



GigaVUE-FM User Interface Guide

GigaVUE-FM

Product Version: 6.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

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

Trademark Attributions

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

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

Change Notes

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

Product Version	Document Version	Date Updated	Change Notes
6.14	1.0	02/25/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE-FM User Interface Guide	1
Change Notes	3
Contents	4
GV-FM-User-Interface-Guide	8
GigaVUE-FM	8
GigaVUE-FM	9
Supported Cloud Environments	10
Get Started with GigaVUE-FM	11
GigaVUE-FM Features and Benefits	11
Supported Nodes	13
Device and Configuration Management	14
How to enable Web Server for Node Management	16
Supported Browsers for GigaVUE-FM	16
Log In to GigaVUE-FM	16
Log Out of GigaVUE-FM	17
Explore GigaVUE-FM Interface	17
Homepage	17
Left Navigation Pane	18
Top Navigation Bar	18
Page-Level Header	19
GigaVUE-FM GUI Navigation	20
Footer	20
Theme Settings	20

Configure a Custom Banner	21
Quick Views	21
Recently Viewed	21
Find Pages	22
Return to the Dashboard	23
Table View Customization	23
Dashboard	25
Physical and Virtual Dashboard	25
Overview of the Physical and Virtual Dashboard	26
Physical Dashboard Profiles	26
Physical Dashboard Quick Views	28
Telemetry Insights Dashboard	28
Prerequisites	29
Executive Health Summary	29
Operational Summary	29
Recommended actions	30
View the Telemetry Insight dashboard	31
Rules and Notes	31
Physical Dashboard Widgets	31
Highest Traffic	32
Lowest Traffic	35
Traffic Comparison By Tags	36
Most Utilized Traffic	40
Least Utilized Traffic	43
Inventory	44
Nodes by Model	44
Nodes by Software Version	45
Status Summary	47
Nodes' Status Summary	47
Port Link Status Summary	48
Unhealthy Maps	49
Unhealthy Flows	50
Port Drops and Errors	50
Unhealthy Fabric Maps	53
Audit Logs	53
Events	56

GigaVUE-FM Health Dashboard	59
Overview of GigaVUE-FM Health Dashboard	60
CPU Utilization	61
Memory Utilization	61
Storage Utilization	62
Alarm Thresholds and Notifications	63
What Next?	63
How to Add the GigaVUE-FM Instance Name	63
Notifications Panel	64
Long-term Notifications	65
Notification Type Icons	65
Notification Banners	66
Notification Banners for Disk Space Utilization	66
How to Search in GigaVUE-FM	68
Performing a Search	70
Search Examples	71
Search Maps	72
Example 1: Search for a Map by Alias	72
Example 2: Search for a Map with an IP Address	73
Example 3: Search for a Map with a MAC Address	75
Example 4: Search for Maps with Down Ports	75
Search for Roles and Users	76
Example 1: Search for Monitor Role	76
Example 2: Search for a User	78
Search Ports	79
Example 1: Search for Down Ports	79
Example 2: Search for Port Details of Devices Managed by GigaVUE-FM	80
Example 3: Search for Port and Linked Resources Using a Port Alias	81
Filtering Search Results	81
How to Apply Filters	82
Analytics	83
Rules, Notes, and Limitations for Analytics	83
GigaVUE-FM Statistics and Data Roll-up	85
Control Filters in Analytics Dashboards	85

Get Started with Analytics UI	86
Work with the Analytics User Interface	89
Share	89
Clone	90
Reporting	90
Set as Default	90
Filter Data Using Tags in Control Filters	90
Search Data	93
Visualizations	93
View System Visualization	93
Create Custom Visualizations	94
Create a Visualization	94
Clone a Visualization	97
Visualizations - Example Work Flows	97
TSVB Chart Displaying Traffic Trend	97
Pie Chart Displaying Alarms Summary	99
Metric Displaying Card Count	101
Bar Chart for Alarms by Severity	102
Dashboards	104
Clone Dashboard	105
Create New Dashboard	106
Edit Dashboard	109
Reports	110
Discover	112
Filter	114
Save Search	114
Find Data	115
Default Dashboards	115
Dashboard	130
Dashboards for Volume-based Licenses Usage	131
Virtual Inventory Statistics and Cloud Applications	
Dashboard	134
Rules and Notes	140
FHA Dashboards for 5G Applications	140
Overall 5G Apps Dashboard	141
Detailed 5G Apps Dashboard	142
NokiaSCP Statistics	144
OracleSCP Statistics	145

