as follows:

- NULL
- RC4
- DES
- 3DES
- AES (including GCM mode)
- CAMELLIA
- SEED
- IDEA

The supported compression algorithm is as follows:

- NULL

The supported digest algorithms are as follows:

- MD5
- SHA1
- SHA2

The supported key sizes are 128, 256, 512, 1024, 2048, and 4096.

The supported TLS extensions are as follows:

- Extended Master Secret, RFC 7627
- Encrypt-then-MAC, RFC 7366

The following table lists the supported ciphers:

Table 1: Supported Ciphers forSSL Decrypt

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_NULL_MD5	RSA	RSA	NULL	0	MD5
TLS_RSA_WITH_NULL_SHA	RSA	RSA	NULL	0	SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
TLS_RSA_WITH_RC4_128_MD5	RSA	RSA	RC4_128	128	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RSA	RC4_128	128	SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
TLS_RSA_WITH_IDEA_CBC_SHA	RSA	RSA	IDEA_CBC	128	SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
TLS_RSA_WITH_DES_CBC_SHA	RSA	RSA	DES_CBC	56	SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	168	SHA
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	128	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES_256_CBC	256	SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	CAMELLIA_128_CBC	128	SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	CAMELLIA_256_CBC	256	SHA
TLS_RSA_WITH_SEED_CBC_SHA	RSA	RSA	SEED_CBC	128	SHA

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_NULL_SHA256	RSA	RSA	NULL	0	SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES_128_CBC	128	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES_256_CBC	256	SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES_128_GCM	128	SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES_256_GCM	256	SHA384

All algorithms used for SSL Decrypt application are FIPS 140-3 compliant.

All key URLs must point to an RSA private key stored in the PEM or PKCS12 format, as follows:

- http://keyserver.domain.com/path/keyfile.pem
- https://keyserver.domain.com/path/keyfile.pem
- ftp://keyserver.domain.com/path/keyfile.pem
- tftp://keyserver.domain.com/path/keyfile.pem
- scp://username[:password]@keyserver.domain.com/path/keyfile.pem

The supported applications are as follows:

- HTTPS
- FTPS
- SMTP, IMAP, and POP3 with StartTLS

Configure SSL Decrypt

To configure SSL Decrypt Application using GigaVUE-FM follow the steps given below:

- Upload SSL Keys
- Create SSL Service
- Key Mapping
- SSL Key Store
- Add SSL Decrypt to Monitoring Session

Upload SSL Keys

To upload an SSL private key, do the following:

1. Go to **Inventory > Resources > Security > SSL Keys**.
2. Click **Add**. The **Create SSL Key** page appears.
3. Enter the following details:

Field	Description
Key Alias	Enter a name for the key.
Comment	Enter a description
Key Type	Select the either of the key type:
PEM	
PassPhrase (optional)	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Store in which the Key is stored.
Private key	Enter the Private Key using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
Certificate	Enter the Certificate using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
PKCS12	
PassPhrase	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Store in which the Key is stored.

4. Click **Save**.

NOTE: SSL Decrypt application does not support HSM.

The following actions can also be performed from the SSL Keys Page:

Field	Description
Edit	To edit a SSL Key, select the key from the list in the SSL Keys page and click the **Edit** button.
Delete	To delete a SSL Key, select the key from the list in the SSL Keys page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Keys in the SSL Keys page.
View certificate	To view the certificate associated with the particular SSL Key, select the key from the list in the SSL Keys page and click the **View Certificate** button.

Create SSL Service

After uploading a private key, you can add a service. A service maps to a physical server, such as an HTTP server. One server can run multiple services. A service is a combination of an IP address and a server port number.

Prerequisite

Before creating a service, upload a private key as described in Upload SSL Keys

To create a SSL service, do the following:

1. Go to **Inventory > Resources > Security > SSL Service**. The SSL Services page appears.
2. Click **Add**. The **Create SSL Service** page appears.
3. On the Create SSL Service page, enter the following details:

Field	Description
Alias	Enter a name for the SSL Service.
Default Service	Enable this to use default service.
Server IP Address	Enter the IP address of the server in which the service runs.
Server Port	Enter the port number of the server.

4. Click **Save**.

The following actions can also be performed from the SSL Service Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the **Edit** button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

Key Mapping

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

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

1. Go to **Inventory > Resources > Security > SSL Key Mapping**. The SSL Key Mapping page appears.
2. Click **Add**.

3. Enter the Key Mapping Alias.
4. Select the SSL Service and Key Alias from the drop-down.
5. Click **Save**.

The following actions can also be performed from the SSL Keys Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the **Edit** button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

SSL Key Store

SSL Key Store is a repository, that allows you to save all the key under a single location. You can create multiple key stores and in each key store you can store multiple keys.

1. Go to **Inventory > Resources > Security > SSL Key Store**. The SSL Key Store page appears.
2. Click **Add**.
3. Enter the **Key Store Alias** and **Comment**.
4. Click **Save**.

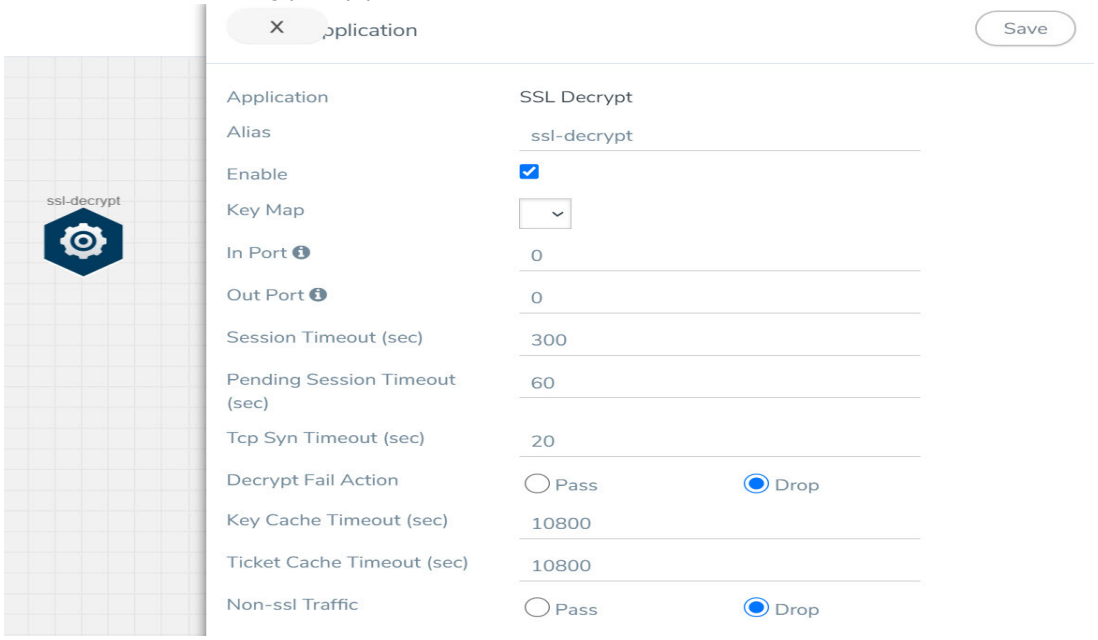
The following actions can also be performed from the SSL Key Store Page:

Field	Description
Edit	To edit a SSL Key Store, select the Key Store from the list in the SSL Key Store page and click the **Edit** button.
Delete	To delete a SSL SSL Key Store, select the SSL Key Store from the list in the SSL Key Store page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Key Store in the SSL Key Store page.

Add SSL Decrypt to Monitoring Session

After mapping your keys with service, to add GigaSMART applications to GigaVUE V Series Node, follow the steps given below,

1. Drag and drop **SSL Decrypt** from APPLICATIONS to the graphical workspace.
2. Click the SSL Decrypt application and select **Details**.



3. Enter the following details in the Application quick view:

Fields	Description
Alias	Enter the alias name for the application.
Enable	Enable the box to enable SSL Decryption.
Key Map	Select the Key Map from the list of available Key Maps. Refer to Key Mapping for more details on how to map the key to SSL Service.
In Port	Enter the source port number from which the traffic should be fetched.
Out Port	Enter the destination port number to which the decrypted traffic should be delivered.
Session Timeout	Enter the value in seconds after which the session should be timeout. The default value is 300 seconds.
Pending Session Timeout	Enter the value in seconds after which the session must timeout if the session is in pending state
Tcp Syn Timeout	Enter the value in seconds after which the session must timeout when the session does not synchronize TCP.
Decrypt Fail Action	Select **Pass** to allow the traffic to pass through the application when the decryption fails and select **Drop** to drop the traffic before passing through the application when the decryption fails.
Key Cache Timeout (sec)	Enter the value in seconds until which the key cache information can be reused for resumption.
Ticket Cache Timeout (sec)	Enter the value in seconds until which the ticket cache information can be reused for resumption.
Non-ssl Traffic	Select **Pass** to allow the non-SSL traffic to pass through the application and select **Drop** to drop the non- SSL traffic before passing through the application.

4. Click **Save**.
5. Click **Deploy**. The Select nodes to deploy the monitoring session page appears.
6. Select the GigaVUE V Series Nodes you want to deploy and select an interface for each GigaVUE V Series Node. Then, click **Deploy**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

You can view the session summary and session details of the SSL Decryption application in the **SESSIONS** tab. Select the **V Series Node IP** and enter the **Server Name**, **Client/ Server IP address**, and **Subnet Mask**. Then, click **Apply** to view the session summary and session details.

You can view the server certificate statistics in the **SERVER CERTIFICATES** tab. Select the **V Series Node IP** from the drop-down and enter the **Key Alias**. Then, click **Apply**.

All the service related details are displayed in the **SERVICES** tab. Select the **V Series Node IP** and **Service Alias** from the drop-down. Then, enter the **IP Address** and **Port**. Click **Apply**.

All the error codes and respective description are displayed in the **ERROR CODES** tab. To view the error code, select the **V Series Node IP** and **Service Alias** from the drop-down. Then, enter the **IP Address** and **Port**. Click **Apply**.

PCAPng Application

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

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

The actual packets are present in the Enhanced Packet Block. The block data is parsed to find the start and end offset of the valid packets and the packet is sent out to the next application.

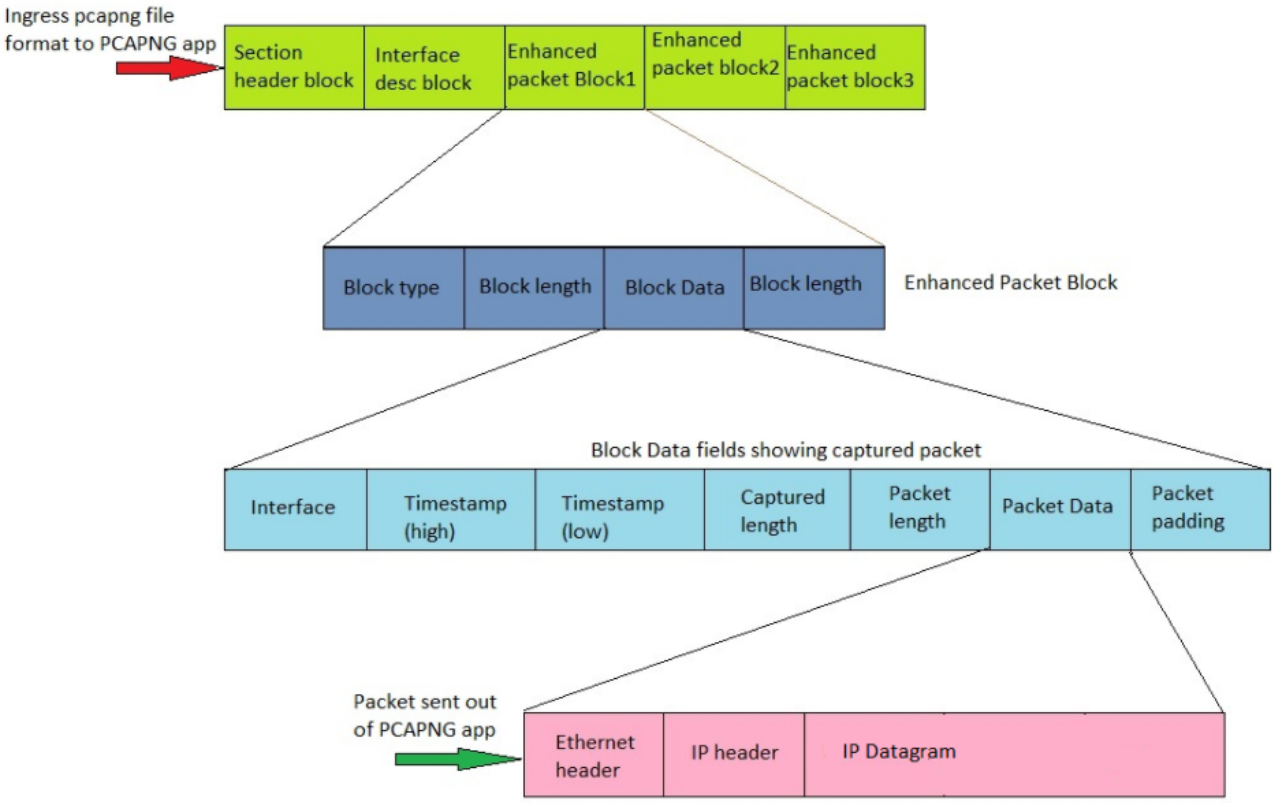
NOTE: Only one EPB in a PCAPng file is supported.

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

Block Combination	Process
SHB+IDB+EPB+data	Packets are parsed, validated, and the data packet is sent out.
SHB+IDB	Packets are dropped.
EPB+Data	Packets are parsed, validated, and the data packet is sent out.

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

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



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

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

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

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

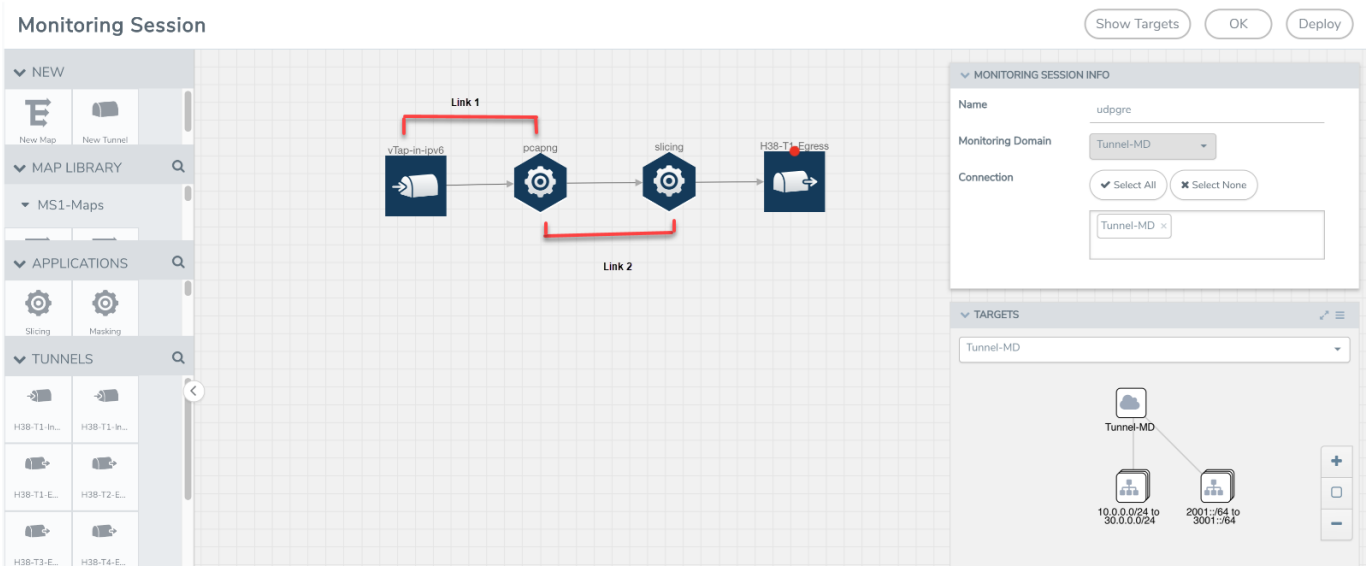
3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

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

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

Refer to the following image for a sample configuration.



What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

5G-Service Based Interface Application

5G-Core is a service-based architecture, in which many control plane network functions are available and communication across these network functions happens through HTTP2 protocol. These HTTP2 transactions are mirrored using some specific network functions, which are in JSON encoded format.

5G-Service Based Interface (SBI) Application synthesizes the HTTP2 transactions with proper L2, L3, and L4 headers from the JSON encoded data that it receives from the UDP-GRE or VXLAN ingress TEPs (Tunnel End Point). Once the headers are synthesized and a complete HTTP2 transaction is formed, the packets are sent to the egress TEP and then sent to the physical or virtual probes.

In Nokia 5G core network, the traffic is mirrored between control functions using HTTP2 protocol, which is mirrored from a service called SCP (Service Control Proxy) a centralised point through which all the communications between all the control plane functions pass. Hence, it becomes the right place to mirror the traffic.

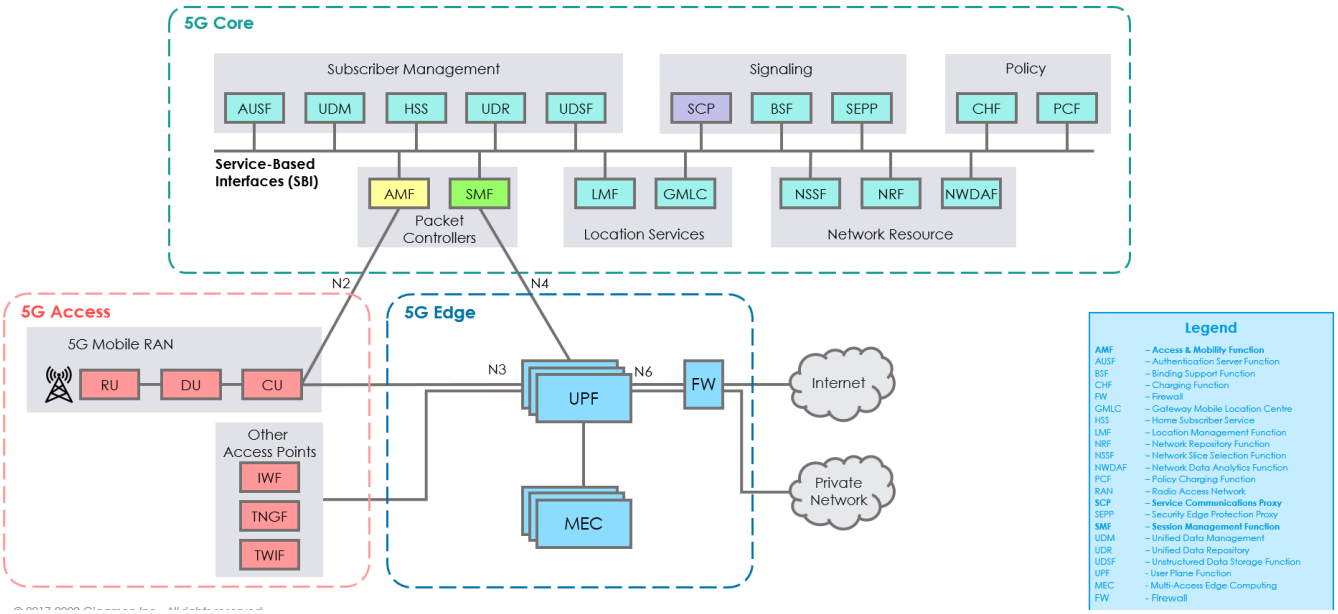
Traffic mirrored here doesn't have enough information about the entire TCP flow information between them. It only has information about request and response details between the control functions. Since the tools cannot infer much with this request and response information alone, it is required to have the entire flow information from TCP handshake to TCP connection close to form a complete TCP flow information that can be sent to the tools.

In Ericsson 5G core, there is a software probe that is used for monitoring the traffic. It captures the traffic, encapsulates it in UDP-GRE, and forwards it to V Series nodes. Here it converts the HTTP2 transactions into JSON data and a set of TCP messages are captured as PCAPng file, which is encapsulated into UDP-GRE with proto ID 0x8047 and is sent to V Series.