EricssonSCP Statistics	145
NokiaHEP3 Statistics	146
Message Statistics	146
Protocol Statistics	147
Ericsson vTAP Statistics	147
Packet Statistics	147
TCP Statistics	148
GigaSMART Mobility Session and Flow Filtering	
Dashboards	148
How to Access the Dashboards	148
Rules and Notes	152
GigaSMART Inline TLS/SSL Dashboards	152
Basic Dashboards	153
Advanced Dashboards	159
System Requirements	159
Configure Advanced dashboard	160
Rules and Notes	160
OpenSearch Indices and Fields Used in Analytics	163
Deprecated Fields in Analytics	167
Analytics Appendix	168
Ports	168
Dimensions	168
Metrics	168
Maps	169
Dimensions	169
Metrics	170
Map Rule	170
Dimensions	170
Metrics	171
Glossary	172

GV-FM-User-Interface-Guide

GigaVUE-FM

GigaVUE-FM

GigaVUE-FM fabric manager (**GigaVUE-FM**) is a web-based fabric management interface that provides high-level visibility and management of both the physical and virtual traffic visibility nodes that form the Gigamon Traffic Visibility Fabric™. GigaVUE-FM can manage the following types of traffic visibility nodes:

- **Physical GigaVUE Nodes** – GigaVUE-FM manages GigaVUE TA Series, and HC Series nodes, allowing for a unified workspace, while also providing an easy-to-use wizard-based approach for configuring Flow Mapping® and GigaSMART® traffic policies. For a list of GigaVUE TA Series, and HC Series nodes supported for management in this release, refer to [Supported Nodes](#).
- **Virtual GigaVUE Nodes** – GigaVUE-FM also extends the GigaVUE feature set into the virtual space by allowing for the discovery, configuration, and management of the new GigaVUE-VM virtual traffic visibility node. GigaVUE-VM provides powerful Flow Mapping® technology for the traffic flowing between virtual machines, allowing you to distribute cloud-based traffic to physical tool ports in the visibility fabric.

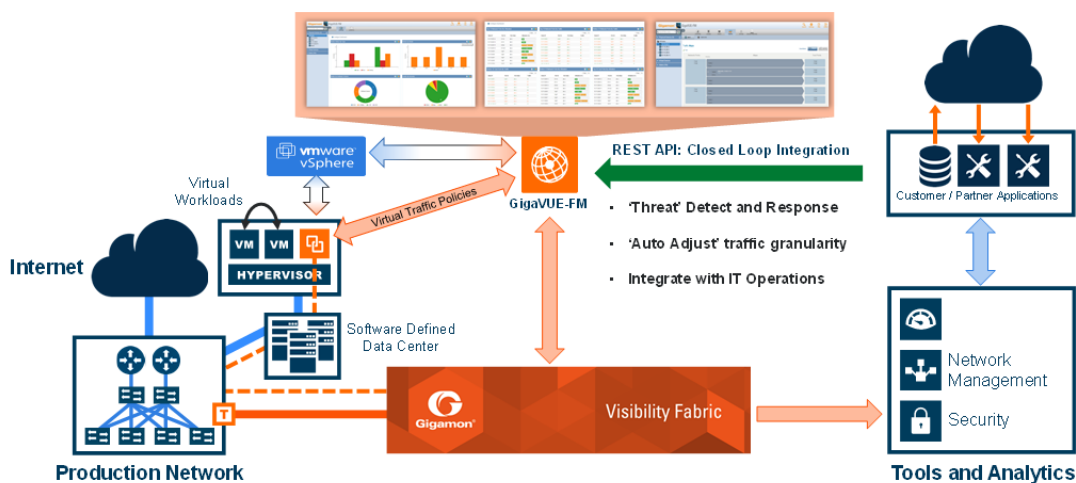


Figure 1 GigaVUE-FM Overview

Learn about:

- how to install and upgrade GigaVUE-FM fabric manager (GigaVUE-FM Installation and Upgrade).
- how to install and upgrade GigaVUE-FM fabric manager using CLI commands ([GigaVUE-FM CLI Commands](#)).
- how to get started with GigaVUE-FM ([Get Started with GigaVUE-FM](#)).
- how to add users, create groups and create roles and other administrative task on GigaVUE-FM ([Administer GigaVUE-FM](#)).
- how to add and manage nodes ([Device and Configuration Management](#), [Supported Browsers for GigaVUE-FM](#)).

- how to manage dashboards ([Get Started with Analytics UI](#), [Analytics](#))
- how to deploy GigaVUE-FM Copilot ([GigaVUE-FM Copilot](#)).

Supported Cloud Environments

The GigaVUE Cloud Suite solution for the various cloud platforms offers network traffic visibility in the respective cloud platforms. The GigaVUE Cloud Suite solutions acquire, optimize and distribute selected traffic to security and monitoring tools. The below table lists the available cloud suites and their respective guides.

Cloud Platform	Guides
Public Cloud	
AWS	GigaVUE Cloud Suite Deployment Guide - AWS GigaVUE Cloud Suite for AWS—GigaVUE V Series 1 Guide
Azure	GigaVUE Cloud Suite Deployment Guide - Azure GigaVUE Cloud Suite for Azure—GigaVUE V Series 1 Guide
Private Cloud	
OpenStack	GigaVUE Cloud Suite for OpenStack—GigaVUE V Series 1 Guide GigaVUE Cloud Suite Deployment Guide - OpenStack
VMware	GigaVUE Cloud Suite Deployment Guide - VMware GigaVUE Cloud Suite for VMware—GigaVUE-VM Guide
Container Visibility	
Kubernetes	GigaVUE Cloud Suite for Kubernetes Container Visibility Configuration Guide
Gigamon Containerized Broker	Gigamon Containerized Broker Deployment Guide
Universal Container Tap	Universal Cloud TAP - Container Deployment Guide
Other Cloud Platforms	
Third party Orchestration	GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Nutanix	GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide

The guides provide instructions on configuring the GigaVUE Cloud components and setting up traffic monitoring sessions for the respective Cloud platform.

Get Started with GigaVUE-FM

GigaVUE-FM fabric manager is a web-based fabric management interface that provides high-level visibility and management of both the physical and virtual traffic visibility nodes that form the Gigamon Traffic Visibility Fabric™. GigaVUE-FM can manage the following types of traffic visibility nodes:

It includes the following major sections:

- [Log In to GigaVUE-FM](#)
- [Log Out of GigaVUE-FM](#)
- [Explore GigaVUE-FM Interface](#)
- [Configure a Custom Banner](#)
- [Quick Views](#)
- [Return to the Dashboard](#)
- [Table View Customization](#)
- [Notifications Panel](#)
- [How to Add the GigaVUE-FM Instance Name](#)
- [How to Search in GigaVUE-FM](#)

GigaVUE-FM Features and Benefits

The GigaVUE-FM is a web-based management interface that provides unified access, centralized administration, and high-level visibility for all GigaVUE traffic visibility nodes in the enterprise or data center, allowing a global perspective which is not possible from individual nodes.