In either case, these are not raw packets that any tools can understand. In the case of Nokia, it doesn't have TCP session information, whereas Ericsson has the session information, but they are in a JSON encoded format. In both cases, it can't be forwarded to tools directly. Hence, we need to synthesize those packets, by adding additional information, such as TCP 3-way handshake, L2 headers and form a TCP flow information that could be forwarded to the tools.

In some versions of Nokia or Ericsson 5G Cores, the IP addresses present in the encoded message is not reliable and the SBI application converts the strings in the form of instance ID (in case of Ericsson) or producer ID (in case of Nokia) to an IP address from the string-IP mapping table.

The instance ID or producer ID must be provided in the form of CSV file. You can upload the CSV file through GigaVUE-FM.



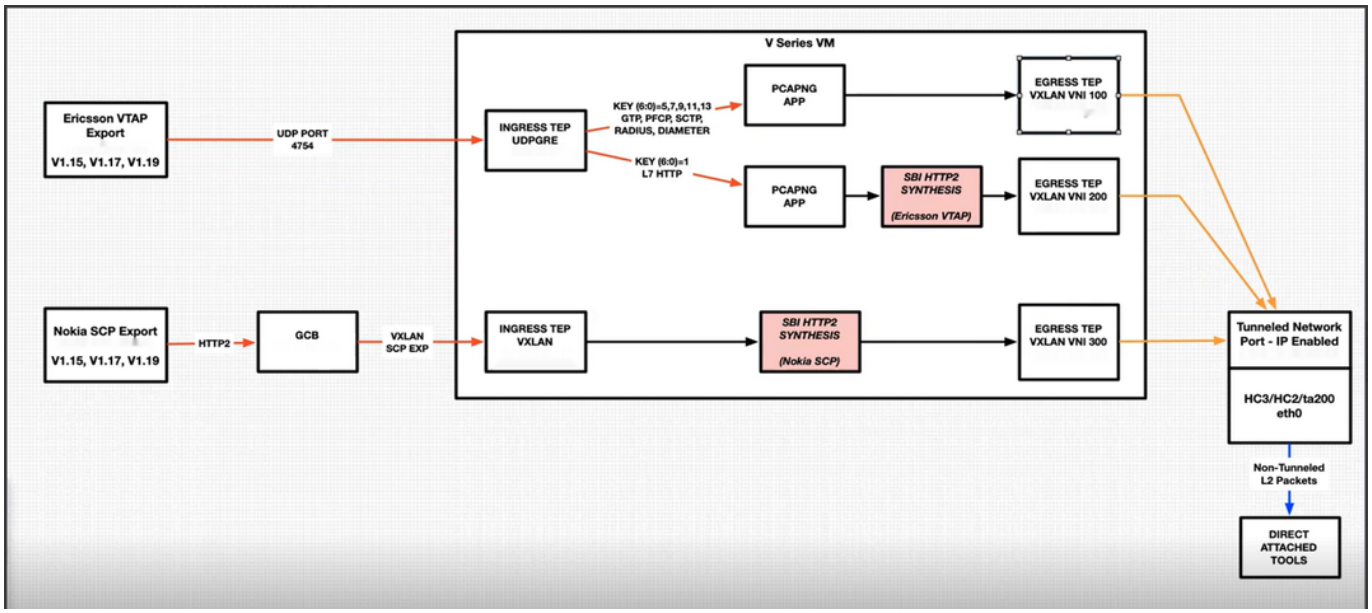
How SBI Application works

In the GigaVUE V Series Node, the SBI application receives the HTTP2 transaction messages as JSON encoded data from any of the following sources:

- VxLAN TEP – In 5G-Nokia, the application receives the JSON encoded data from the VXLAN ingress TEPs
- PCAPng application - In 5G-Ericson, the application receives the JSON encoded data from the PCAPng application, whereas the PCAPng application receives the data from the UDP-GRE TEP.

In the SBI application, JSON encoded data traffic is further parsed to extract the source-destination information and is used to synthesize the complete HTTP2 transaction with proper L2, L3, and L4 headers and HTTP2 headers and HTTP2 body of the original HTTP2 transactions. Once the headers are synthesized and a complete HTTP2 transaction is formed, the packets are then given to the egress TEP to send it to the physical/virtual probes.

The following figure shows the block diagram of the data flow in the V Series containing the SBI application.



In 5G-SBI application, the V Series node can log the following details to CSV files:

- **Transaction details** - Represents the transaction or flow of request and response packets into the application. The details of the flow or transaction are recorded in the CSV file for 5 minutes or 60 minutes based on the configuration.
- **Flow statistics details** - Represents the packet and flow statistics in 60 seconds time interval.

These files help you to understand the records or traffic efficiently. The files are named as per the date and time in which the files were created. When the number of files and its size grows, the application automatically detects the old files and delete them.

Supported Platforms:

The application is supported on the following platforms:

- VMware
- OpenStack

Rules and Notes

- The maximum number of HTTP2 headers (in the synthesized HTTP2 transactions) that is supported is 64.

- The PCAPng application that is linked to 5G-SBI application (on the right side) should only be linked to UDP-GRE TEP with key value 1 on the left side. If it is linked to other UDP-GRE TEPs(key values other than 1), then the behavior cannot be defined and leads to unexpected result.
- The maximum number of NF entries supported is 4K.

Configuration of 5G-SBI Application

In V Series, 5G-SBI application receives all the mirrored traffic from any of the following sources:

- 5G-Nokia SCP
- 5G-Ericsson

In GigaVUE-FM, the application has a field **type**, which determines whether the data is collected from 5G-Nokia or 5G-Ericsson. Based on the **type** configured, the packets received are processed.

For example, in the case of 5G-Nokia this application reads the headers (source ip/port, destination ip/port), packet type (request or response) information from the HTTP2 message. Based on the retrieved information it synthesises a TCP flow.

In the case of 5G-Ericsson, after receiving the packets from the TEP, the packets are forwarded to PCAPng application for parsing. After parsing, the JSON type data from PCAPng has the information such as source ip/port, destination ip/port, message type. Using this information HTTP2 transaction can be synthesised.

In GigaVUE-FM, to configure the 5G-SBI application refer to any of the following sections based on the source type:

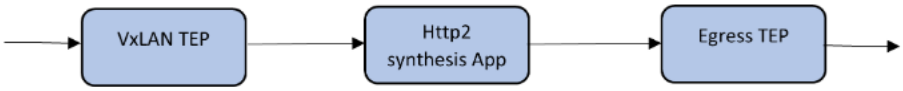
- Configuration of 5G-SBI Application for 5G-Nokia
- Configuration of 5G-SBI Application for 5G-Ericsson

Configuration of 5G-SBI Application for 5G-Nokia

In GigaVUE-FM, for 5G-Nokia, you must do the following to add the 5G-SBI application in the monitoring session of a monitoring domain in the V Series:

S.No	Steps	Refer to
1	Create VXLAN Ingress TEP to receive the HTTP2 post messages from GCB/UCT in a monitoring session.	*Create Ingress and Egress Tunnel* section in GigaVUE Cloud Suite Deployment

		Guide - VMware (ESXi) and GigaVUE Cloud Suite Deployment Guide - OpenStack Guides.
2	Add 5G-SBI Application (HTTP2 header synthesis) in the monitoring session.	Configuration of 5G-SBI Application for 5G-Nokia
3	Create a link between VXLAN ingress TEP and 5G-SBI Application in the Monitoring Session.	
4	Create egress TEP.	*Create Ingress and Egress Tunnel* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) and GigaVUE Cloud Suite Deployment Guide - OpenStack Guides.
5	Create a link between 5G-SBI Application (HTTP2 header synthesis) and Egress TEP in the Monitoring Session.	



Adding 5G-SBI Application in 5G-Nokia

Prerequisites

The pre-requisite to add a 5G-SBI application in 5G-Nokia is:

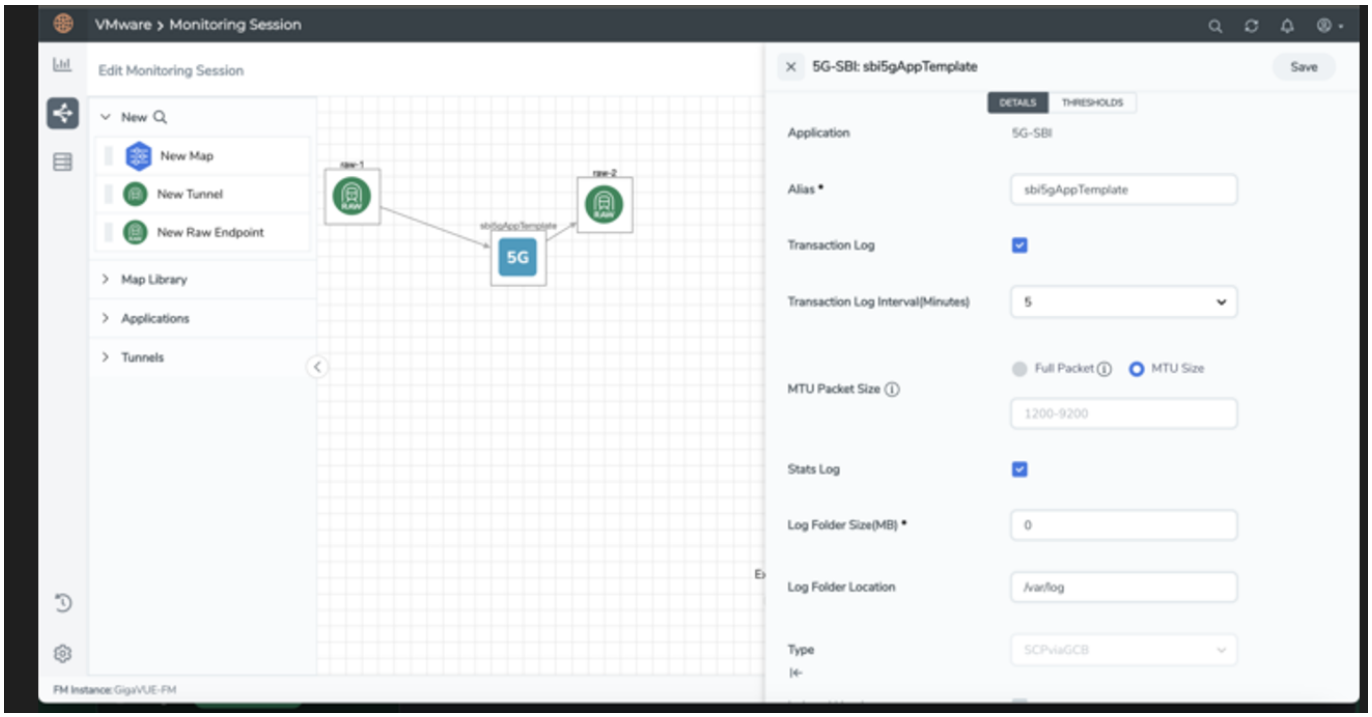
- You must upload CSV file containing a valid FQDN name and a valid IPv4/IPv6 address. To upload the CSV file, refer toAdding CSV file for IP Mapping

You can add a 5G-SBI application for:

- New monitoring session - You can add the 5G-SBI application after creating a new monitoring session and when the canvas appears.
- Existing session - Click **Edit** on existing monitoring session, the GigaVUE-FM canvas appears.

To add a 5G-SBI application:

1. In the canvas, Drag and drop 5G-SBI application and select **Details**. The Application quick view appears.
2. On the Application quick view, enter or select the required information as described in the following table:



Field	Description
Application	The name **5g-sbi** appears by default.
Alias	The name **sbi5gAppTemplate** appears by default.
Transaction log	Enable the check box to collect the log of transaction or flow of request and response packets into the application. **Note**: The transaction log cannot be enabled when the numTCPflows and numStreamsPerFlow parameters are configured with maximum values.
Transaction log interval	Specify the time to collect the transaction log. You can collect the transaction log for 5 minutes or 60 minutes.
MTU Packet Size	The MTU packet size range is 1200 to 9200 bytes. You can select the **MTU Size** option and specify a value between 1200 to 9200 bytes.
Stats log	Enable the check box to collect packet and flow statistics.
Log Folder Size	Specify the folder size to save the CSV files.
Log Folder Location	Specify the location of the folder in which the CSV files are saved.
Type	Select the option **SCPviaGCB**from the drop-down list.
Indexed Headers	Enable the check box to index the headers.

Compressed Headers	Enable the check box to compress the headers.
Ip Mapping	Select the required CSV file from the drop-down list with FQDN name. Refer to Adding CSV file for IP Mapping to get the required CSV file in the drop-down list. In case of inadequate information (i.e., NF lookup failure), the appropriate counter is incremented and the synthesized packet is sent out with inappropriate IP address.
Mode	Nokia SCP is selected by default
Number of SCP Flows	Specify the range of SCP flow (The request ID and producer ID forms a SCP flow). The minimum value is 128. The maximum value is 16000. The default value is 2000.
Request Timeout	Specify the time for the request packet to wait for the response packet in the flow. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Response Timeout	Specify the time for the response packet to wait for the request packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 2 seconds. **Note**: When you receive a message indicating that an HTTP2 Response for a HTTP2 Stream ID is indicated and you do not receive a HTTP2 Request for the same HTTP2 Stream ID within the Response Timeout timer value, the Stream gets timed out and the ResponseTimedOut error counter gets incremented. Currently the RequestTimedOut error counter gets incremented erroneously.
Nokia Use 3Gpp Target API Root	When detecting Producer IP/FQDN, treat the 3GPP Target API Root to be predictive of the Producer IP if the value is non-zero. The default value is 1.
Thresholds	Specify the threshold value to configure the packet-drop settings.
Threshold Templates	Select the threshold template.
Time Interval	Select the time interval in seconds.

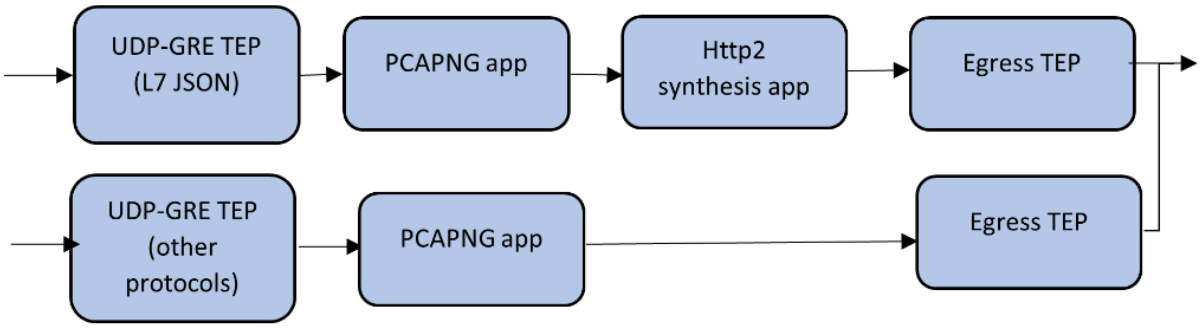
Rules and Notes

- The following configuration parameters are non-editable and it can be configured only during the initial configuration:
  - type
  - mode
  - eevtapVersion
  - numTCPFlows
  - numStreamsPerFlow
  - numSCPFlows

Configuration of 5G-SBI Application for 5G-Ericsson

In GigaVUE-FM, for 5G-Ericsson, you must do the following to configure the 5G-SBI application in the monitoring session of a monitoring domain in the V Series:

S.No	Steps	Refer to
1	Configure UDP-GRE Ingress TEP to receive the HTTP2/L7-JSON messages.	Create Ingress and Egress Tunnel - VMware Create Ingress and Egress Tunnels - OpenStack
2	Configure multiple other TEPs for other control protocol PDUs.	N/A
3	Configure two instances of PCAPng application and link ingress TEPs and PCAPng application instances in the Monitoring Session.	PCAPng Application
4	Add 5G-SBI Application (HTTP2 header synthesis) in the monitoring session.	Adding 5G-SBI Application in 5G-Ericsson
5	Create a link between TEP and 5G-SBI Application.	N/A
6	Create egress TEP.	Create Ingress and Egress Tunnel - VMware Create Ingress and Egress Tunnels - OpenStack
7	Create a link between PCAPng and egress TEPs or SBI and egress TEPs in the Monitoring Session.	N/A



Adding 5G-SBI Application in 5G-Ericsson

Prerequisites

The pre-requisite to add a 5G-SBI application in Ericsson is:

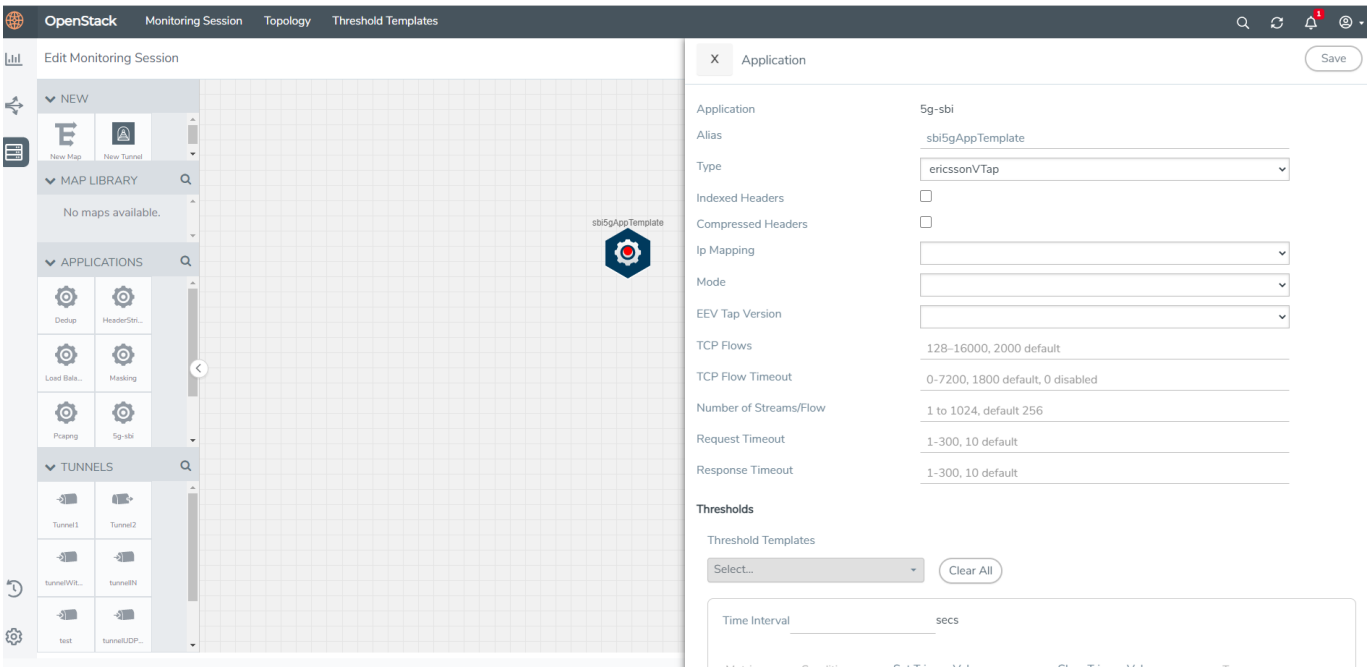
- ▪ You must upload a CSV file containing a valid Network Function Instance ID (NFID) and a valid IPv4/IPv6 address. To upload the CSV file.

You can add a 5G-SBI application for:

- New monitoring session - You can add the 5G-SBI application after creating a new monitoring session and when the canvas appears.
- Existing session - Click **Edit** on existing monitoring session, the GigaVUE-FM canvas appears.