The following table summarizes the major benefits of GigaVUE-FM:

Table 1: Features and Benefits of GigaVUE-FM

Benefit	Descriptions
Centralized Management and Control	Provides centralized management, monitoring, and configuration of the physical and virtual traffic policies for the Visibility Fabric, allowing administrators to map and direct network traffic to the tools and analytics infrastructure.
Programmable APIs for Software	REST APIs that can be used by the traffic monitoring or IT operations management tools to perform various tasks, such as

Benefit	Descriptions
Defined Visibility	• Improve security through better network detection, reaction, and response by automating NetFlow generation and SSL decryption so that current security appliances are not overtaxed when performing deep packet inspection. • Program the Visibility Fabric flow maps when security threats are detected. • Discover the Visibility Fabric nodes for inventory and status collection. • Performing common tasks, such as provisioning and ticketing of network port configurations. • Programmatically create, update, or delete port properties, including port-type, admin state, speed, and others. • Programmatically create, update, or delete traffic maps and GigaSMART operations. Note: GigaVUE-FM can handle only 150 concurrent (write - POST/PUT/PATCH/DELETE) API requests at any given time.
Fabric-wide reporting	Summarized and customizable dashboards for inventory, node or cluster status, events, audit trail, and Top-N/Bottom-N port/map usage with options to export and schedule HTML or PDF reports for off-line viewing.
Advanced Monitoring	Proactively monitor and troubleshoot hot spots in your Visibility Fabric: • Top-N, Bottom-N Network/Tool Port and Map usage widgets in the dashboard • Global search across the Visibility Fabric for quick access to monitoring hot spots • Audit trail of user operations for enterprise security compliance • Historical trend analysis (1 hour, 1 day, 1 week, 1 month) for port and traffic policies • Quick Views for easy access to Visibility Fabric details (node, port, traffic policies)
Scheduling capabilities	Initiates version updates to one or many fabric nodes to streamline software rollouts in an automated fashion.
Backup and Restore Capabilities	Supports configuration backup and restore across multiple visibility nodes to quickly back-out changes if required due to errors or change control requirements. Note: Restoration of backed up configuration fails in G-Series. Alternatively you can download the file from GigaVUE-FM and use the GigaVUE-OS-CLI to restore the configuration.

Benefit	Descriptions
Improved Operational Efficiencies	Minimizes resources required to configure, manage, and monitor multiple visibility nodes: • Create/Update/Delete port properties including port-type, admin state, speed, and others • Create/Update/Delete traffic maps and GigaSMART operations
Near-Real Time Config Status	Provides Near-Real Time (NRT) status of the following: • Configuration changes performed using GigaVUE-FM APIs: Immediately reflected in the GigaVUE-FM GUI. • State changes occurring in the device (for example, oper up/down changes happening in the device): Immediately reflected in the GigaVUE-FM GUI. • Configuration changes made in the devices (for example, attributes such as 'alias' changed by the user in the device through CLI or API): Get reflected in GigaVUE-FM only after the next config sync cycle, which could be few minutes. Note: ▪ You must enable SNMP traps in GigaVUE-FM for the NRT status updates to get reflected. However, SNMP traps are enabled by default in GigaVUE-FM. Refer to the "SNMP Traps" section in the <i>GigaVUE Administration Guide</i> for more details. ▪ To avoid flooding of alarms, devices implement SNMP throttling. Refer to the "SNMP Throttling" section in the <i>GigaVUE Administration Guide</i>.
Scalability	Provides a reliable and stable environment for managing a large number of physical devices without any impact to the performance. • Vertical Scale: Allows GigaVUE-FM to manage approximately 1000 Nodes. • Horizontal Scale: Allows GigaVUE-FM to manage approximately 3000 Nodes. Horizontal scale support is applicable only in GigaVUE-FM High Availability mode. Horizontal scale support involves service distribution to the standby nodes.

Supported Nodes

GigaVUE-FM provides supports the following GigaVUE Nodes

- GigaVUE TA Series
- HC Series

NOTE: After upgrading to software version 5.15, GigaVUE-FM will no longer support to manage GigaVUE G Series Nodes and all the existing GigaVUE G Series Nodes in GigaVUE-FM will be removed.

GigaVUE-FM provides support for GigaVUE TA Series, and HC Series nodes through the administration of physical nodes (Device Management and Configuration Management) feature.

Topics:

- [Device and Configuration Management](#)
- [How to enable Web Server for Node Management](#)

Device and Configuration Management

During the initial start up of GigaVUE-FM, it performs a discovery on GigaVUE® HC Series and TA Series nodes listed in the table below. It supports the versions listed in the following table. GigaVUE-FM allows you to perform configuration tasks on these devices.

Table 2: GigaVUE-FM Managed GigaVUE Nodes Software Version **GigaVUE HC Series Nodes**

GigaVUE Series	Node	Compatible GigaVUE-OS versions
GigaVUE HC Series Nodes	GigaVUE-HC1	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-HC1-Plus	v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-HC3 CCv2	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-HCT	v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-HC2 CCv1 (End of Sale)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx
	GigaVUE-HC2 CCv2 (End of Sale)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx
	GigaVUE-HC3 CCv1 (End of Support)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx

Table 3: GigaVUE-FM Managed GigaVUE Nodes Software Version **GigaVUE TA Series Nodes**

GigaVUE Series	Node	Compatible GigaVUE-OS versions
GigaVUE TA Series Nodes	GigaVUE-TA25	v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-TA25E	v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-TA200	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-TA200E	v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7.xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-TA400	v5.14xx, v5.15xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx, v6.6.xx, v6.7.xx, v6.8xx, v6.9xx, v6.10xx, v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-TA400E	v6.11.xx, v6.12.xx, v6.13.xx, v6.14.xx
	GigaVUE-TA10 (End of Sale)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx
	GigaVUE-TA40 (End of Sale)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx
	GigaVUE-TA100 (End of Sale)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx, v6.2.xx, v6.3.xx, v6.4.xx, v6.5.xx
	GigaVUE-TA100-CXP (End of Sale)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx, v5.8.xx, v5.9.xx, v5.10.xx, v5.11.xx, v5.12.xx, v5.13.xx, v5.14.xx, v5.15.xx, v5.16.xx, v6.0.xx, v6.1.xx
	GigaVUE-TA1 (End of Support)	v5.4.xx, v5.5.xx, v5.6.xx, v5.7.xx

For more information on GigaVUE-OS that has reached EOS, refer to [Summary of Software release Status for GigaVUE-OS GigaVUE-FM and Cloud-Suite](#).

NOTE: Although GigaVUE-FM may recognize earlier versions of GigaVUE® TA and HC Series nodes, the versions listed in the above table are the officially supported versions. Earlier versions are not managed by GigaVUE-FM.

How to enable Web Server for Node Management

GigaVUE-FM can only discover and manage nodes with their web servers enabled and operating on the default HTTP port of 80. The request from Port 80 is immediately redirected to port 443 (HTTPS) for secure connections over SSL.

Supported Browsers for GigaVUE-FM

GigaVUE-FM supports the following browsers:

OS	Browser	Minimum Browser Version
Windows®	Mozilla Firefox™	143.0.1
	Microsoft Edge	140.0.3485.94
	Google® Chrome®	140.0.7339.208
Mac OSX	Google® Chrome®	140.0.7339.214
	Mozilla Firefox™	143.0.1
	Apple® Safari®	26.0.1
	Microsoft Edge	140.0.3485.94
Linux	Google® Chrome®	137.0.7151.27
	Mozilla Firefox™	138.0.4

Log In to GigaVUE-FM

The GigaVUE-FM login page provides information about the security policy login banner beside the username and password fields. The login banner is customizable. For more information about configuring a custom banner, refer to [Configure a Custom Banner](#).

GigaVUE-FM is preconfigured with one user with the fm_super_admin role assigned (username - admin, password - admin123A!!). The default password (admin123A!!) on the admin account must be changed to a non-default password (as it is no longer allowed to have the default password).



- If GigaVUE-FM is deployed inside AWS or OpenStack then, use the **Instance ID** as the default password.



- If you try to access the GigaVUE-FM internal page URLs (for example Port page `<fmipaddress>/app/#/node/10.115.32.12/ports/ports`) without logging in to GigaVUE-FM, then after logging in, you will be redirected to the Dashboard page and not the specific page that you tried to access.
- When there is a change in the IP address of GigaVUE-FM, the cms server must be restarted. Only when the cms server is restarted, the new IP address will be updated in all the relevant places.
- Log in to GigaVUE-FM once the page appears, as the session is valid for about 15 minutes.