To add a 5G-SBI application:

1. In the canvas, Drag and drop 5G-SBI application and select **Details**. The Application quick view appears.



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

Field	Description
Application	The name **5g-sbi** appears by default.
Alias	The name **sbi5gAppTemplate** appears by default.
Type	Select the option **ericssonVTap**from the drop-down list.
Indexed Headers	Enable the checkbox to index the HTTP2 headers in the 5G-SBI application.
Compressed Headers	Enable the checkbox to compress the HTTP2 headers in the 5G-SBI application.
Ip Mapping	Select the required CSV file from the drop-down list with required Network Function Instance ID (NFID) instance mapping. Refer to

	Adding CSV file for IP Mapping to get the required CSV file in the drop-down list.
Mode	L7json is selected by default. L7native is not supported in 6.1
EEV Tap Version	Select 1 or 2 from the drop-down list box.
TCP Flows	Specify the concurrent TCP flow range. The minimum value is 128 seconds, and the maximum value is 16000 seconds. The default value is 1000 seconds.
TCP Flow Timeout	Specify the flow range for which the TCP flow should remain valid in the application. The minimum value is 0 and the maximum value is 7200 seconds. The default value is 1800 seconds
Number of Streams per Flow	Specify the Number of Streams per flow. The minimum value is 1. The maximum value is 1024. The default value is 256.
Request Timeout	Specify the time for the request packet to wait for the response packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Response Timeout	Specify the time for the response packet to wait for the request packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 2 seconds.
Threshold Templates	Select the threshold template.
Time Interval	Select the time interval in seconds.

Adding CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-SBI**. The Proxy Server Configuration page appears.
2. Select any of the following from the **Type** as per the requirement:
   - **SCPviaGCP** - Adding the CSV file containing a valid FQDN name and a valid IPv4/IPv6 address for IP mapping in 5G-Nokia.
   - **ericcsonVTap** - Adding the CSV file containing a valid NF-instance ID and a valid IPv4/IPv6 address for IP mapping in 5G-Ericsson.
3. Enter the name for the CSV file in the **Alias** field.
4. Click **Choose File** in **FileName** field to upload the CSV file into GigaVUE-FM.
5. Click **Save** to add the CSV file.

5G-Cloud Application

5G-Core is a service-based architecture in which many control plane network functions are available and communication across these network functions happens through HTTP2 protocol. These HTTP2 transactions are mirrored using some specific network functions, which are in JSON-encoded format.

The 5G Cloud application supports synthesizing of L2, L3, L4, and HTTP2 headers from the JSON-encoded data of the 5G core network. Currently, Ericsson VTAP 5G core input format is supported in DPDK based platforms and in non-DPDK based platforms, Casa vTAP, Oracle SCP, Nokia SCP Inbound, and Nokia SCP Inbound/Outbound input formats are supported.

In non-DPDK mode, V Series Node supports processing of the HTTP2/HTTP2S input formats and extracts the actual packet in the 5G core, and then sends it out on the egress tunnel to probe using either VXLAN or L2GRE or UDP-GRE Tunnel. To achieve this, V Series supports two new applications:

- GVHTTP2
- 5G-Cloud

Supported Platforms

The application is supported on the following platforms:

- VMware ESXi
- OpenStack
- Third Party Orchestration

To know more about the configuration of GVHTTP2 and 5G-Cloud application for Casa vTAP, Oracle SCP, and Nokia SCP, refer to the following sections:

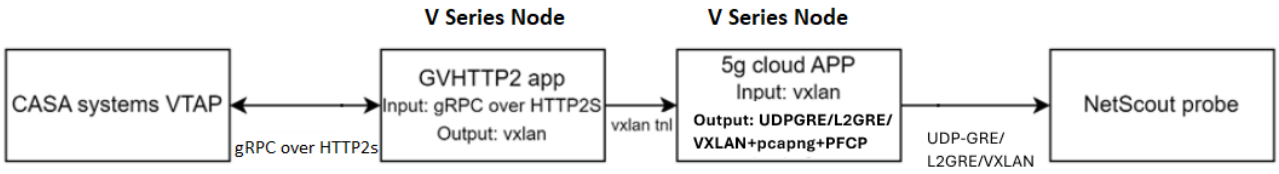
- 5G-Cloud Casa vTAP Support
- 5G-Cloud Oracle and Nokia SCP Support
- 5G-Cloud Ericsson SCP Support
- 5G Cloud Nokia HEP3 Support (Non-SBI)

5G-Cloud Casa vTAP Support

V Series Node supports receiving data from 5G Casa network functions in the Casa vTAP input format. This augments the currently existing functionality of receiving data from Ericsson network functions in Ericsson vTAP format and receiving data from Nokia network

functions in Nokia format. 5G-Cloud Casa vTAP is a non-service-based interface architecture in which input from the Casa vTAP system is processed, decoded, and sent out through an egress tunnel.

Casa systems vTAP network function mirrors the traffic in the 5G core and sends it out in gRPC encoded protobuf format. To convert the encoded protobufs to actual network traffic in 5G core, V Series Node supports two applications, GVHTTP2 and the 5G-Cloud.



GVHTTP2 Application

The first application, GVHTTP2, acts as an HTTP2 server. It receives the gRPC data over HTTP2 and establishes a TCP connection with the Casa vTAP system by acknowledging it. The application will extract the HTTP2 header and HTTP2 body, which are gRPC encoded, then encapsulate the data into a VXLAN header and send it out over the VXLAN tunnel to the next application, 5G-Cloud.

5G-Cloud Application

The 5G-Cloud application receives the VXLAN packet, decapsulates, and decodes the gRPC protobuf content. The application will extract the PFCP packets (N4 traffic) and convert the traffic into PCAPng format. It then sends the extracted packets to the NetScout tool probe over the UDP-GRE/L2GRE/VXLAN tunnels.

NOTE: Since the NetScout probe only understands Ericson vTAP format, which is UDP-GRE encapsulated in PCAPng format, the same is followed in the Casa vTAP system. As part of the 6.7 release, only N4 non-SBI traffic (PFCP) is supported.

Configuration of 5G-Cloud Casa vTAP

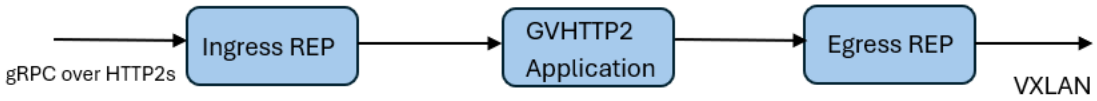
To configure the GVHTTP2 and 5G-Cloud applications in GigaVUE-FM, refer to the following sections:

- Configuration of GVHTTP2 Application for Casa vTAP
- Configuration of 5G-Cloud Application for Casa vTAP

Configuration of GVHTTP2 Application for Casa vTAP

In GigaVUE-FM, you must do the following to add the GVHTTP2 application in the Monitoring Session of a Monitoring Domain:

1. Create an ingress REP (Raw End Point) to receive the gRPC data over TCP on top of HTTP2. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.
2. Add the GVHTTP2 application in the Monitoring Session.
3. Create a link between ingress REP and the GVHTTP2 application.
4. Create egress REP.
5. Create a link between the GVHTTP2 application and egress REP.

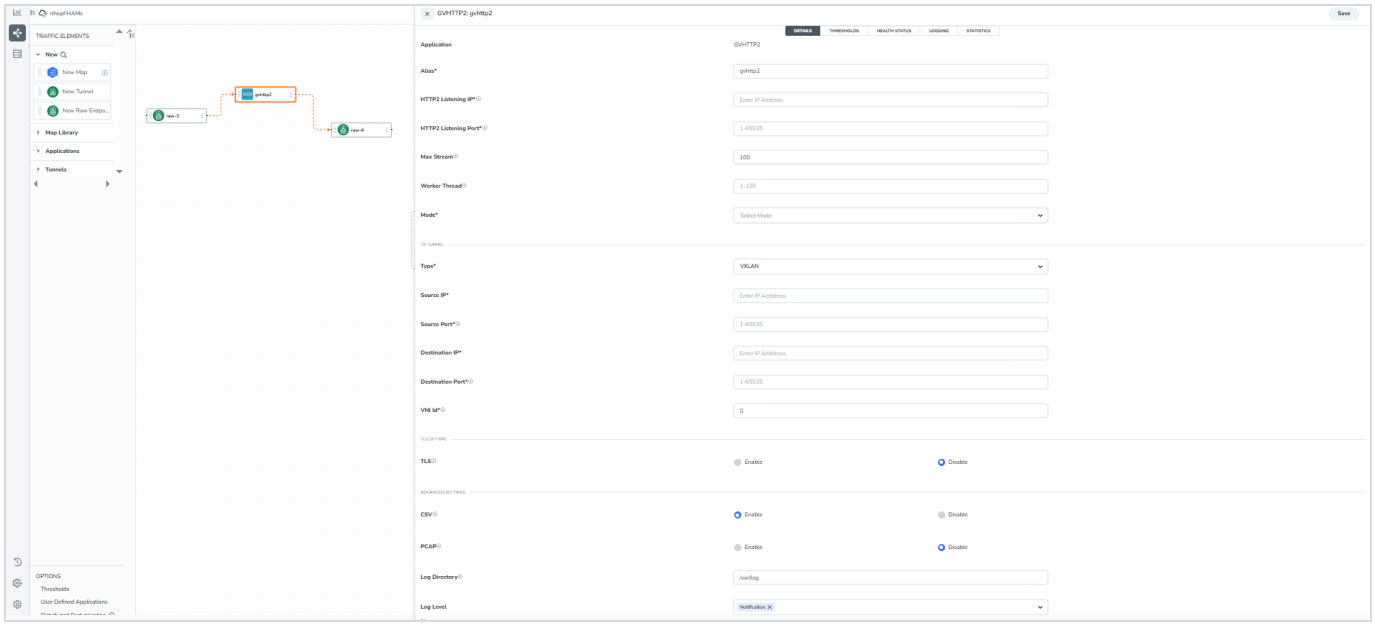


You can add a GVHTTP2 application to:

- **New Monitoring Session** - Add the GVHTTP2 application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a GVHTTP2 application:

1. In the canvas, drag and drop the GVHTTP2 application and select **Details**. The GVHTTP2 quick view appears.



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

Field	Description
Application	The name **GVHTTP2** appears by default.
Alias	Enter the alias name as **gvhttp2**.
HTTP2 Listening IP	Specify the HTTP2 IP address. The application will listen to the traffic on the specified IP address.
HTTP2 Listening Port	Specify the HTTP2 Port. The application will listen to the traffic on the specified port. Enter a value between 1 and 65535.
Max Stream	Specify the maximum number of concurrent streams in one HTTP2 session. Enter a value between 1 and 100. The default value is 100.
Worker Thread	Specifies the number of worker threads. Enter a value between 1 and 128. The default value is one.
Mode	Select **Casa vTAP** as mode from the drop-down menu.
TX Tunnel (Specifies the tunnel configuration from GVHTTP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the source port to bind for sending the packet. Enter a value between 1 and 65535.
Destination IP	Specify the destination IP address to which packets will be sent.
Destination Port	Specify the destination port where packets will be sent.
VNI id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
TLS Setting	
TLS	Select a TLS/SSL Monitor Mode from one of the following options:

	▪ Enable—When the monitor mode is enabled, the TLS/SSL decryption or encryption is off. ▪ Disable—This is the default value. When the monitor mode is disabled, the TLS/SSL decryption or encryption is on.
Advanced Setting	
Log Directory	Specify the path to store the log files.
Log Level	In the log level drop-down list, select the severity log level of the events from the following options: • PCAP • CSV • Info • Detail • Full-Parse

Downloading Logs for GVHTTP2 application

You can view the log files of a V Series Node or download them as CSV or .txt file.

To download the log files to a local environment:

1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click the **APPS LOGGING** link.
3. The **GVHTTP2 Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Configuration of 5G-Cloud Application for Casa vTAP

In GigaVUE-FM, you must do the following to configure the 5G-Cloud application in the Monitoring Session of a Monitoring Domain:

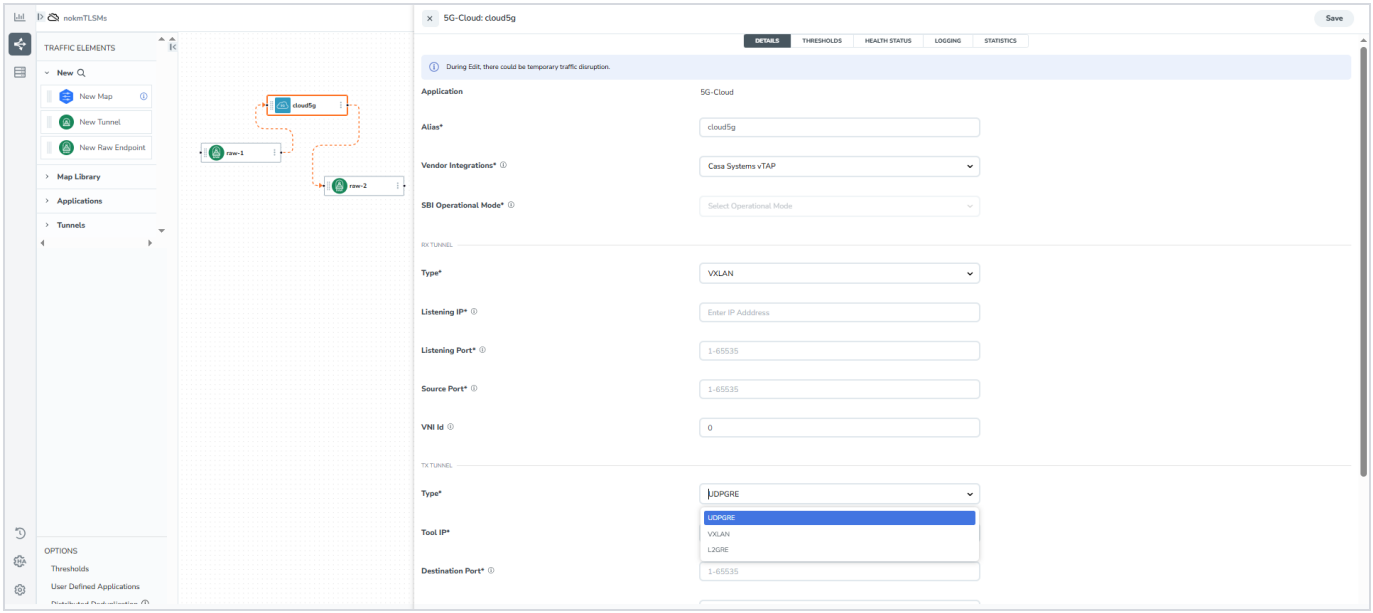
1. Create ingress REP to extract the HTTP2 body (gRPC content). Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)for more information on creating a REP.
2. Add the 5G-Cloud application in the Monitoring Session.
3. Create a link between ingress REP and the 5G-Cloud application.
4. Create egress REP.
5. Create a link between the 5G-Cloud application and egress REP.

You can add a 5G-Cloud application to:

- **New Monitoring Session** - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



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

Field	Description
Application	The name **5g-Cloud** appears by default.
Alias	Enter the alias name as **cloud5g**.
Vendor Integrations	From the drop-down list, select **Casa Systems vTAP**.

RX Tunnel (Specifies the tunnel configuration from GVHTTP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.
Listening IP	Specify the tunnel's local listen IP address (TX tunnel destination IP address used in GVHTTP2) to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is 0.
TX Tunnel	
Type	Select the tunnel type from the drop-down list. The available tunnel types are: • UDPGRE • VXLAN • L2GRE
Tool IP	Specify the remote IP address to which the packet will be sent.
Destination Port	Specify the tunnel destination port where the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind for sending the packet. Enter a value between 1 and 65535.
VNI ID **(Applicable only when the selected tunnel type is VXLAN**)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key **(Applicable only when the selected tunnel type is L2GRE**)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU. **Note**: For V Series Node version 6.8.00 and above, the range should be between 1400 and 8800. The default value is 8800. For V Series Node version below 6.8.00, range should be between 1500 and 8800. The default value is 8800.
Log Directory	Specify the path to store the log files.
Log Level	In the tunnel log level drop-down list, select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug

Downloading Logs for 5G-Cloud application

You can view the log files of a V Series Node or download them as CSV or .txt file.

To download the log files to a local environment:

1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and go to **TRAFFIC PROCESSING** tab. On the **cloud5g** application, click the ⋮ menu button and select **Details**. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. The **CLOUD5G Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Limitations

- The 5G-Cloud application does not validate the VNI ID configured by the user in the GVHTTP2 application when processing the VXLAN packets.
- The VNI ID configured by the user will not be validated while processing the packets received on the ingress interface. So, the 5G-Cloud application will not drop the VXLAN received on the ingress interface if the VNI ID received in the packet does not match the VNI ID configured by the user.
- After deploying the Monitoring Session from GigaVUE-FM, users can only change the following configuration parameters for the GVHTTP2 application:
  - Server (Listen IP Address and Port Number)
  - VXLAN (Source IP and Port Number)
  - VXLAN (Destination IP and Port Number)
- After deploying the Monitoring Session from GigaVUE-FM, users can only change the following configuration parameters for the 5G-Cloud application:
  - Ingress VXLAN (Listen IP, Listen Port Number, and Source Port Number)
  - Egress UDP-GRE/L2GRE/VXLAN Tunnels (Destination IP Address, Destination Port, Source IP, and Source Port)

Rules and Notes

- On a V Series Node, only one application (GVHTTP2 or 5G-Cloud or AMX) can be deployed across Monitoring Sessions.
- GVHTTP2, 5G-Cloud, and AMX applications should not be combined with general GigaSMART applications in a Monitoring Session or across Monitoring Sessions.

- For GVHTTP2, 5G-Cloud, and AMX applications, the source and destination links should be Raw Endpoints.
- Support for GVHTTP2, 5G-Cloud, and AMX applications is limited to 'none' tapping type.
- The 5G-Cloud and GVHTTP2 applications require the "VBL-ADD-ADV5GC" or "VBL-ADD-5GC" license.
- To deploy a Monitoring Session, ensure that the 'HTTP2 Listening IP address' and 'TX Tunnel Source IP address' in GVHTTP2 corresponds to the IP addresses of one of the V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the 'RX Tunnel Listening IP address' and 'TX Tunnel Source IP address' in 5G-Cloud correspond to the IP addresses of one of the V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the TX Tunnel Destination IP address used in GVHTTP2 and the RX Tunnel Listening IP address used in 5G-Cloud are the same.

NOTE: For information on stats details of Casa vTAP for GVHTTP2 and 5G-Cloud applications, refer to Appendix - Casa vTap Statistics.

5G-Cloud Oracle and Nokia SCP Support

GigaVUE V Series Node supports receiving data from 5G network functions in Oracle SCP and Nokia SCP input formats. In both Oracle and Nokia SCP, 3GPP standard method is followed, which has all the standard network components implemented.

Oracle SCP

Oracle systems input format is HTTP2/HTTP2S POST over TCP with TLS enabled. In Oracle SCP, the 5G-Cloud application synthesizes the packets and egresses them to the tool port after it has received all the 4-leg transactions. Oracle SCP processing in the 5G-Cloud application supports converting the discovery and the 4-legged (consumer, SCP, and producer) transactions to packets as per 3GPP Model C and Model D.

Model C

The Consumer knows the producer and sends messages through SCP. Model C comprises of 4-legged transactions between the consumer, SCP, and the producer. The 5G-Cloud application converts the 4-legged transactions to packets and sends them to the probe.

Model D

SCP sends discovery messages to discover the producer after receiving the messages from the consumer. Model D comprises of 2-legged transactions between the consumer and the SCP, 4-legged transactions between the SCP, SCP discovery, and the NRF to find the producer, and the 2-legged transactions between the producer and the SCP. The 5G-Cloud

application converts the 4-legged transactions between the consumer, SCP, and the producer to packets and sends them to the probe. The 5G-Cloud application also converts the discovery transactions between the SCP and the NRF and sends them to the probe.