Log Out of GigaVUE-FM

To log out of GigaVUE-FM, click on the user-profile drop-down () icon on the top right of GigaVUE-FM GUI and select **Logout**.

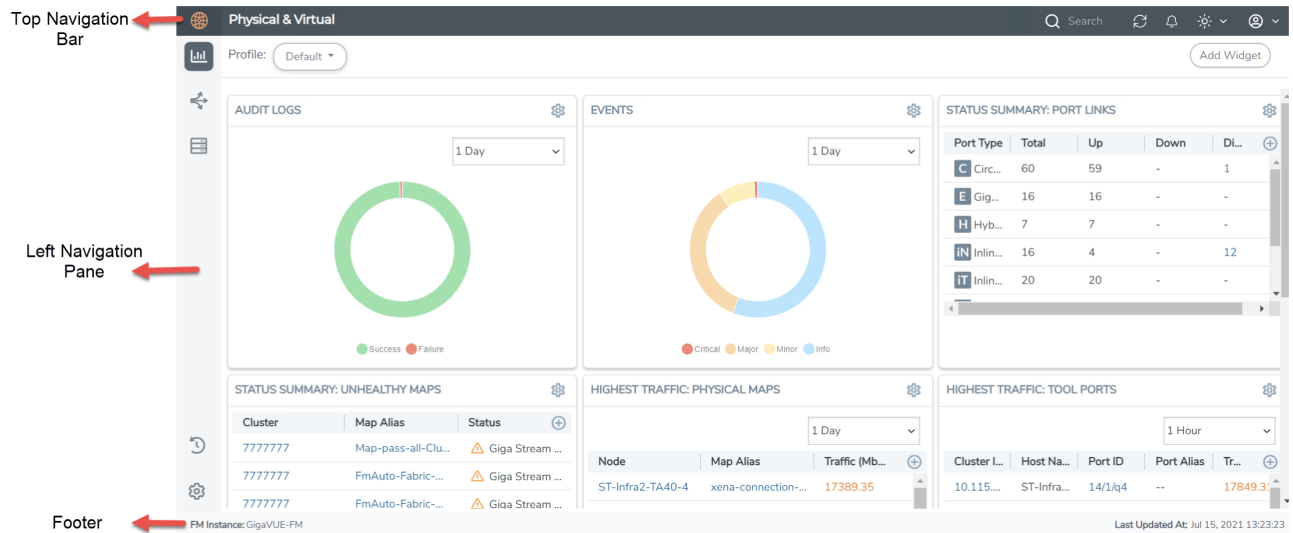
NOTE: You will be automatically logged out of GigaVUE-FM after a period of inactivity (based on the auto-logout time configured). To configure the auto-logout time, refer to the "Preferences" section in the GigaVUE Administration Guide.

Explore GigaVUE-FM Interface

Homepage

When you first log in to GigaVUE-FM, the Dashboard - Physical & Virtual page is displayed by default as shown in the following figure.

NOTE: You can add widget in GigaVUE-FM only if you have an active license.



Left Navigation Pane

The GigaVUE-FM landing page has a left navigation pane that expands into a floating pane which navigates to the following menus :

- **Dashboards**  : Consists of the physical and virtual dashboards, the health monitor dashboards, and the Analytics dashboards. This page also includes the alarms, the events, and the audit logs pages.
- **Traffic**  : Consists of the fabric solutions that the users must configure to monitor the flow of traffic.
- **Inventory**  : Consists of the physical and virtual resources which the users must configure before configuring the traffic flow and solutions.
- **Recently Viewed**  : Displays the list of recently viewed pages. Refer to [Recently Viewed](#) Section for detailed information.
- **Settings**  : Consists of administrative, authentication, system resources that needs to be configured by the user.

Top Navigation Bar

The top navigation bar contains:

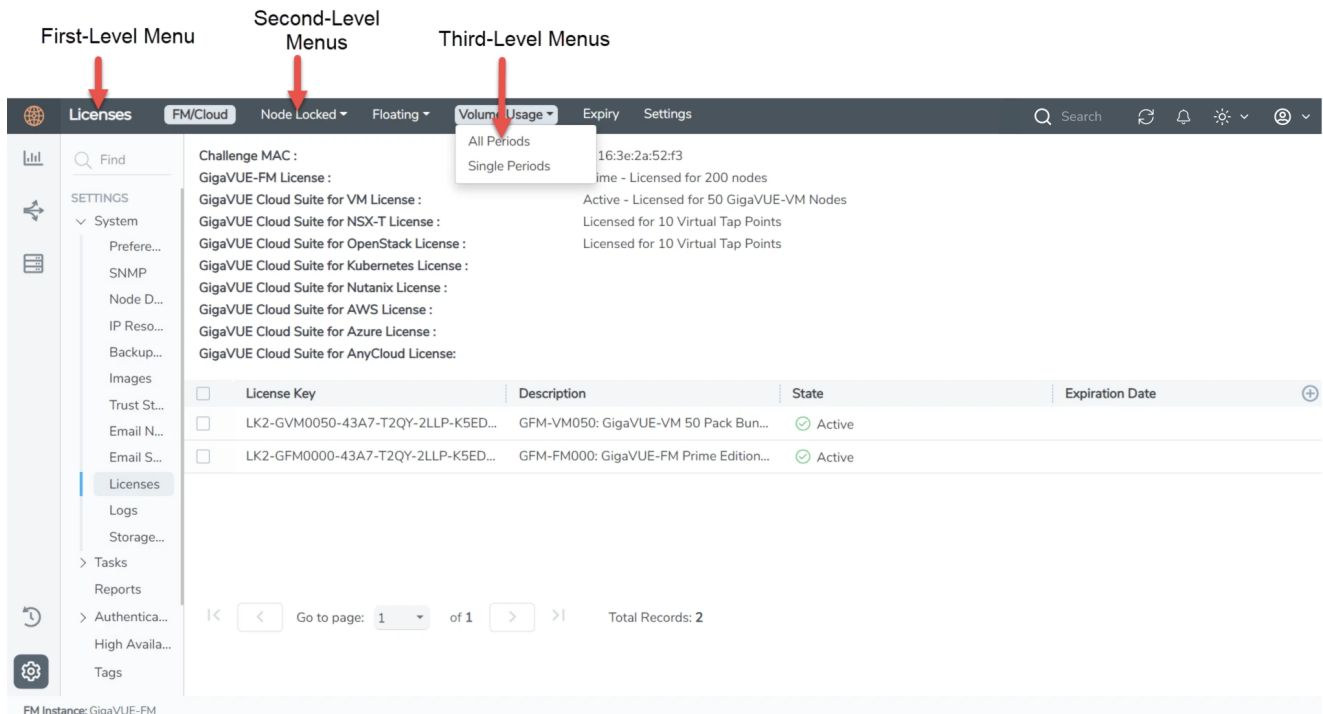
- Page-level headers
- Search 
- Refresh 

- Rediscover  - You can view the rediscover icon on the top navigation bar only when you click a node or a cluster ID (Go to **Inventory** > **Physical** > **Nodes**). Click the  icon to pull the latest configuration from the GigaVUE-OS device. This works same as the Rediscover option in the Physical Nodes page. For more information refer to [Cluster Discovery Behavior](#).
- Theme  - For information on the Theme  icon refer to [Theme Settings](#).
- Profile  options- Help  option is available under . To create keyboard shortcuts to navigate to different menu pages, click on  and select Keyboard Shortcuts.

NOTE: The Save Configuration  option is available in the Node Overview, Flow Maps, and Active Visibility pages.

Page-Level Header

The page-level headers of the GigaVUE-FM instance are displayed as shown in the figure.



- The first-level menu is displayed as the Main Header in the top navigation bar.
- The second-level menus are displayed next to the first-level menu.

NOTE: The second-level menus that overflow in the top navigation bar are displayed as a drop-down with an option to expand or collapse.

- The third-level menus are displayed as drop-down under the second-level menus.