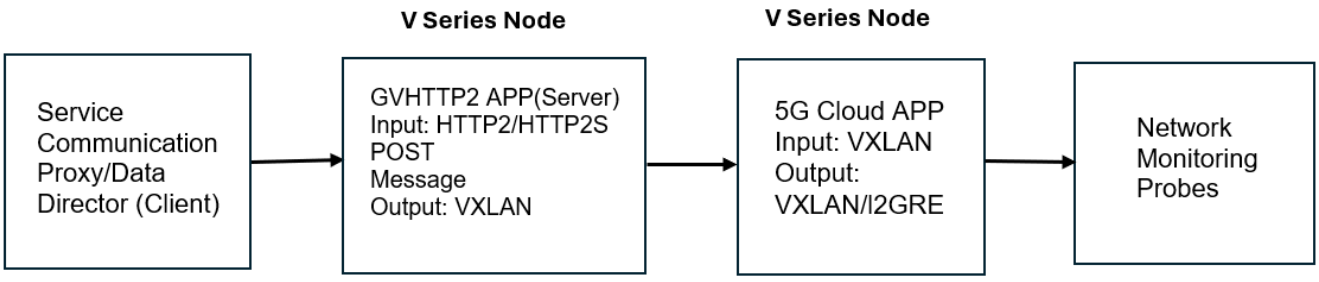
5G- Cloud application will ensure that both the discovery transaction and the 4-legged transaction are transmitted in order, to the connected tool or probe.

Nokia SCP

In Nokia SCP, traffic is mirrored between control functions using the HTTP2 protocol. This traffic is mirrored from a service called SCP (Service Control Proxy), a centralized point through which all the communications between all the control plane functions pass. SCP encrypts all the messages that are going across the control plane network functions and forwards that information in JSON-encoded format to GVHTTP2.

Both Model C and Model D transactions can be received from the SCP. However, Model D cannot be identified as Model D, because a separate message id is used for the discovery messages. In the case of Model D, SCP will include the Model D discovery transactions that happened with NRF along with the network function communication. Therefore, 6 transactions will be forwarded from SCP for a single request and response pair between any two network functions. The Model C transactions will be processed in 2 modes:

- Transparent (2 legged): The 5G-Cloud application will synthesize a direct transaction between the network functions. The 4-legged transactions received between the consumer, SCP, and the producer are synthesized to look like 2-legged transactions between the consumer and the producer.
- Inbound and outbound (4 Legged): The 5G-Cloud application will synthesize indirect transactions, meaning all transactions between any network function will go via SCP. All the transactions received in Model C or Model D are synthesized and sent to the probes.



GVHTTP2 Application

The first application, GVHTTP2, acts as an HTTP2 server, receives the data over HTTP2 frame and establishes a TCP connection with multiple Oracle SCP/DD or Nokia SCP pods. It receives the HTTP2 headers and stores them in a temporary buffer. Once it receives all the headers and body of that stream, it acknowledges back to the client. The application will extract the HTTP2 header and HTTP2 body, encapsulate the data into a VXLAN header, and send it out over the VXLAN tunnel to the next application, 5G-Cloud.

5G-Cloud Application

The 5G-Cloud application receives and decapsulates the VXLAN packet. It extracts the HTTP2 body, parses the SCP/DD JSON mirrored message, and associates the mirrored message transaction ID to track the complete transaction. It then synthesizes TCP Flow and HTTP2 Session representing full 5G CNF / SCP / 5G CNF transaction data and sends it out over L2GRE/VXLAN tunnel to the probe.
The 5G-Cloud application runs in Oracle SCP, Nokia SCP Transparent, and Nokia SCP Inbound-Outbound modes.

- In Nokia SCP Inbound-Outbound mode, both Inbound (between Consumer and SCP) and Outbound (between SCP and Producer) traffic is synthesized and sent to the connected Tool port. In Nokia SCP Transparent mode, only Inbound (between Consumer and SCP) traffic is processed and sent to the Tool Port.
- In the Nokia SCP Transparent mode, the 5G-Cloud Application will drop the Outbound traffic from the SCP (if received in the input).
- In the Nokia SCP Transparent mode, the Producer replaces the SCP in transactions between the Consumer and the SCP.
- In the Nokia SCP Transparent mode, authority header value will be replaced (if the replace authority configuration is enabled).

Configuration of 5G-Cloud Oracle/Nokia SCP

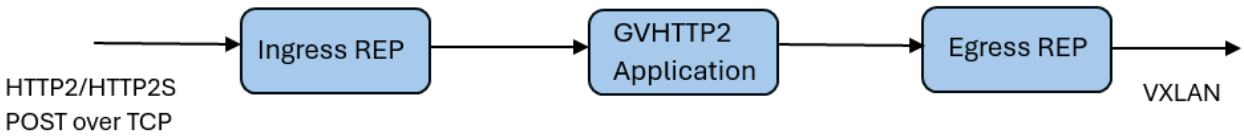
To configure the GVHTTP2 and 5G-Cloud applications in GigaVUE-FM, refer to the following sections:

- Configuration of GVHTTP2 Application for Oracle SCP/Nokia SCP
- Configuration of 5G-Cloud Application for Oracle SCP/Nokia SCP

Configuration of GVHTTP2 Application for Oracle SCP/Nokia SCP

In GigaVUE-FM, you must do the following to add the GVHTTP2 application in the Monitoring Session of a Monitoring Domain:

1. Create an ingress REP (Raw End Point) to receive the HTTP2/HTTP2S data over TCP. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.
2. Add the GVHTTP2 application in the Monitoring Session.
3. Create a link between ingress REP and the GVHTTP2 application.
4. Create egress REP.
5. Create a link between the GVHTTP2 application and egress REP.

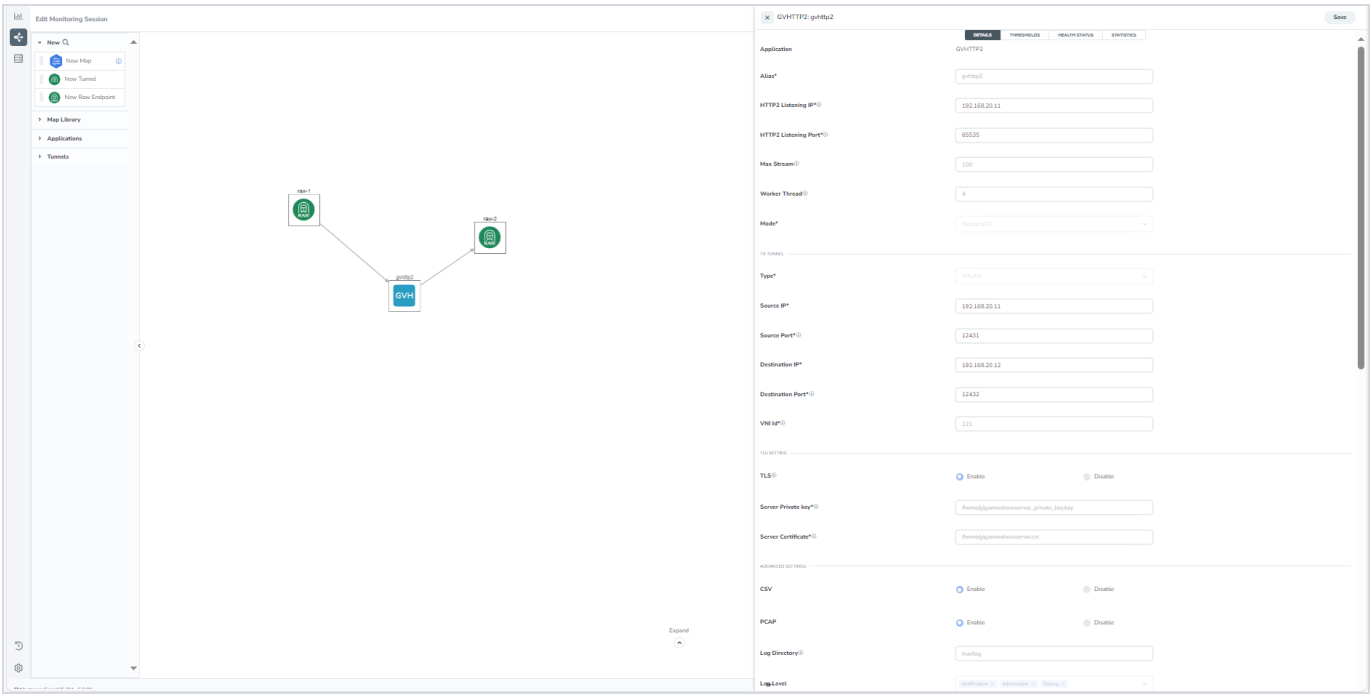


You can add a GVHTTP2 application to:

- New Monitoring Session - You can add the GVHTTP2 application after creating a new Monitoring Session and when the canvas appears.
- Existing Monitoring Session - Click **Edit** on the existing Monitoring Session, and the GigaVUE-FM canvas appears.

To add a GVHTTP2 application:

1. In the canvas, drag and drop the GVHTTP2 application and select **Details**. The GVHTTP2 quick view appears.



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

Field	Description
Application	The name **GVHTTP2** appears by default.
Alias	Enter the alias name as **gvhttp2**.
HTTP2 Listening IP	Specify the HTTP2 IP address. The application will listen to the traffic on the specified IP address.
HTTP2 Listening Port	Specify the HTTP2 Port. The application will listen to the traffic on the specified port.
Max Stream	Specify the maximum number of concurrent streams in one HTTP2 session. Enter a value between 1 and 100. The default value is 100.
Worker Thread	Specifies the number of worker threads. Enter a value between 1 and 128. The default value is four.
Mode	Select Oracle SCP or Nokia SCP as mode from the drop-down menu.
TX Tunnel (Specifies the tunnel configuration from GVHTPP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the source port to bind for sending the packet. Enter a value between 1 and 65535.
Destination IP	Specify the destination IP address to which packets will be sent.
Destination Port	Specify the destination port where packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.

	The default value is zero.
TLS Setting	
TLS	Select a TLS/SSL Monitor Mode from one of the following options: ▪ Enable—When the monitor mode is enabled, the TLS/SSL decryption or encryption is off. ▪ Disable—This is the default value. When the monitor mode is disabled, the TLS/SSL decryption or encryption is on.
Server Private key*	Specify the server private key only when TLS is enabled.
Server Certificate*	Specify server certificate only when TLS is enabled.
Advanced Setting	
CSV	Enable or disable the CSV log level.
PCAP	Enable or disable the PCAP log level.
Log Directory	Specify the path to store the log files.
Log Level	In the log level drop-down list, select the severity log level of the events from the following options. The default value level is Notification. • Notification • Information • Debug

Download Logs - GVHTTP2 application

You can view the log files of a V Series Node or download them as .CSV or .txt file.

To download the log files to a local environment:

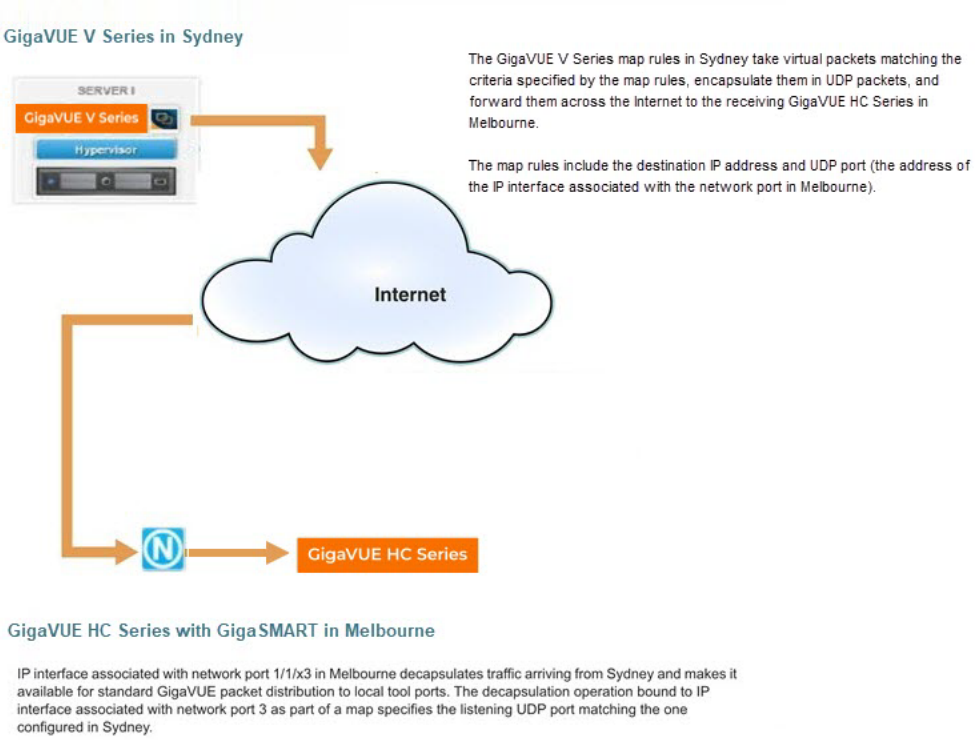
1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click the **APPS LOGGING** link.
3. The **GVHTTP2 Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Configuration of 5G-Cloud Application for Oracle SCP/Nokia SCP

In GigaVUE-FM, you must do the following to configure the 5G-Cloud application in the Monitoring Session of a Monitoring Domain:

1. Create ingress REP to extract the HTTP2 body. Refer to *Create Raw Endpoint* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more information on creating a REP.

2. Add the 5G-Cloud application in the Monitoring Session.
3. Create a link between ingress REP and the 5G-Cloud application.
4. Create egress REP.
5. Create a link between the 5G-Cloud application and egress REP.



Adding 5G-Cloud Application in Oracle SCP/Nokia SCP

Prerequisites

The pre-requisite to add a 5G-Cloud Application in Oracle SCP/Nokia SCP is:

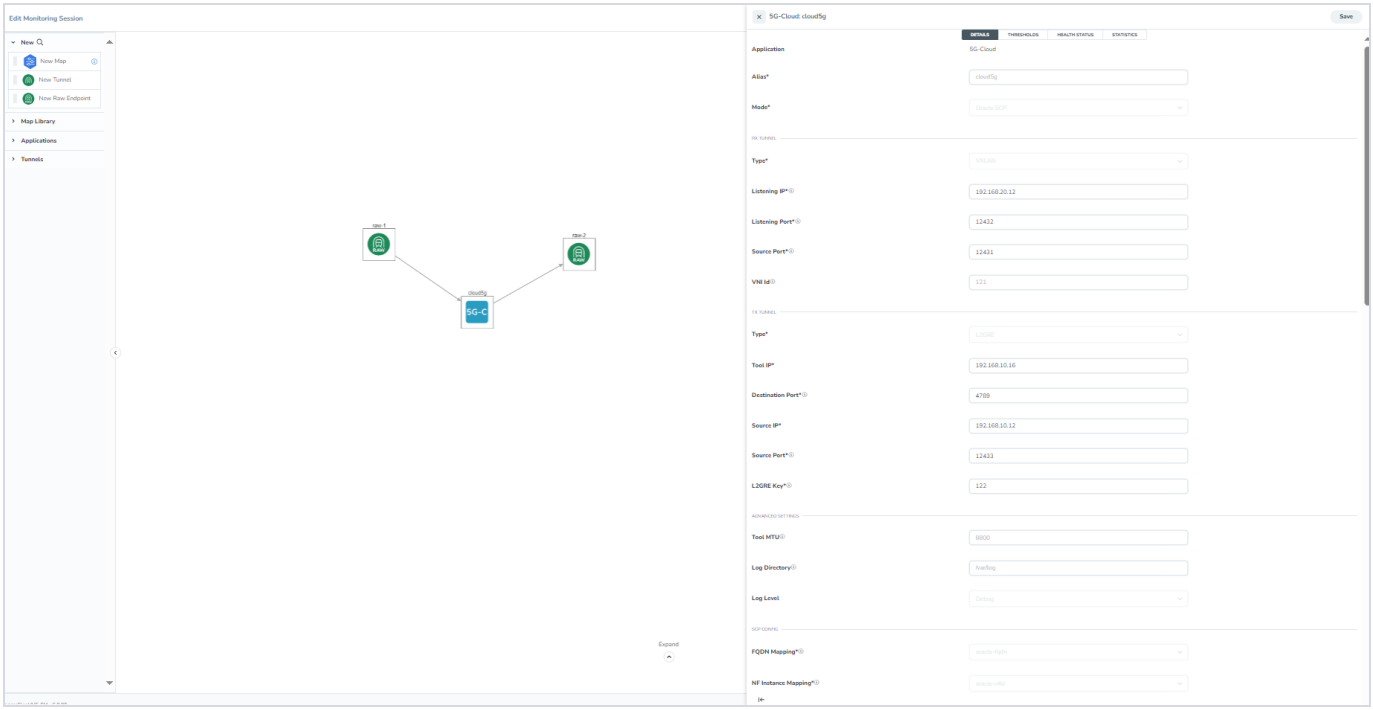
- You must upload CSV files containing a valid FQDN, NF Instance, and User Agent ID's and a valid IPv4/IPv6 addresses. To upload the CSV file, refer to Adding CSV file for IP Mapping.

You can add a 5G-Cloud application to:

- New Monitoring Session - You can add the 5G-Cloud application after creating a new Monitoring Session and when the canvas appears.
- Existing session - Click **Edit** on the existing Monitoring Session, and the GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



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

Field	Description
Application	The name **5g-Cloud** appears by default.
Alias	Enter the alias name as **cloud5g**.
Mode	From the drop-down list, select the required mode from the following options: • Oracle SCP • Nokia SCP Transparent • Nokia SCP Inbound/Outbound
RX Tunnel (Specifies the tunnel configuration from GVHTPP2 to 5G-Cloud)	
Type	Specify the tunnel type. VXLAN is selected by default.
Listening IP	Specify the tunnel's local listen IP address (TX tunnel destination IP address used in GVHTTP2) to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
TX Tunnel	

Type	Specify the tunnel type.
Tool IP	Specify the remote IP address to which the packet will be sent.
Destination Port	Specify the tunnel destination port where the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind for sending the packet. Enter a value between 1 and 65535.
VNI Id **(Applicable only when the selected tunnel type is VXLAN**)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key **(Applicable only when the selected tunnel type is L2GRE**)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU. **Note**: For V Series Node version 6.8.00 and above, the range should be between 1400 and 8800. The default value is 8800. For V Series Node version below 6.8.00, range should be between 1500 and 8800. The default value is 8800.
Log Directory	Specify the path to store the log files.
Log Level	In the tunnel log level drop-down list, select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug
SCP Config	
FQDN Mapping	Specify the alias name created for the uploaded FQDN table CSV file. You can also add new FDQN by utilizing the **ADD** button. **Note**: **Header details**: gigamon@test-5gc-new:/var/log/cloud5g_tabledir$ cat FQDN.txt FQDN,IngressIP1,IngressIP2,IngressPort,EgrIP,NFType,NFLocation (The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional) **Examples - 5G-Cloud FQDN Entries**: **Oracle SCP**:

	FQDN.txt:scp1.pp2.scp.5gc.mnc001.mcc208.3gppnetwork.org,10.64.104.30,10.64.104.36,9443,10.64.104.45,SCP,plolp **Nokia SCP**: s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,172.23.13.187,,8080,,SCP,plolp
NF Instance Mapping	Specify the alias name created for the uploaded NFID table CSV file. You can also add new NF Instance by utilizing the **ADD** button. **Note**: **Header details**: gigamon@test-5gc-new:/var/log/cloud5g_tabledir$ cat NFID.txt NFID,IngressIP1,IngressIP2,IngressPort,EgrIP,NFType,NFLocation (The fields NFID and ingressIP1 are mandatory. All other fields are optional) **Examples - 5G-Cloud NFID Entries:** • **Oracle SCP**: NFID.txt:04fba086-6ac1-4472-9ee3-cf10e57849f8,10.64.107.85,10.64.107.79,8080,,SMF,plolp • **Nokia SCP**: 8b94c7ee-d750-4bcd-95be-634b31a5fa0d,172.23.14.4,,8080,,AMF,jeolp
User Agent Mapping	Specify the alias name created for the uploaded User Agent table CSV file. You can also add new User Agent by utilizing the **ADD** button. **Note**: **Header details**: gigamon@test-5gc-new:/var/log/cloud5g_tabledir$ cat UA.txt UserAgent,IngressIP1,NFType,NFLocation (The fields useragentID and ingressIPAddress are mandatory. All other fields are optional) **Examples - 5G-Cloud User Agent Entries:** • **Oracle SCP**: pp5gs2nd15gcam01,10.64.106.67,AMF,jeolp • **Nokia SCP**: pp5gs2nd15gcam01,10.64.106.67,AMF,plolp pp5gs2nd15gcam02,10.64.106.107,AMF,plolp ofrpp25gcsmsf01,10.64.106.138,SMSF,jeolp
SCP Advanced Config	
No. of TCP Flows	Specify the total number of concurrent TCP flows. Enter a value between 128 and 2048. The default value is 1024.
No. of Transaction Flows	Specify the total number of Transaction Stream Flows allocated for tracking active Transaction Streams. Enter a value between 128 and 5500. The default value is 2048.
TCP Flow Timeout	Specify the TCP flow timeout ranging between 0 to 7200. The default value is 900.
SCP Transaction Timeout	Specify the SCP transaction timeout value ranging between 1 and 300. The default value is 10. **Note**: The recommended timeout value is between 10 and 20 seconds. An increase in the transaction timeout value will impact the total number of transactions that can be processed in parallel.
Minimum TCP Client Port	Specify the minimum value to be used for TCP client port ranging between 1023 and 65535. The default value is 32768.
Maximum	Specify the maximum value to be used for client port ranging between 1023 and 65535. The default value is 36863.

TCP Client Port	
Header Index	Enable or disable the header indexing flag from the available options. The default value is disable.
Header Compression Code **Note**: HTTP/2 requests and responses typically contain a large number of redundant headers. HTTP/2 uses header compression to compress headers significantly.	Enable or disable the header compression code from the available options. The default value is disable.
Gigamon Header **Note**: Helps in the debugging process to identify all transactions.	Enable or disable the Gigamon Header from the available options. The default value is Enable.
Nokia Use 3gpp Target API Root **(Applicable only when the selected mode is Nokia SCP Transparent)**	Specify the value which upon detecting producer IP/FQDN, treats the 3gpp Target API Root to be predictive of the Producer IP if value is non-zero as either enable or disable. The default value is disable.
Nokia	Specify the value which upon detecting producer IP/FQDN, treats the 3gpp Target API Root to

Replace Authority **(Applicable only when the selected mode is Nokia SCP Transparent)**	be predictive of the Producer IP if the value is non-zero as either enable or disable. The default value is disable.
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None

Download Logs - 5G-Cloud application

You can view the log files of a V Series Node or download them as .CSV or .txt file.

To download the log files to a local environment:

1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click the **APPS LOGGING** link.
3. The **CLOUD5G Logging** page displays the logs currently available. You can download the preferred logs by selecting the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download Files** from the **Actions** menu.
5. The system downloads the selected files to your local environment.

Adding CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field

3. Select any of the following from the **Type** as per the requirement:
    - **5G-Cloud FQDN** - Adding the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping. Adding FQDN is mandatory.
    - **5G-Cloud NF Instance** - Adding the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping.
    - **5G-Cloud UA** - Adding the CSV file containing a valid user agent ID and a valid IPv4/IPv6 address for IP mapping.
4. Click **Choose File** in **FileName** field to upload the CSV file into GigaVUE-FM.
5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

NOTE: For Oracle SCP, configuration of FQDN Mapping, NF Instance Mapping, and User Agent Mapping are mandatory. For Nokia SCP Transparent and Nokia SCP Inbound/Outbound, configuration of FQDN Mapping is mandatory.

Limitations

- The following configuration parameters for the GVHTTP2 application are non-editable and can be configured only during the initial configuration:
    - Mode
    - TX Tunnel – txType
    - Worker thread
    - RX VNI Id
    - Max Streams
    - TLS configuration
    - Log Level
    - Log Directory
- The following configuration parameters for the 5G-Cloud application are non-editable and can be configured only during the initial configuration:
    - Mode
    - TX Tunnel – txType
    - RX Tunnel - rxType
    - RX VNI Id
    - Tool MTU
    - Log Directory
    - Log Level
    - Header Index
    - Header Compression Code
    - Packet capture log level

- SCP log level
- Gigamon Header
- FQDN Mapping
- NF Instance Mapping
- User Agent Mapping

Rules and Notes

- The 5G-Cloud and GVHTTP2 applications require the "VBL-250T-ADD-5GC" license.
- It is recommended to use SRIOV enabled drivers for better performance and higher throughput. Refer to **Procedure to deploy V Series Node in VMware ESXi with SR-IOV Adapte** topic in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration guide for more details.
- On a V Series Node, only one application (GVHTTP2 or 5G-Cloud or AMX) can be deployed across Monitoring Sessions.
- GVHTTP2, 5G-Cloud, and AMX applications should not be combined with general GigaSMART applications in a Monitoring Session or across Monitoring Sessions.
- For GVHTTP2, 5G-Cloud, and AMX applications, the source and destination links should be Raw Endpoints.
- Support GVHTTP2, 5G-Cloud, and AMX applications is limited to 'none' tapping type.
- Configuration of GVHTTP2 and 5G-Cloud in V Series Node will fail in versions less than v6.7.00.
- To deploy a Monitoring Session, ensure that the 'HTTP2 Listening IP address' and 'TX Tunnel Source IP address' in GVHTTP2 correspond to the IP addresses of one of the V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the 'RX Tunnel Listening IP address' and 'TX Tunnel Source IP address' in 5G-Cloud correspond to the IP addresses of one of the V Series Node interfaces.
- To deploy a Monitoring Session, ensure that the TX Tunnel Destination IP address used in GVHTTP2, and the RX Tunnel Listening IP address used in 5G-Cloud are the same.
- When you have already deployed the 5G-Cloud application with all the table files uploaded, you should undeploy and redeploy the Monitoring Session again with the updated files to update the table.
- In the GVHTTP2 application, when the TLS/SSL configuration is enabled, the private key and certificate path must be configured.
- Before upgrading GigavUE V Series Node, user should undeploy the Monitoring Session where the GVHTTP2 application is deployed and take the backup of the SSL certificate and private key files. Following the upgrade, user should manually install/copy the private key and the certificate file in GigaVUE V Series Node and redeploy the GVHTTP2 application.
- To upload the table configuration file in CSV format, go to Inventory -> Virtual ->Settings -> 5G-Apps, enter the alias, type the CSV file name, and upload it.

- To download the files, go to Inventory -> Virtual ->Settings -> 5G-Apps and select the alias name to be downloaded.
- From release version 6.9.00, the maximum Transaction Flow value for V Series Nodes with memory less than 32 GB is 5500. For V Series Nodes classified as extra-large with memory greater than 32 GB, the maximum Transaction Flow value is 26000.
- From release version 6.9.00, to make use of the multithreading support for egress/ingress tunnels in GVHTTP2/5G-Cloud applications, you should update the thread count after the VSN is upgraded.
- The configuration of the 5G-Cloud application should be performed on extra-large VMs.
  - Configuration specifications for extra large VM:
    - vCPUs: 12-20
    - RAM: 32 GB
    - Disk: 160 GB
  - Supported Ports: Management Ports, Tunneling Ports, and 2 Data Ports

FHA Dashboards for 5G-Cloud Applications

After configuring the GVHTTP2 and 5G-Cloud applications, you can monitor the statistics for Oracle SCP and Nokia SCP by the reports displayed in the Dashboard.

To access the details, refer to **FHA Dashboards for 5G-Cloud Applications** topic in GigaVUE Fabric Management Guide.

5G-Cloud Ericsson SCP Support

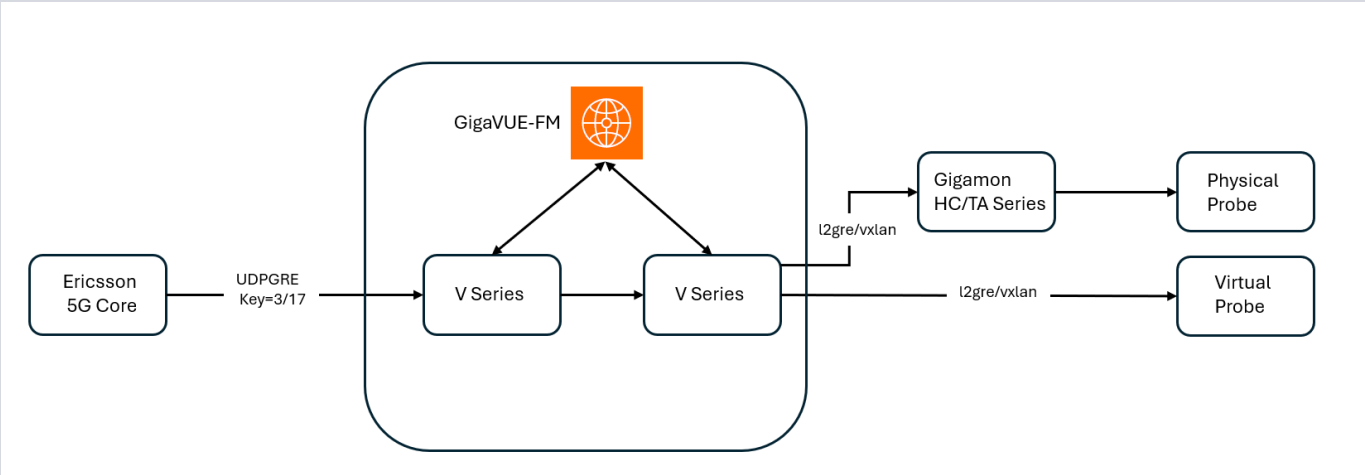
The 5G Core follows a service-based architecture where control plane network functions communicate using the HTTP2 protocol. In Ericsson SCP Mode, HTTP2 transactions are mirrored through the Service Communication Proxy (SCP) and encapsulated using UDP-GRE for further processing.

Ericsson SCP

In **Ericsson vTAP**, traffic is tapped from the Packet Core Controller (PCC), including AMF and SMF, in Layer 7 HTTP SBI JSON format. The 5G SBI application supports this PCC traffic, ensuring efficient processing and monitoring. Refer to 5G-Service Based Interface Application.

In **Ericsson SCP** mode, the Service Communication Proxy (SCP) mirrors 5G SBI traffic within the Cloud Core Signaling Controller, capturing communication between multiple network functions via SCP.

The 5G-Cloud application in GigaVUE V Series Nodes is enhanced to receive and process traffic from the Ericsson SCP and forward it to the monitoring tools. This setup supports both configuration and visualization through GigaVUE-FM integration.



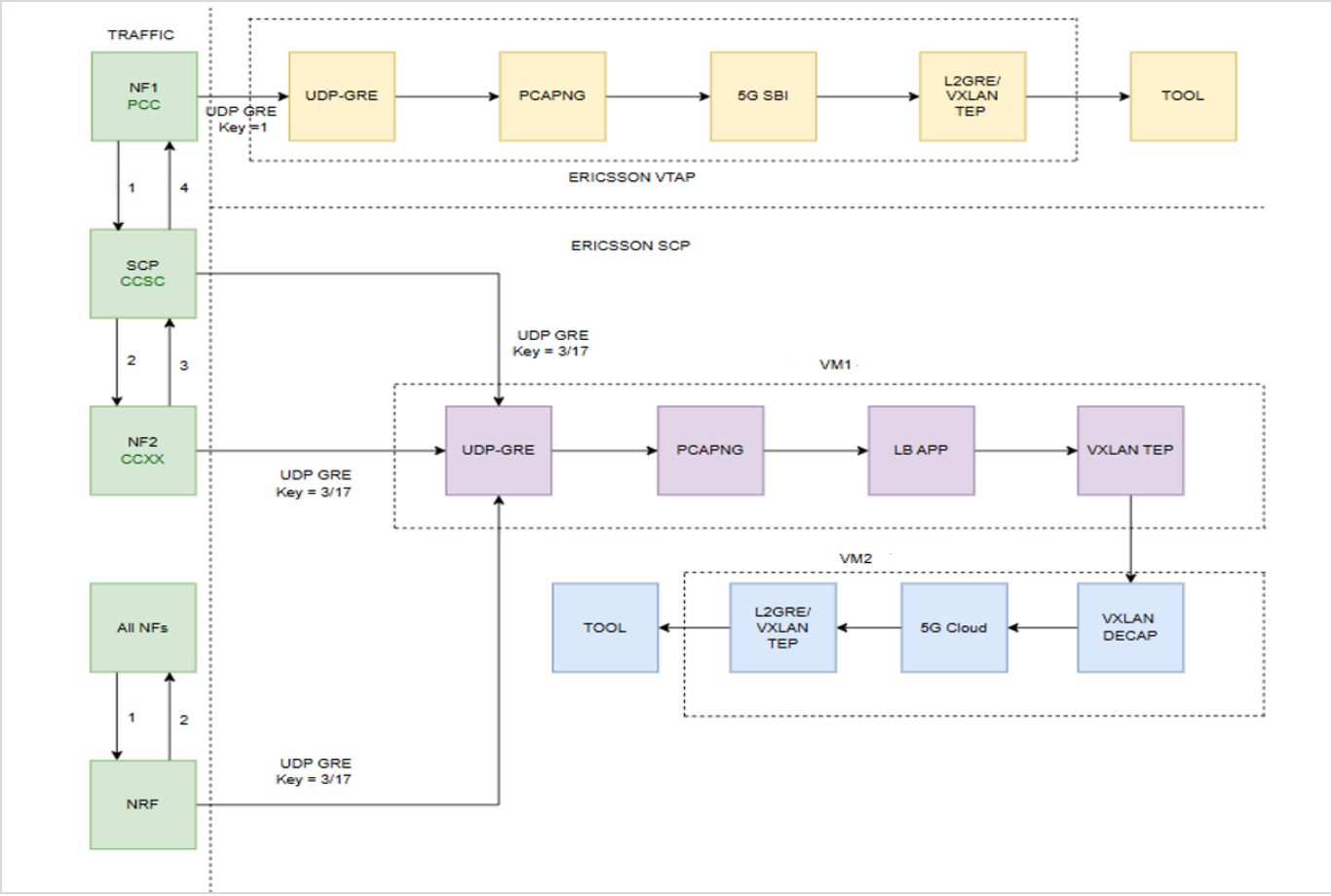
Traffic from the Ericsson 5G Core is encapsulated using UDP-GRE tunnels, with specific keys 3 and 17, to identify different traffic flows from SCP. GigaVUE-FM serves as the centralized management platform orchestrating the visibility fabric, which includes the V Series Nodes. The V Series Nodes inspect, aggregate, and process the incoming packets. After processing, traffic is encapsulated using L2GRE or VXLAN tunneling protocols and forwarded to either physical or virtual probes as follows:

- **Physical Probe**: If IP connectivity is not available, the traffic is sent to a GigaVUE HC/GigaVUE TA Series device, which serves as a traffic aggregator and distributor. The device decapsulates and distributes the traffic to the probe.
- **Virtual Probe**: If IP connectivity is available, the processed traffic is forwarded directly to virtual probe for detailed traffic inspection and analytics.

This end-to-end solution ensures comprehensive visibility into 5G network traffic, facilitating efficient monitoring and performance analysis across both physical and cloud-based infrastructures.

How Ericsson SCP Solution works

The following image shows the block diagram of the data flow in the V Series Nodes.



The encapsulated traffic enters the system, and based on the key values, is passed through a PCAP-NG, 5G SBI, and LB application to capture and monitor the data.

For traffic mirroring and flow processing in Ericsson VTap 5G Core network with key value 1, refer to 5G-Service Based Interface Application

When traffic is processed through keys 3 and 17, the **PCAPng** application reads and validates various blocks within received PCAPng files before forwarding them to the Load Balancing application. It processes data based on the packet type, which includes a combination of the following blocks. Refer to PCAPng Application.

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

The **Load Balancing** application efficiently distributes traffic with different flow IDs across multiple cores, enabling parallel processing of packets with distinct stream IDs. It ensures that request and response frames with the same stream ID are processed sequentially within the same core, preventing race conditions where these frames might otherwise be handled in parallel across different cores. Refer to Load Balancing.

The extracted data is encapsulated within a VXLAN and routed to the 5G-Cloud application. The 5G-Cloud application processes VXLAN packets by first decapsulating them to extract the HTTP2 headers and body. It then parses the EEVTAP TCP mirrored message and maps the transaction ID to track the full transaction.

After synthesizing the TCP flow and HTTP2 session to represent the complete 5G CNF/SCP/5G CNF transaction data, it forwards the data over an L2GRE/VXLAN tunnel to the probe. Refer to Create Ingress and Egress Tunnels.

Notes:

- Ericsson SCP will process only Model C traffic.
- You can deploy traffic ingress applications together in a single V Series Node and Monitoring Session. However, for the 5G-Cloud and egress applications, you must deploy a separate Monitoring Session and V Series Node.
- You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session.
- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.

Configuration of 5G-Cloud Ericsson SCP

In GigaVUE-FM, you must do the following to configure the 5G-Cloud application in the Monitoring Session of a Monitoring Domain in the V Series:

V Series Node 1:

S.No	Steps	Refer to
1	Configure UDP-GRE Ingress TEP to receive the HTTP2 messages. **Note**: You should configure individual UDP-GRE tunnels for each of the following key values: • Key Value 1: Ericsson vTAP . • Key Values 3 and 17: Ericsson SCP.	Create Ingress and Egress Tunnel (VMware vCenter) Create Ingress and Egress Tunnels (OpenStack) Create Ingress and Egress Tunnel (Third Party Orchestration)
2	Configure PCAPng application and link ingress TEP and PCAPng application instances in the Monitoring Session.	PCAPng Application
3	Configure LB application and link LB application and PCAPng	Load Balancing

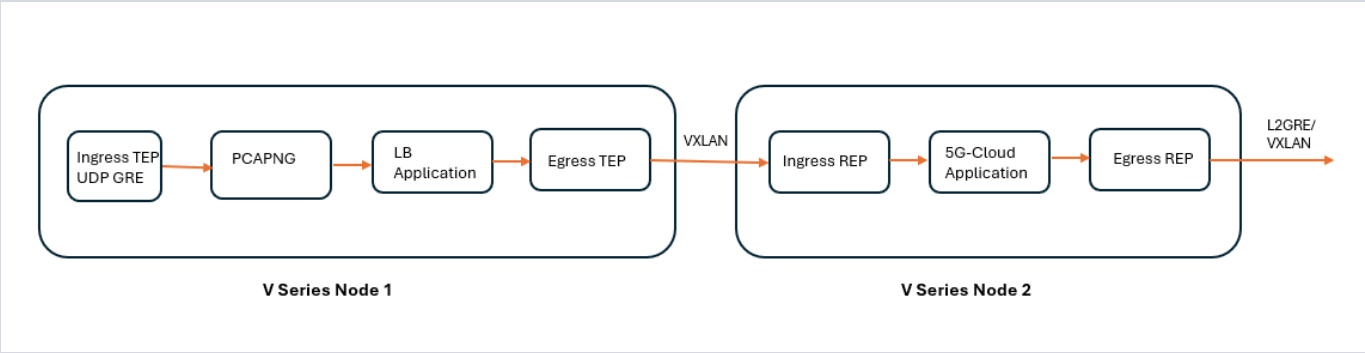
	application instances in the Monitoring Session.	
4	Create a VXLAN egress TEP.	Create Ingress and Egress Tunnel (VMware vCenter) Create Ingress and Egress Tunnels (OpenStack) Create Ingress and Egress Tunnel (Third Party Orchestration)
5	Create a link between egress TEP and LB application.	

Note: When upgrading GigaVUE-FM with a Monitoring Session in V Series Node 1 to version 6.12 from an earlier release, follow these steps to ensure a successful migration:

- Undeploy the existing V Series Node 1 Monitoring Session.
- Delete any Egress VXLAN TEPs with the Multi-Tunnel feature enabled.
- Recreate the Egress VXLAN TEP with the required configuration and enable the Multi-Tunnel flag.
- Establish a Link connection between the LB application and the Egress VXLAN TEP.
- Deploy the Monitoring Session.

V Series Node 2:

S.No	Steps	Refer to
1	Create a ingress REP to extract the HTTP2 body.	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (OpenStack) Create Raw Endpoint (Third Party Orchestration)
2	Create a link between the VXLAN egress TEP and ingress REP.	
3	Add the 5G-Cloud application in the Monitoring Session.	5G-Cloud Application
4	Create a link between ingress REP and the 5G-Cloud application.	
5	Create egress REP.	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (OpenStack) Create Raw Endpoint (Third Party Orchestration)
6	Create a link between the 5G-Cloud application and egress REP.	



Add 5G-Cloud Application in Ericsson SCP

Pre-requisite:

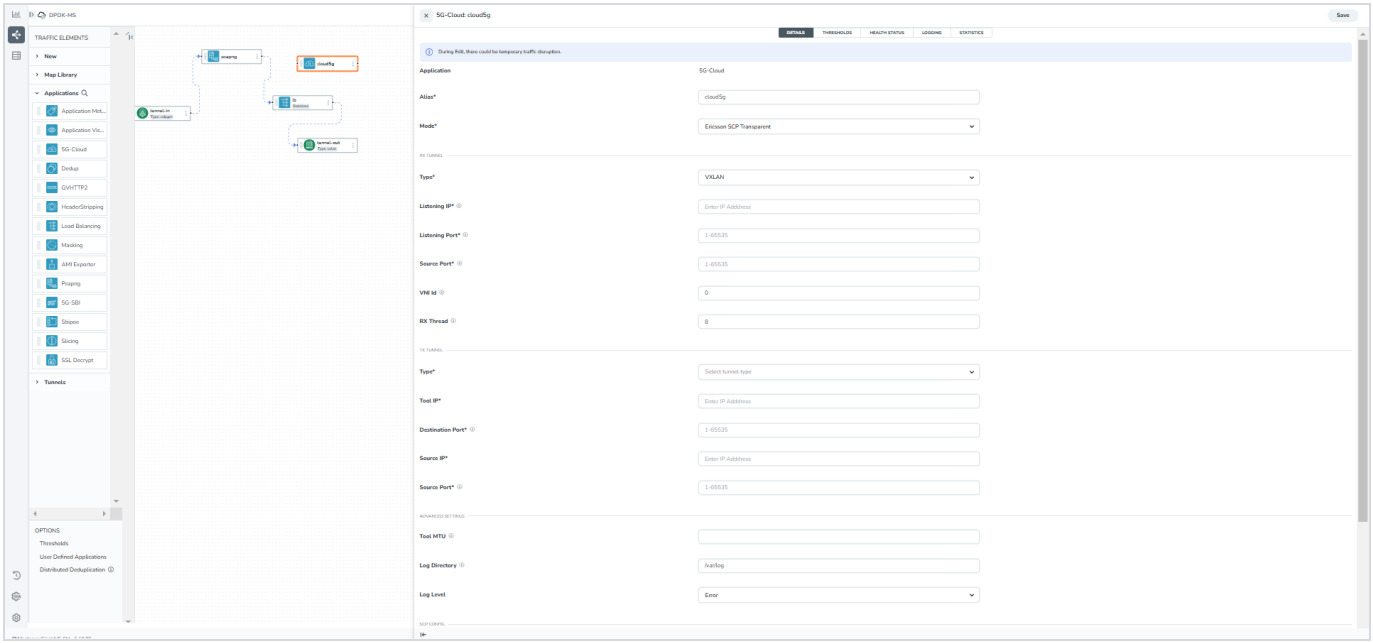
- You must upload CSV files containing a valid FQDN, NF Instance, and User Agent IDs and a valid IPv4/IPv6 address. Refer to Add CSV file for IP Mapping.

You can add a 5G-Cloud application to:

- New Monitoring Session - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- Existing session - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



2. On the application quick view, enter or select the required information as described in the 5G Cloud Ericsson SCP Configuration - Field References.

NOTE: It is recommended to maintain a 60-90 second delay when undeploying and deploying a Monitoring Session in GigaVUE-FM.

5G Cloud Ericsson SCP Configuration - Field References

Field	Description
Application	The name **5g-Cloud** appears by default.
Alias	Enter the alias name as **cloud5g**.
Mode	From the drop-down list, select **Ericsson SCP Transparent**.
RX Tunnel	
Type	Specify the tunnel type. The default is VXLAN.
Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
VNI Id	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215. The default value is zero.
RX Thread	Specify the RX value to receive the packet. Enter a value between 1 and 16. The default value is 8.
TX Tunnel	
Type	Specify the tunnel type. The available tunnel types are: • VXLAN • L2GRE
Tool IP	Specify the remote IP address to send the packet.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
VNI Id **(Applicable only when the selected tunnel type is VXLAN)**	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key **(Applicable only when the selected tunnel type is L2GRE)**	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU.

Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug
SCP Config	
FQDN Mapping	Specify the alias name created for the uploaded FQDN table CSV file.
NF Instance Mapping	Specify the alias name created for the uploaded NFID table CSV file.
User Agent Mapping	Specify the alias name created for the uploaded User Agent table CSV file.
TCP Server Ports	Specify the TCP server port or port range to allow TCP communication endpoints.
SCP Advanced Config	
No. of TCP Flows	Specify the total number of concurrent TCP flows. Enter a value between 128 and 2048. The default value is 1024.
No. of Transaction Flows	Specify the total number of Transaction Stream Flows allocated for tracking active Transaction Streams. Enter a value between: • 128 and 26000 for V Series Node of extra large form factor (total memory ≥ 32GB). • 128 and 5500 for V Series Node of large form factor (total memory < 32GB). The default value is 2048.
TCP Flow Timeout	Specify the TCP flow timeout ranging between 0 to 7200. The default value is 900.
SCP Transaction Timeout	Specify the SCP transaction timeout value ranging between 1 and 300. The default value is 10. **Note**: The recommended timeout value is between 10 and 20 seconds. An increase in the transaction timeout value will impact the total number of transactions that can be processed in parallel.
Minimum TCP Client Port	Specify the minimum value to be used for TCP client port ranging between 1023 and 65535. The default value is 32768.
Maximum TCP Client Port	Specify the maximum value to be used for client port ranging between 1023 and 65535. The default value is 36863.
SCP Processing Threads	Specify the number of worker threads for processing In-Out packets. Enter a value between 1 and 16. The default value is 8.
TCP Client Ports per Thread	Specify the number of TCP client ports for each worker thread. Enter a value between 100 and 8000. The default value is 1000.
Header Index	Enable or disable the header indexing. The default value is disabled.
Header Compression Code	Enable or disable the header compression code. The default value is disable.
Gigamon Header	Enable or disable the Gigamon Header. The default value is Enable.

Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None
HTTP2 Monitored Flows	
Number of Streams	Specify the number of monitored stream flows. Enter a value between 1024 and 16384. The default is 1024.
Request Timeout	Specify the HTTP/2 request timeout in seconds. Enter a value between 1 and 300. The default is 15 seconds.
Response Timeout	Specify the HTTP/2 response timeout in seconds. Enter a value between 1 and 300. The default is 2 seconds.
TCP Monitored Flows	
Number of Flows	Specify the number of monitored TCP flows. Enter a value between: • 1024 and 32768 for V Series Node of extra large form factor (total memory > 32GB). • 1024 and 2048 for V Series Node of lesser form factor. The default value is 2048.
Flow Timeout	Specify the timeout for TCP flows in seconds. Enter a value between 1 and 7200. The default value is 60 seconds.
Flow Reassembly Timeout	Specify the timeout for TCP flow reassembly in seconds. Enter a value between 1 and 7200. The default value is 500 seconds.

Download Logs - 5G-Cloud application

You can view the log files of a V Series Node or download them as .CSV or .txt files.

To download the log files to a local environment:

1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and click **Details** on the 5G-Cloud application. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. Select the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.

4. Select the log files to download, and then click **Download > Files**. The system downloads the selected files to your local environment.

Add CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field
3. From the Type drop-down list, select one of the following:
   - **5G-Cloud FQDN** - Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.
   - **5G-Cloud NF Instance** - Add the CSV file containing a valid NF instance ID and a valid IPv4/IPv6 address for IP mapping.
   - **5G-Cloud UA** - Add the CSV file containing a valid user agent ID and a valid IPv4/IPv6 address for IP mapping.
4. Click **Choose File** in the **FileName** field to upload the CSV file into GigaVUE-FM.

Notes - Header details of the CSV file:

- **FQDN Mapping**: gigamon@vseries:/var/log/cloud5g_tabledir$ cat FQDN.txt (The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional)
  - Header details: FQDNid,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation
  - Example: s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,170.00.13.187,,8080,,SCP,plolp
- **NF Instance Mapping**: gigamon@vseries:/var/log/cloud5g_tabledir$ pwd NFID.txt (The fields NFID and ingressIP1 are mandatory. All other fields are optional)
  - Header details: NFID,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation
  - Example: 8b94c7xx-d700-4xcd-90be-634x11a5xx0d,100.23.14.4,,8080,,AMF,plolp
- **User Agent Mapping**: gigamon@vseries:/var/log/cloud5g_tabledir$ pwd UA.txt (The fields useragentID and ingressIPAddress are mandatory. All other fields are optional)
  - Header details: UserAgent,IngressIP1,NFType,NFLocation
  - Example: xx5gs20015gcay01,192.64.10.67,AMF,plolp

The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional.

5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

FHA Dashboards for 5G-Cloud Applications

After configuring the 5G-Cloud application, you can monitor the statistics for Ericsson SCP by the reports displayed in the Dashboard. To access the details, refer to FHA Dashboards for 5G-Cloud Applications.

5G Cloud Nokia HEP3 Support

NOTE: CMM Solution is now available as an Early Access feature, giving you the opportunity to explore its capabilities before the general availability (GA).

Nokia HEP3 (Homer Encapsulation Protocol Version 3) method is supported by Nokia for network functions across 3G,4G, 5G and the IMS core. HEP3 efficiently organizes and encodes data for various network protocols and enhances the functionality of Nokia's core network solutions by accommodating diverse packet requirements.

The 5G-Cloud application supports processing the Nokia HEP3 format from the **IMS** network functions and 3G, 4G network functions. Non-SBI traffic is received as a TCP stream with HEP3 encoding by the 5G Cloud application. The 5G-Cloud application receives encapsulated traffic from the IMS vTAP in HEP3 over TCP, using either clear text or mTLS. Non-SBI control traffic is decoded from HEP3, emphasizing data handling without IP translation.

Nokia Cloud Mobility Manager (**CMM**), including AMF and MME, generates SBI and Non-SBI traffic over HTTP2 using clear text / TLS. The gvHTTP2 application receives this traffic and forwards it to the 5G-Cloud application. The 5G-Cloud synthesizes SBI payloads into L2GRE/VXLAN packets, enabling seamless monitoring across 5G core interfaces.

In **Nokia SCP** mode, the traffic is mirrored between the 5G control functions using HTTP2 protocol, which is mirrored from a service called SCP (Service Communication Proxy). The 5G-Cloud application receives the JSON encoded data from the VXLAN ingress TEPs. Refer to Nokia SCP.

The system supports the following types of traffic:

- 5G Cloud Nokia HEP3 Support (Non-SBI)
- 5G Cloud Nokia HEP3 Support (SBI)

Supportability Table

The supportability table provides a quick reference to the supported Nokia functions:

Traffic Type	Source Functions	Protocols	Reference
Non-SBI	3G, 4G, IMS	HEP3 over TCP with Clear Text / mTLS	5G Cloud Nokia HEP3 Support
SBI	CMM (AMF, MME)	HEP3 over HTTP2 over TCP with Clear Text / TLS	5G Cloud Nokia HEP3 Support

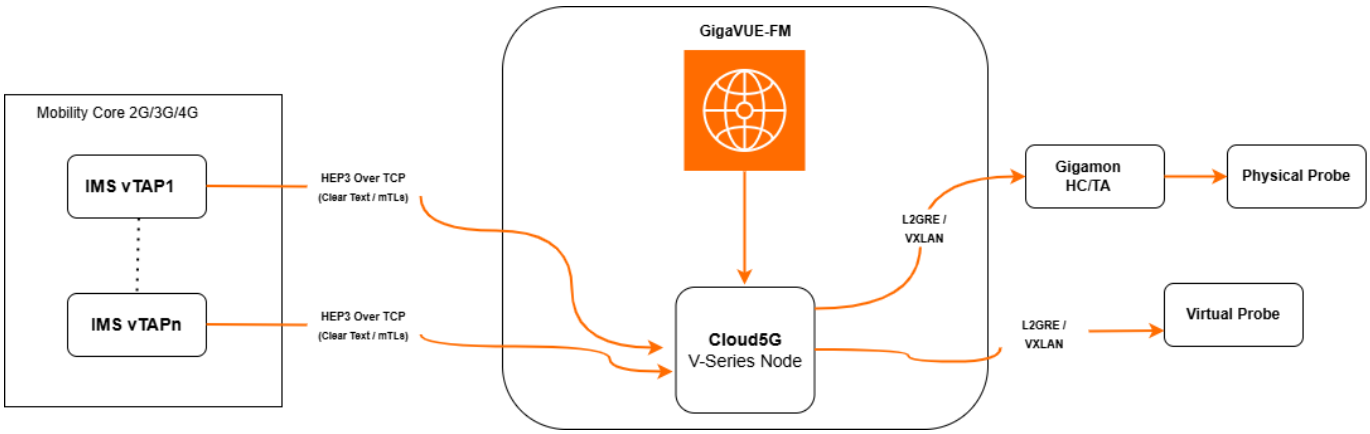
5G Cloud Nokia HEP3 Support (Non-SBI)

Nokia HEP3 method is supported by Nokia for network functions across 3G,4G, 5G and the IMS core. HEP3 efficiently organizes and encodes data for various network protocols and enhances the functionality of Nokia's core network solutions by accommodating diverse packet requirements.

The 5G-Cloud application supports processing the Nokia HEP3 format from the non-SBI network functions – IMS network functions and 3G, 4G network functions. Traffic (clear text or secured with mTLS) is received as a TCP stream with HEP3 encoding by the 5G Cloud application. The 5G-Cloud application receives encapsulated traffic from the IMS vTAP in HEP3 over TCP, using either clear text or mTLS.. Non-SBI control traffic is decoded from HEP3 (Homer Encapsulation Protocol Version 3), emphasizing data handling without IP translation.

How Nokia HEP3 Solution works

The following image shows the ingress and egress data flow through the V Series Node for Nokia HEP3 solution.



The traffic (clear text or secured with mTLS) from the client vTAP systems is transported over TCP. The 5G-Cloud application processes and manages the incoming TCP traffic and terminates the TCP connection. The application then processes the TCP payload and synthesizes the data.

GigaVUE-FM serves as the centralized management platform orchestrating the visibility fabric, which includes the 5G-Cloud V Series Node. The V Series Nodes inspect, aggregate, and process the incoming traffic. After processing, traffic is encapsulated using L2GRE or VXLAN tunneling protocols and forwarded to either physical or virtual probes as follows:

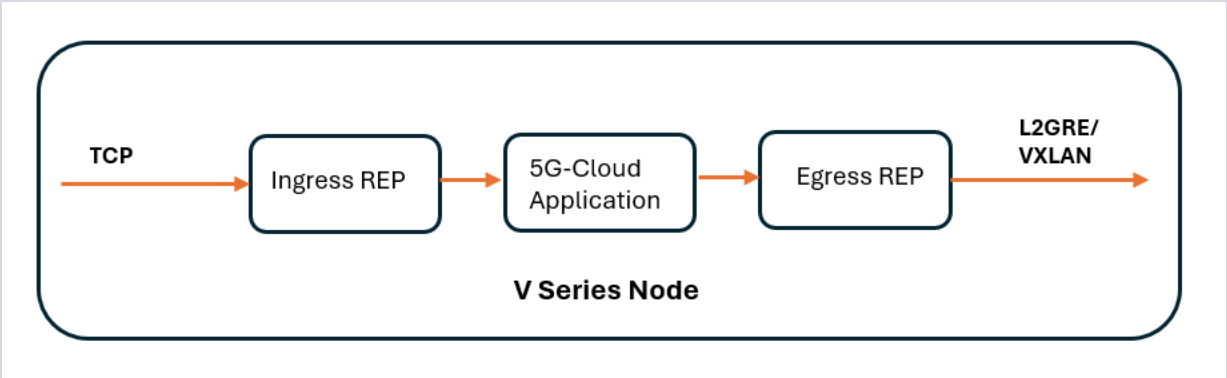
- **Physical Probe**: If IP connectivity is not available, the traffic is sent to a GigaVUE HC/GigaVUE TA Series device, which serves as a traffic aggregator and distributor. The device decapsulates and distributes the traffic to the probe.
- **Virtual Probe**: If IP connectivity is available, the processed traffic is forwarded directly to virtual probe for detailed traffic inspection and analytics.

This end-to-end solution ensures comprehensive visibility into 5G network traffic, facilitating efficient monitoring and performance analysis across both physical and cloud-based infrastructures.

Configuration of 5G-Cloud Nokia HEP3

In GigaVUE-FM, you must do the following to add the 5G-Cloud application in the Monitoring Session of a Monitoring Domain:

S.No	Steps	Refer to
1	Create an ingress REP to receive the data over TCP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (OpenStack) Create Raw Endpoint (Third Party Orchestration)
2	Add the 5G-Cloud application in the Monitoring Session	5G-Cloud Application
3	Create a link between ingress REP and the 5G-Cloud application	NA
4	Create egress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (OpenStack) Create Raw Endpoint (Third Party Orchestration)
5	Create a link between the 5G-Cloud application and egress REP	NA



Configure Nokia HEP3 in 5G-Cloud Application

Pre-requisite:

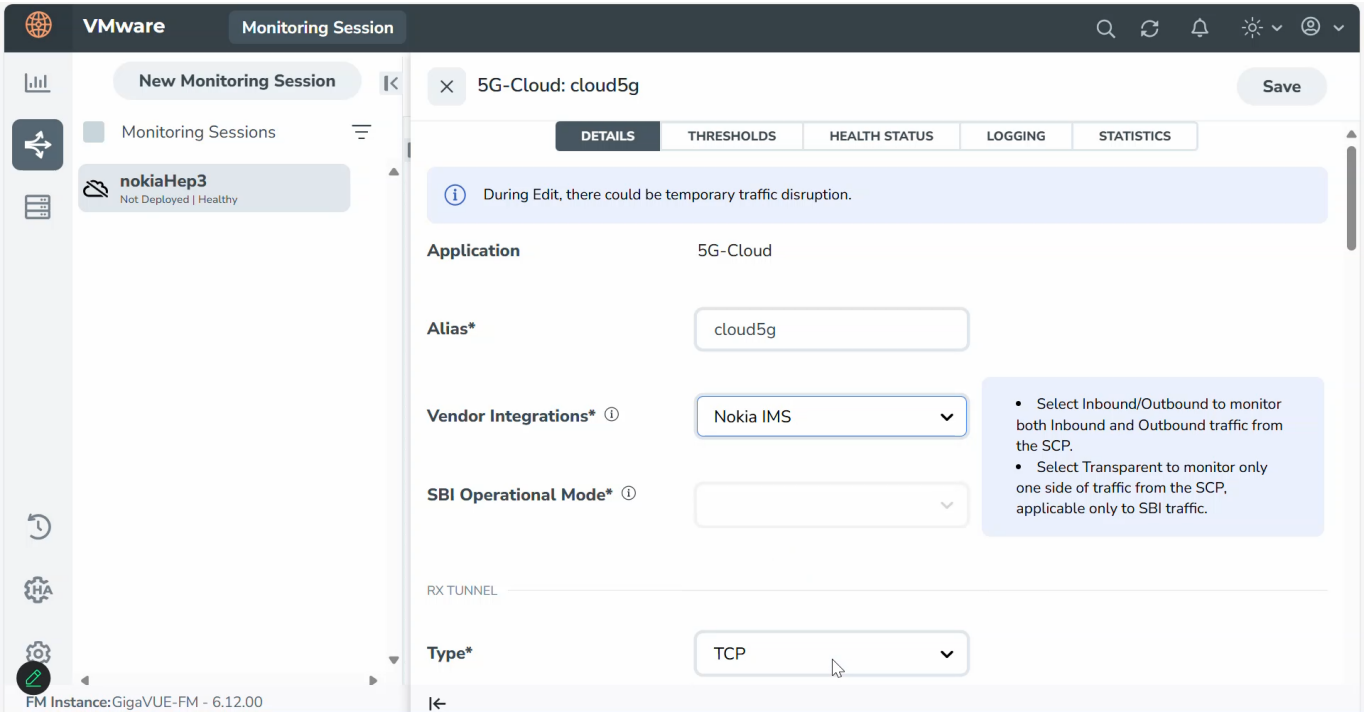
- You must upload CSV files containing a valid FQDN and a valid IPv4/IPv6 address. Refer to Add CSV file for IP Mapping.

You can add a 5G-Cloud application to:

- **New Monitoring Session** - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



2. On the application quick view, enter or select the required information as described in the Reference - Configuration Table .

NOTE: It is recommended to maintain a 60-90 second delay when undeploying and deploying a Monitoring Session in GigaVUE-FM.

Reference - Configuration Table

Field	Description
Application	The name **5g-Cloud** appears by default.
Alias	Enter the alias name as **cloud5g**.
Vendor Integrations	From the drop-down list, select **Nokia IMS**.
SBI Operational Mode	The Operational Mode will be grayed out on selecting Nokia CMM/IMS.
RX Tunnel	
Type	Specify the tunnel type. The default is TCP.
Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
TX Tunnel	
Type	Specify the tunnel type. The available tunnel types are: • VXLAN

	• L2GRE
Tool IP	Specify the remote IP address to send the packet.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
VNI Id **(Applicable only when the selected tunnel type is VXLAN**)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key **(Applicable only when the selected tunnel type is L2GRE**)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU. **Note**: For V Series Node version 6.8.00 and above, the range should be between 1400 and 8800. The default value is 8800. For V Series Node version below 6.8.00, range should be between 1500 and 8800. The default value is 8800.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug
HEP3 Config	
Number of Ingress TCP Connections	Specify the number of concurrent TCP connections VTAP can establish. Enter a value between 128 and 2048. The default value is 1024.
Ingress TCP Timeout	Specify the timeout value for an Ingress TCP connection in seconds. Enter a value between 30 and 3600 seconds. The default is 60 seconds. **Note**: If no packets are received within the configured time, the TCP connection will be terminated due to timeout.
Number of Egress TCP Flows	Specify the total number of TCP Flows allocated for tracking non-SBI traffic. Enter a value between: • 1024 and 2000000 for V Series Node of extra-large form factor (total memory ≥ 32GB). • 1024 and 16384 for V Series Node of large form factor (total memory < 32GB). The default value is 4096.
Egress TCP Flow Timeout	Specify the timeout value for an Egress TCP flow in seconds. Enter a

	value between 30 and 7200 seconds. The default is 900 seconds. **Note**: If no packets are received within the configured time, the TCP flow will be terminated due to timeout.
Number of Receiver Threads	Specify the number of receiver threads for processing incoming packets. Enter a value between 1 and 128. The default value is 8.
mTLS Config	
mTLS	Enable or disable mTLS encryption or decryption using the toggle button in mTLS/SSL Monitor Mode.
mTLS key	If mTLS encryption is enabled, select the mTLS key alias for the SSL certificate from the drop-down list. To create key alias click on the Add button beside the textbox. For further details refer to Configure SSL Decrypt.
SCP Config	
FQDN Mapping	Select the alias name created for the uploaded FQDN table CSV file from the drop down or add one by clicking on the Add button.
NF Instance Mapping (Optional)	Select the alias name created for the uploaded NFID table CSV file from the drop down or add one by clicking on the Add button..
User Agent Mapping (Optional)	Select the alias name created for the uploaded User Agent table CSV file from the drop down or add one by clicking on the Add button..
TCP Server Ports	Specify the TCP server port or port range to allow TCP communication between endpoints. Valid port range is between 1 and 65535. **NOTE:** TCP communication is allowed only on the configured ports.
SCP Advanced Config	
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
Timestamp	Select the required timestamp used to save the Egress PCAPs., The available timestamps are: • Remote • Local **Note**: Timestamp option will be disabled if the Packet capture level is set to None.
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None

Download Logs - 5G-Cloud application

You can view the log files of a V Series Node or download them as .CSV or .txt files.

To download the log files to a local environment:

1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and go to **TRAFFIC PROCESSING** tab. On the **cloud5g** application, click the ⋮ menu button and select **Details**. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. Select the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download > Files**. The system downloads the selected files to your local environment.

Add CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field
3. From the Type drop-down list, select **5G-Cloud FQDN**.
4. Click **Choose File** in the **FileName** field to upload the CSV file into GigaVUE-FM. Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.

Notes - Header details of the CSV file:

FQDN Mapping: gigamon@vseries:/var/log/cloud5g_tabledir$ cat FQDN.txt

- **Header Details:**
  FQDNid,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation,IMSIP,IMSIntfName,IMSMask,IMSType
- **Example:**
  s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,170.00.13.187,,8080,,SCP,plolp,2000:4000:124:a0d9:ac1:4::,92,303 314 315,sbc

The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional.

The fields imsipaddress, imsinterfacename, imsmask and imstype are applicable only when the Integrated solution Vendor is "Nokia HEP3".

5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

FHA Dashboards for 5G-Cloud Applications

After configuring the 5G-Cloud application, you can monitor the statistics for Nokia HEP3 by the reports displayed in the Dashboard. To access the details, refer to FHA Dashboards for 5G-Cloud Applications.

5G Cloud Nokia HEP3 Support (SBI)

NOTE: CMM Solution is now available as an Early Access feature, giving you the opportunity to explore its capabilities before the general availability (GA).

Nokia 5G network functions use the HEP3 binary format to encode and send packets. HEP3 supports both HTTP2 and TCP protocols, enabling efficient traffic transmission across core network functions. This solution supports traffic processing from Nokia Cloud Mobility Manager (CMM), and the Service Communication Proxy (SCP).

Cloud Mobility Manager (CMM) includes AMF and MME network functions. It generates both Service-Based Interface (SBI) and non-SBI traffic and sends it over HTTP2. The gvHTTP2 application receives CMM traffic and forwards it to the 5G Cloud application, which synthesizes SBI and non-SBI payloads into L2GRE/VXLAN packets before sending them to probes. This approach provides extended visibility across 5G core interfaces and enables operators to monitor both SBI and non-SBI traffic seamlessly.

How Nokia HEP3 Solution works

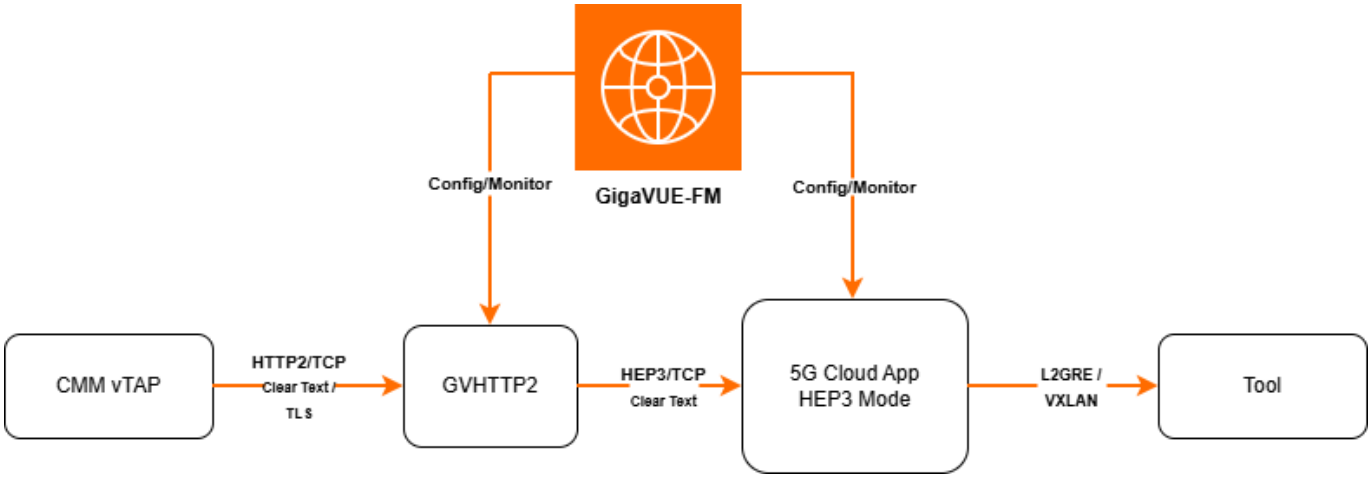
Nokia vTAP systems in the mobility core send HEP3 data over both HTTP2 and TCP. The system supports traffic from the network functions:

- 5G-Cloud Oracle and Nokia SCP Support
- Nokia CMM Solution

Nokia CMM Solution

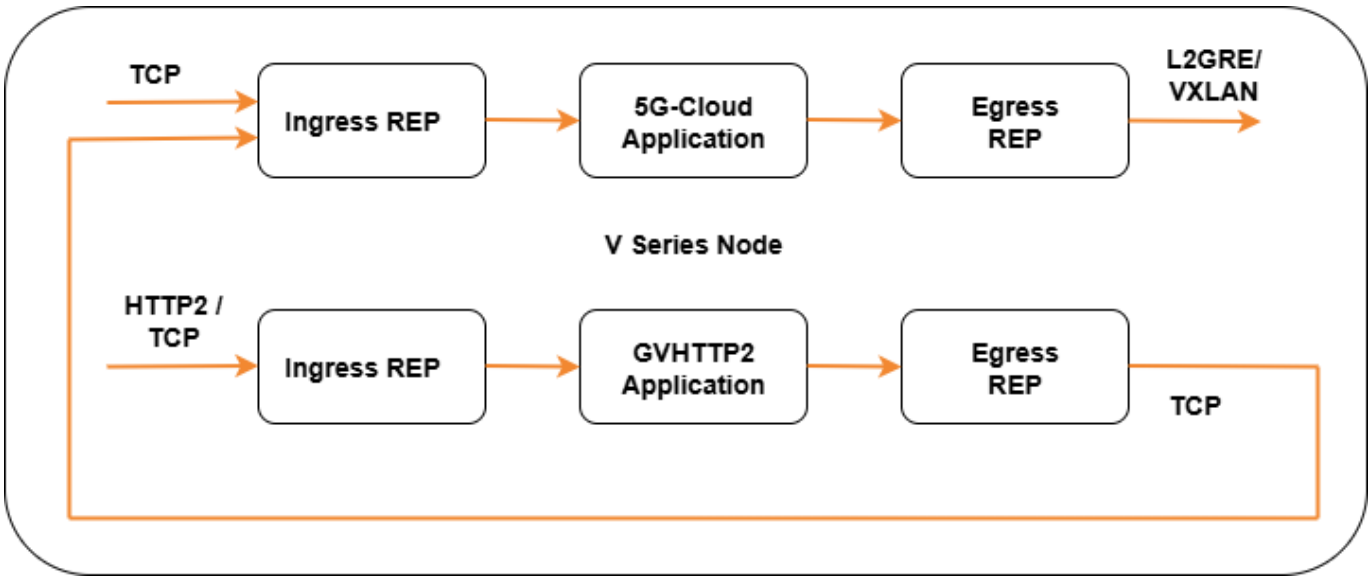
NOTE: CMM Solution is now available as an Early Access feature, giving you the opportunity to explore its capabilities before the general availability (GA).

The following image shows the ingress and egress data flow through the V Series Node for Nokia HEP3 solution.



The Cloud Mobility Manager (CMM) function includes key control-plane elements such as AMF and MME. CMM generates both SBI and non-SBI traffic, making it central to mobility management in the 5G Core.

- CMM vTAPs sends traffic HEP3 over HTTP/2 in stream mode. This traffic is transmitted as HTTP2 over TCP, encrypted either in cleartext or TLS.
- Further the GVHTTP2 V Series Node transmits all processed traffic to the 5G-Cloud VM using HEP3 over TCP.
- Next the traffic is tunneled using L2GRE/VXLAN to the probe.
- The GigaVUE-FM provides configuration and monitoring.



Configure Nokia HEP3 in 5G-Cloud Application

Pre-requisite:

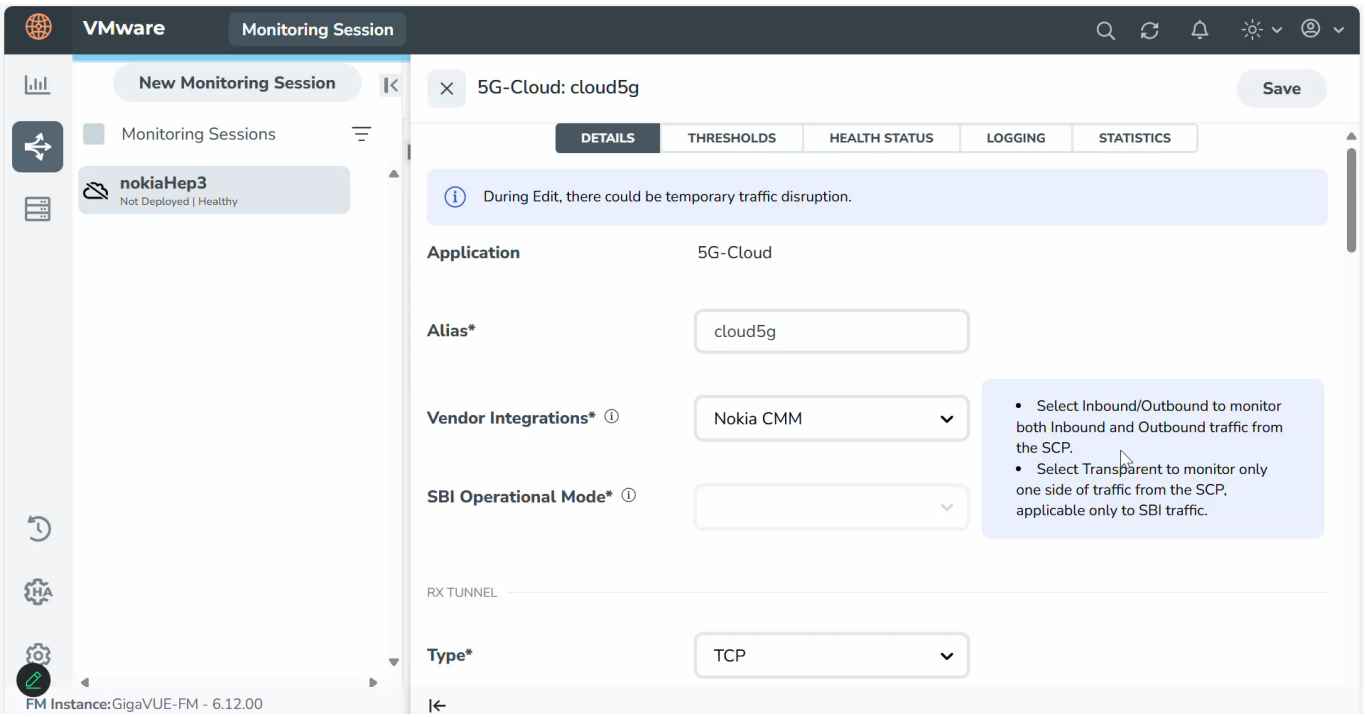
- You must upload CSV files containing a valid FQDN and a valid IPv4/IPv6 address. Refer to Add CSV file for IP Mapping.

You can add a 5G-Cloud application to:

- **New Monitoring Session** - Add the 5G-Cloud application after creating a new Monitoring Session and when the GigaVUE-FM canvas appears. Refer to Create a Monitoring Session section in the respective GigaVUE Cloud Suite Deployment Guide.
- **Existing session** - Select any existing Monitoring Session and go to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas appears.

To add a 5G-Cloud application:

1. In the canvas, drag and drop the 5G-Cloud application and select **Details**. The 5G-Cloud quick view appears.



2. On the application quick view, enter or select the required information as described in the Configuration of 5G-Cloud Application for CMM vTAP.

NOTE: It is recommended to maintain a 60-90 second delay when undeploying and deploying a Monitoring Session in GigaVUE-FM.

Configuration of 5G-Cloud Application for CMM vTAP

Field	Description
Application	The name **5g-Cloud** appears by default.

Alias	Enter the alias name as **cloud5g**.
Vendor Integrations	From the drop-down list, select **Nokia CMM** .
SBI Operational Mode	The Operational Mode will be grayed out on selecting Nokia CMM/IMS.
RX Tunnel	
Type	Specify the tunnel type. The default is TCP.
Listening IP	Specify the tunnel's local listen IP address to receive the packet.
Listening Port	Specify the tunnel's local listening port to bind to receive the packet. The application will listen to the traffic coming to the specified port. Enter a value between 1 and 65535.
Source Port	Specify the tunnel destination port from where the packets will be sent. Enter a value between 1 and 65535.
TX Tunnel	
Type	Specify the tunnel type. The available tunnel types are: • VXLAN • L2GRE
Tool IP	Specify the remote IP address to send the packet.
Destination Port	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
VNI Id **(Applicable only when the selected tunnel type is VXLAN**)	Specify the VNI to use for the VXLAN traffic. Enter a value between 0 and 16777215.
L2GRE Key **(Applicable only when the selected tunnel type is L2GRE**)	Specify the key for the L2GRE tunnel type. Enter a value between 0 and 4294967295.
Advanced Setting	
Tool MTU	Specify the tool port MTU. **Note**: For V Series Node version 6.8.00 and above, the range should be between 1400 and 8800. The default value is 8800. For V Series Node version below 6.8.00, range should be between 1500 and 8800. The default value is 8800.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug
HEP3 Config	

Number of Ingress TCP Connections	Specify the number of concurrent TCP connections VTAP can establish. Enter a value between 128 and 2048. The default value is 1024.
Ingress TCP Timeout	Specify the timeout value for an Ingress TCP connection in seconds. Enter a value between 30 and 3600 seconds. The default is 60 seconds. **Note**: If no packets are received within the configured time, the TCP connection will be terminated due to timeout.
Number of Egress TCP Flows	Specify the total number of TCP Flows allocated for tracking non-SBI traffic. Enter a value between: • 1024 and 2000000 for V Series Node of extra-large form factor (total memory ≥ 32GB). • 1024 and 16384 for V Series Node of large form factor (total memory < 32GB). The default value is 4096.
Egress TCP Flow Timeout	Specify the timeout value for an Egress TCP flow in seconds. Enter a value between 30 and 7200 seconds. The default is 900 seconds. **Note**: If no packets are received within the configured time, the TCP flow will be terminated due to timeout.
Number of Receiver Threads	Specify the number of receiver threads for processing incoming packets. Enter a value between 1 and 128. The default value is 8.
Number of Egress SCTP Flows	Specify the total number of SCTP flows allocated to track Non-SBI traffic. The valid range is from 128-2000000. The default value is 1024.
Egress SCTP Flow Timeout	Specifies the timeout value for an Egress SCTP flow. Valid value range is 30 to 7200 seconds. The default value is 900 seconds. **Note**: If no packets are received within the configured time, the SCTP flow will be terminated due to timeout.
mTLS Config	
mTLS	Enable or disable mTLS encryption or decryption using the toggle button in mTLS/SSL Monitor Mode.
mTLS key	If mTLS encryption is enabled, select the mTLS key alias for the SSL certificate from the drop-down list. To create key alias click on the Add button beside the textbox. For further details refer to Configure SSL Decrypt.
SCP Config	
FQDN Mapping	Select the alias name created for the uploaded FQDN table CSV file from the drop down or add one by clicking on the Add button.
NF Instance Mapping (Optional)	Select the alias name created for the uploaded NFID table CSV file from the drop down or add one by clicking on the Add button..
User Agent Mapping (Optional)	Select the alias name created for the uploaded User Agent table CSV file from the drop down or add one by clicking on the Add button..
TCP Server Ports	Specify the TCP server port or port range to allow TCP communication between endpoints. Valid port range is between 1 and 65535. **NOTE:** TCP communication is allowed only on the configured ports.

SCP Advanced Config	
Packet Capture Level	Select the packet capture level from the drop-down list: • All • Receive • Transmit • None
Timestamp	Select the required timestamp used to save the Egress PCAPs., The available timestamps are: • Remote • Local **Note**: Timestamp option will be disabled if the Packet capture level is set to None.
5G-Cloud Log Level	Select the required 5G-Cloud CSV log level from the drop down list. The default value is None. • All • Flow • Message • Transaction • None

Configuration of GvHTTP2 Application for CMM vTAP

Field	Description
Application	The name **gvhttp2** appears by default.
Alias	Enter the alias name as **gvhttp2**.
Vendor Integrations	From the drop-down list, select **Nokia CMM**.
HTTP2 Listening IP	Specify the HTTP2 IP address. The application will listen to the traffic on the specified IP address.
HTTP2 Listening Port	Specify the HTTP2 Port. The application will listen to the traffic on the specified port.
Max Stream	Specify the maximum number of concurrent streams in one HTTP2 session. Enter a value between 1 and 100. The default value is 100.
Worker Thread	Specify the number of parallel threads that can be sued to process the requests. Enter a value between 1 and 16. The default value is 1.
TX Tunnel	
Type	Specify the tunnel type as Nokia HEP3 over TCP from the dropdown for Nokia CMM.
Source IP	Specify the source IP address to use when sending the packet.
Source Port	Specify the tunnel source port to bind when sending the packet. Enter a value between 1 and 65535.
Destination IP	Specify the tunnel destination port to which the packet will be sent. Enter a value between 1 and 65535.
Destination Port	Specify the tunnel destination port to which the packet will be sent.

	Enter a value between 1 and 65535.
Number of Egress TCP Connections	Specify the number of concurrent TCP connections GvHTTP2 can establish. Enter the value from 1 to 200. The default value is 4.
TLS Config	
TLS	Enable or disable TLS encryption or decryption using the toggle button.
Server Private key	Enter the path where the private key is stored.
Server Certificate	Enter the path where the certificate is stored.
Advanced Setting	
CSV	Enable this option to capture all stats counters for GvHTTP2.
PCAP	Enable this option to capture the packets at egress.
Log Directory	Specify the path to store the log files.
Log Level	Select the severity log level of the events from the following options: • None • Fatal • Error • Notification • Information • Debug

Download Logs - 5G-Cloud / GvHTTP2 Application

You can view the log files of a V Series Node or download them as .CSV or .txt files.

To download the log files to a local environment:

1. Go to **Traffic** > **VIRTUAL** > select your cloud platform.
2. Select the required Monitoring Session and go to **TRAFFIC PROCESSING** tab. On the **cloud5g** / **gvhttp2**application, click the ⋮ menu button and select **Details**. Go to **LOGGING** in the quick view. The **Logging** page displays the logs currently available.
3. Select the required Days, Timestamps, File Name, and Type (TextLog and FlowStats) details.
4. Select the log files to download, and then click **Download > Files**. The system downloads the selected files to your local environment.

Add CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-Apps**. The 5G-Apps Configuration page appears.
2. Click **New**. Enter the name for the CSV file in the **Alias** field
3. From the Type drop-down list, select **5G-Cloud FQDN**.

4. Click **Choose File** in the **FileName** field to upload the CSV file into GigaVUE-FM. Add the CSV file containing a valid FQDN ID and a valid IPv4/IPv6 address for IP mapping.

Notes - Header details of the CSV file:

FQDN Mapping: gigamon@vseries:/var/log/cloud5g_tabledir$ cat FQDN.txt

- Header details: FQDNid,IngressIP1,IngressIP2,IngressPort,EgressIP,NFType,NFLocation,IMSIP,IMSIntfName,IMSMask,IMSType
- Example: s25scp01.scp.5gc.mnc003.mcc525.3gppnetwork.org,170.00.13.187,,8080,,SCP,plolp,2000:4000:124:a0d9:ac1:4::,92,303 314 315,sbc

The fields fqdnID and ingressIPAddress1 are mandatory. All other fields are optional.

The fields imsipaddress, imsinterfacename, imsmask and imstype are applicable only when the Integrated solution Vendor is "Nokia HEP3".

5. Click **Validate** to validate the CSV file.
6. Click **Save** to add the CSV file.

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 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.

Appendix - Casa vTap Statistics

This section provides the stats details for GVHTTP2 and 5G-Cloud applications. For more information on counter details, refer to the respective application on the GigaVUE API Reference page.

NOTE: Currently, the following stats are not supported in GigaVUE-FM. You should login to the corresponding V Series Node to execute the commands.

GVHTTP2 Application

The following table provides information on the counter details and their usage for the GVHTTP2 application:

S.No	Counter Name	Counter Description
1	http2TransactionsSuccessful	Total HTTP2 Transaction successes that occurred in the GVHTTP2 Server.
2	http2StreamInitializeCount	Total HTTP2 New Streams that have been observed by the GVHTTP2 Server.
3	http2StreamCloseCount	Total HTTP2 Streams that have been successfully completed by the GVHTTP2 Server.
4	http2StreamPrepareResponseCount	Total calls to ask GVHTTP2 to prepare a response for inbound stream transactions.
5	http2StreamOnHeaderCount	Total calls to GVHTTP2 when a header value for a given stream has been observed.
6	http2StreamOnDataChunkCount	Total calls to GVHTTP2 when a data chunk for a given stream has been observed.
7	http2StreamOnRecvFrameCount	Total calls to GVHTTP2 when Receive Frame has occurred for any HTTP2 frame.
8	http2StreamOnRecvFrameEndStreamCount	Total calls to GVHTTP2 when the last HTTP2 Frame has been received indicating that the end of the stream has occurred.
9	http2GETRequests	Total HTTP2 GET Requests received by the GVHTTP2 Server.
10	http2POSTRequests	Total HTTP2 POST Requests received by the GVHTTP2 Server.
11	http2PUTRequests	Total HTTP2 PUT Requests received by the GVHTTP2 Server.
12	http2OtherRequests	Total HTTP2 Requests not GET, POST, or PUT received by the GVHTTP2 Server.

S.No	Counter Name	Counter Description
13	http2ValidURI	Total HTTP2 Requests that have valid PATH for the current GVHTTP2 Mode.
14	http2NewSessions	Total TCP Sessions newly initiated by Client applications connecting to the GVHTTP2 Server.
15	http2TerminateSessions	Total TCP Sessions that have been terminated by the Client applications connecting to the GVHTTP2 Server.
16	http2OpenSessions	Total TCP Open / Accept Sessions received by Client Applications connecting to the GVHTTP2 Server.
17	http2CloseSessions	Total TCP Sessions that have closed either by Client Applications or GVHTTP2 Server.
18	vxlanTXPackets	Total number of packets that have been successfully transmitted to the VXLAN TX Tunnel.
19	vxlanTXBytes	Total number of bytes that have been successfully transmitted to the VXLAN TX Tunnel.
20	vxlanThreadCount	Total number of thread cycles that occurred during the interval.
21	http2TransactionsFailed	Total HTTP2 Transaction failures that occurred in the GVHTTP2 Server.
22	http2StreamTimeouts	Total times when the start of a new HTTP2 Stream has occurred but is not completed within the predefined timeout.
23	http2StreamHeaderOverflows	Total events where header has been received, but there is no space in the GVHTTP2 server code to accept the Header Value.
24	http2StreamBufferOverflows	Total events where data frames have been received, but there is no space in the GVHTTP2 server code to accept the data frame.
25	http2InvalidURI	Total HTTP2 Requests that have invalid PATH for the current GVHTTP2 Mode.
26	http2SSLConnectionFailures	Total SSL Connection Failures that occur when the GVHTTP2 Server receives a TCP Connection but fails SSL negotiation.
27	http2SocketFailures	Total Socket Failures either in mTLS or Clear Text mode.
28	vxlanTXSocketSendErrors	Total number of packets that could not be transmitted to the VXLAN TX Tunnel because of socket error.
29	vxlanTXSocketSizeErrors	Total number of packets that could not be transmitted to the VXLAN TX Tunnel because the size of the packet is too large.
30	vxlanThreadTimeouts	Total number of calls to select that timed out

S.No	Counter Name	Counter Description
		waiting for received data. This is not an error.
31	vxlanRXPackets	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the VXLAN thread.
32	vxlanRXBytes	Total number of RX Bytes received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the VXLAN thread.
33	vxlanRXDrops	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been dropped by the VXLAN thread because there are no more RX descriptors in the ingress queue of the VXLAN thread.
34	vxlanRXOversized	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that the VXLAN thread has dropped because the RX message size is too large.
35	vxlanQueueCurrBufferIn	Buffer index of the queue slot for a current packet to be inserted into the VXLAN Thread RX Queue.
36	vxlanQueueCurrBufferOut	Buffer index of the queue slot for a current packet to be removed from the VXLAN Thread RX Queue.
37	vxlanQueueNumBuffers	Total number of buffers in the VXLAN RX Queue.
38	vxlanQueueMaxQueueSize	Total number of packets that were in the VXLAN RX Queue during the current interval.
39	vxlanQueueBufferSize	Size of each RX Packet buffer in the VXLAN RX Queue.
40	vxlanQueuePacketsQueuedIn	Total number of packets that have been put into the VXLAN RX Queue.
41	vxlanQueuePacketsQueuedOut	Total number of packets that have been removed from the VXLAN RX Queue.
42	vxlanQueuePacketsQueuedFull	Total number of packets that attempted to be queued when the VXLAN RX Queue was full.
43	nghttp2Errors	Total errors that occur within the nghttp2 library used by the GVHTTP2 server application.
44	pcapRXPackets	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been created in the PCAP thread.
45	pcapRXBytes	Total number of RX Bytes received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have

S.No	Counter Name	Counter Description
		been created in the PCAP thread.
46	pcapRXDrops	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that have been dropped by the PCAP thread because there are no more RX descriptors in the ingress queue of the PCAP thread.
47	pcapRXOverSized	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that the PCAP thread has dropped because the RX message size is too large.
48	pcapRXErrors	Total number of RX Packets received from inbound HTTP2 Stream transactions received by the GVHTTP2 server from the Client VTAP that the PCAP thread has dropped because of an error.
49	pcapQueueCurrBufferIn	Buffer index of the queue slot for a current packet to be inserted into the PCAP Thread RX Queue.
50	pcapQueueCurrBufferOut	Buffer index of the queue slot for a current packet to be removed from the PCAP Thread RX Queue.
51	pcapQueueNumBuffers	Total number of buffers in the PCAP RX Queue.
52	pcapQueueMaxQueueSize	Total number of packets that were in the PCAP RX Queue during the current interval.
53	pcapQueueBufferSize	Size of each RX Packet buffer in the PCAP RX Queue.
54	pcapQueuePacketsQueuedIn	Total number of packets that have been put into the PCAP RX Queue.
55	pcapQueuePacketsQueuedOut	Total number of packets that have been removed from the PCAP RX Queue.
56	pcapQueuePacketsQueuedFull	Total number of packets that attempted to be queued when the PCAP RX Queue was full.
57	pcapFiles	Total number of PCAP Files written during this interval.
58	pcapOpenErrors	Total number of file errors that occurred while trying to create new PCAP Files during this interval.
59	pcapWriteErrors	Total number of file errors that occurred while trying to write data to PCAP Files during this interval.
60	pcapFlushErrors	Total number of file errors that occurred while trying to flush cached data to PCAP Files during this interval.
61	pcapCloseErrors	Total number of file errors that occurred while

S.No	Counter Name	Counter Description
		trying to close PCAP Files during this interval.
62	pcapPackets	Total number of PCAP Packets written during the interval.
63	pcapBytes	Total number of PCAP Bytes written during the interval.
64	diskLoggingThreadTimeouts	Total number of calls to delay waiting to receive data in the PCAP file thread. This is not an error.
65	diskLoggingThreadCount	Total number of thread cycles that occurred during the interval.

5G-Cloud Application

The following table provides information on the counter details and their usage for the 5G-Cloud application:

S.No	Counter Name	Counter Description
1	rxPkts	Total number of RX Packets / Messages from the GVHTTP2 Application.
2	txPkts	Total number of packets that have been successfully transmitted to the UDPGRE TX Tunnel.
3	rxPktBytes	Total number of RX Bytes for messages from the GVHTTP2 Application.
4	txPktBytes	Total number of bytes that have been successfully transmitted to the UDPGRE TX Tunnel.
5	rxDrops	Total number of RX Packets received from inbound VXLAN Tunnel by the 5G-Cloud Application from the GVHTTP2 Server APP that have been dropped by the PCAP thread because there are no more RX descriptors in the ingress queue of the PCAP thread.
6	txDrops	Total number of Tx Packets that have been dropped by the 5G-Cloud APP because there are no more RX descriptors in the egress queue.
7	rxThreadCount	Total number of receive thread cycles that occurred during the interval.
8	txThreadCount	Total number of Transmit thread cycles that occurred during the interval.
9	rxSelectTimeouts	Total number of calls to select that timed out

S.No	Counter Name	Counter Description
		waiting for received data. This is not an error.
10	txThreadTimeout	Total number of calls to egress Queue (Timed Semaphore wait) that timed out waiting for received data. This is not an error.
11	rxIPv4Pkts	Total number of IPv4 Packets received by the 5G-Cloud Application (this counter is not used currently).
12	rxIPv6Pkts	Total number of IPv6 Packets received by the 5G-Cloud Application (this counter is not used currently).
13	rxTcpPkts	Total number of TCP Packets received by the 5G-Cloud Application (this counter is not used currently).
14	rxNonTcpPkts	Total number of Non-TCP Packets received by the 5G-Cloud Application (this counter is not used currently).
15	rxVlanPkts	Total number of VLAN Packets received by the 5G-Cloud Application (this counter is not used currently).
16	rxPktsTooShort	Total Number of Incomplete Packets received by the 5G-Cloud Application (this counter is not used currently).
17	rxSelectNoEvents	Total Number of Errors while reading the packet data from the ingress Socket.
18	rxOversizedBuffers	Total number of RX Packets received by the 5G-Cloud Application from the GVHTTP2 Server that have been dropped because the RX message size is too large.
19	rxRecvFromNonCritical	Total number of socket timeout (timed out without Receiving any packet) for the ingress Interface.
20	rxErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of an error in Processing the Packet.
21	rxProtocolIDErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of error in IP Protocol ID (this counter is used only when L2GRE is used as ingress Tunnel Type hence it is not used currently).
22	rxIPProtocolErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of an error in IP Protocol (this counter is used only when L2GRE is used as ingress Tunnel Type; hence, it is not used currently).

S.No	Counter Name	Counter Description
23	rxIPPayloadLengthErrors	Total number of Rx Packets dropped by the 5G-Cloud Application because of an error in IP payload length (this counter is not used currently).
24	txSocketErrors	Total number of packets that could not be transmitted to the UDPGRE TX Tunnel because of socket error.
25	elPkts	Total number of Packets successfully written into the log files.
26	elFiles	Total number of files opened successfully to log the packets.
27	elErrors	Total number of errors while opening the file to write the packets.

Appendix-5G Cloud Nokia HEP3 Support (SBI)

The following table provides information on the counter details and their usage for the 5G-Cloud application:

S.No	Counter Name	Counter Description
1	sslAccept	Total TCP Open / Accept Sessions received by Client Applications connecting to the Server.
2	sslAcceptSSLPending	Total number of times SSL Connection is temporary suspension of the handshake, awaiting further action from the application's client hello callback.
3	sslAcceptSSLWantedRead	Total number of times SSL Connection needs to read more data from the network to proceed, but no data is currently available for reading.
4	sslAcceptSSLWantWrite	Total number of times there was error in writing complete data to the socket.
5	sslAcceptSSLAcceptFailure	Total number of times a new SSL connection is not accepted because of certificate, protocol or other errors.
6	sslRecvSuccess	Total number of times a new SSL connection has been accepted successfully.
7	sslRecvBytes	Total number of RX Bytes received from the vTAP in SSL Mode.
8	sslRecvSSLPending	Total number of times SSL Connection

S.No	Counter Name	Counter Description
		establishment is which indicates that TLS handshake routine is interrupted by client hello callback.
9	sslRecvSSLWantRead	Total number of times read operation is retried when data is available for reading.
10	sslRecvSSLWantWrite	Total number of times write operation is retried when data is available for writing.
11	sslRecvSSLReadFailures	Total number of times TLS/SSL connection has been closed cleanly by the peer while handshake is in progress.
12	sslBadCert	Total number of times there is error in establishing SSL connection with client because certificates are rejected by the peer.
13	sslCertVerifyFailure	Total number of times where client attempting to establish a secure connection (using SSL/TLS) with a server could not verify the server's SSL certificate.
14	sslUnknownProtocol	Total number of times there is error in establishing SSL connection with client because when the server cannot recognize or negotiate SSL/TLS protocol version.
15	sslHandshakeFailure	Total number of times there is error in establishing SSL connection with client because Handshake could not negotiate a cipher/protocol.
16	sslAlertUnknownCA	Total number of times there is error in establishing SSL connection with client because Certificate authority not recognized.
17	sslNoSharedCipher	Total number of times there is error in establishing SSL connection with client because no cipher overlap with peer.

Slicing

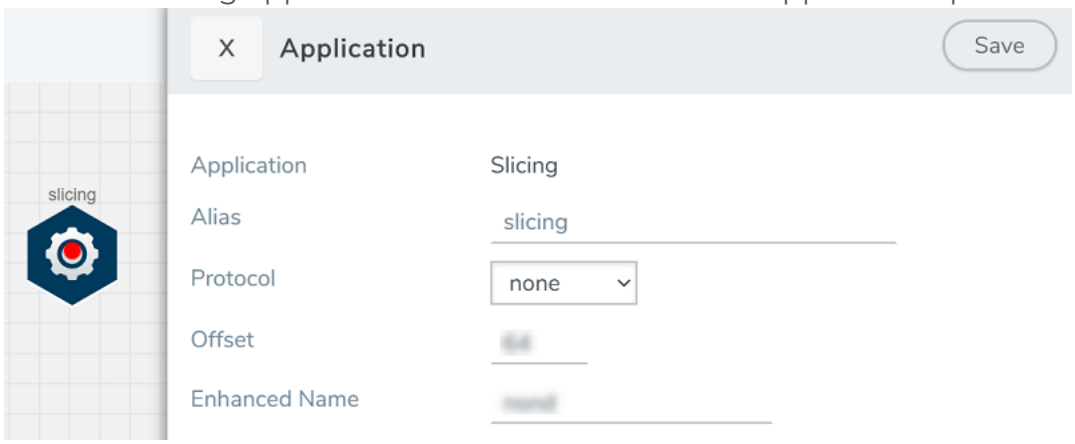
Packet Slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead of storing full packet data.

Packets can have multiple variable-length headers, depending on where they are captured, the different devices that have attached their own headers along the way, and the protocols in use (for example, IPv4 versus IPv6). Because of this, slicing operations with a hard-coded offset will not typically provide consistent results.

To address this, the Slicing application lets you configure Packet Slicing using protocols that allow you to start slicing from a particular number of bytes after a specific packet header (IPv4, IPv6, UDP, and so on). The Slicing application parses through Layer 4 (TCP/UDP) to identify the headers in use, slicing based on the variable offset identified for a particular header instead of a hard-coded number of bytes.

To add a Slicing application:

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



3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the application.
Protocol	The following are the protocols that you can select for from the protocol drop-down list: o **None** –Slice starting a specific number of bytes from the start of the packet. o **IPV4** – Slice starting a specified number of bytes after the IPv4 header. o **IPV6** – Slice starting a specified number of bytes after the IPv6 header. o **UDP** – Slice starting a specified number of bytes after the UDP header. o **TCP** – Slice starting a specified number of bytes after the TCP header. o **FTP** – Identify using TCP port 20 and slice payloads using offset from the TCP header. o **HTTPS** – Identify using TCP port 443. Slice encrypted payloads using offset from the TCP header. o **SSH** – Identify using TCP port 22. Slice encrypted payloads using offset from the TCP header. The Slicing application can provide slicing for GTP tunnels, provided the user payloads are unencrypted. Both GTPv1 and GTPv2 are supported – GTP' (GTP prime) is not supported. Keep in mind that only GTP-u (user plane packets) are sliced. Control plane packets (GTP-c) are left unmodified because of their importance for analysis. o **GTP** – Slice starting a specified number of bytes after the outer GTP header. o **GTP-IPV4** – Slice starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. o **GTP-UDP** – Slice starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. o **GTP-TCP** – Slice starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specify the length of the packet that must be sliced.

4. Click **Save**.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

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)