GigaVUE-FM GUI Navigation

Use the navigation sidebar and the appropriate page-level headers to navigate to the various GUI pages. Depending on the user role and access rights of the user, the fields and buttons in the individual pages may either be enabled or disabled. Mandatory fields in the GUI are pages are notified appropriately.

Footer

The footer of GUI displays the GigaVUE-FM instance name, Node Synchronized time when accessing pages related to nodes, and NRT time stamp.

NOTE: On Windows Server 2019, some layout elements, such as the bottom bar, may not display correctly due to [system-level display behavior](#). Additionally, certain screens could have minor issues with font rendering, spacing, or resolution scaling.

Theme Settings

The theme setting options  allow you to choose among light, dark, and system themes. Once the theme is set, the settings remain the same, even when you log out of GigaVUE-FM, close or reopen the browser, or open a new tab for GigaVUE-FM. It is also independent of the browser settings.

The following table shows the options available when you click on the theme settings



icon:

S.No	Options	Description
1	Light theme 	UI changes to light color. It is the default theme.
2	Dark theme 	UI changes to Dark color.
3	System 	UI applies the theme based on the Operating System theme settings.

NOTE: When you cannot view the theme changes applied in Fabric Health Analytics (FHA), clear the browser cache and reload to view the updated changes.

Configure a Custom Banner

It is recommended to configure a pre-login banner which states the security policy of your company or organization. The banner appears on the login screen before the users log into GigaVUE-FM.

Only the users with fm_admin and fm_super_admin role assigned can view and configure the custom banner.

To configure the custom banner:

1. Go to **Settings** and select **Systems > Preferences**.
2. Click **Edit** and the Edit Preferences page appears.
3. Enter the custom banner message in the **Login infobox** text box.
4. Click **Save**.

Quick Views

A quick view provides easy access to Visibility Fabric details such as nodes, ports, and traffic policies. In GigaVUE-FM, you can click on items such as port ID, map alias, port error counts, and so on, and get detailed information about the selected item.

Recently Viewed



Click on  icon on the left navigation pane to view the list of recently viewed pages.

- You can view up to last 100 pages that you have visited.
- The pages are listed in chronological order with the most recent entry listed at the top.
- Click on a link to navigate to that page.
- Use the 'Find in Recently Viewed' to filter the required pages.

Recently Viewed

Earlier Today

Fm - PhysicalNode	/fm/physicalNode
Tasks - AdminTasks	/fm/settingsfm/tasks/adminTasks
TopDashboard - Dashboard	/fm/topDashboard/dashboard
Flows - Flowhealth	/fm/flows/flowhealth
Flows - ActiveVisibilityPhysicalNodes	/fm/flows/activeVisibilityPhysicalNodes
Flows - MapPhysicalNodes	/fm/flows/mapPhysicalNodes
Maps - Maps	/node/cluster-one/flows/maps/maps/maps/
FabricMapMenu - FabricMapsList	/fm/flows/fabricMaps/fabricMapMenu/fabricMapsList/
Fm - ChangePassword	/fm/changePassword

Find Pages

The Find option in the expanding tool bar allows you to search and quickly navigate to the pages without navigating through each of the menus and submenus.

- Enter the name of the page that you want to search (fully or in part). The number of matching entries under each of the menu and submenu category is displayed.
- Click the link under the category to navigate to the respective page.

For example, if you search for the term 'node', then the corresponding matching entries in the menus and submenus are displayed.

The screenshot shows the GigaVUE-FM interface with a search bar at the top containing the text 'node'. Below the search bar, the results are displayed in a table. The table has columns for Type, Status, Node Summary, Start Time, End Time, and Log. The results show several entries for 'ImageInstall' tasks, all with a status of 'Success'.

Type	Status	Node Summary	Start Time	End Time	Log
grade	Success	-	2021-02-23 12:28:00	-	-
grade	Success	-	2021-02-22 10:42:00	-	-
grade	Success	-	2021-02-19 10:22:00	-	-
grade	Success	-	2021-02-17 11:07:00	-	-
grade	Success	-	2021-02-16 15:21:00	-	-

Return to the Dashboard

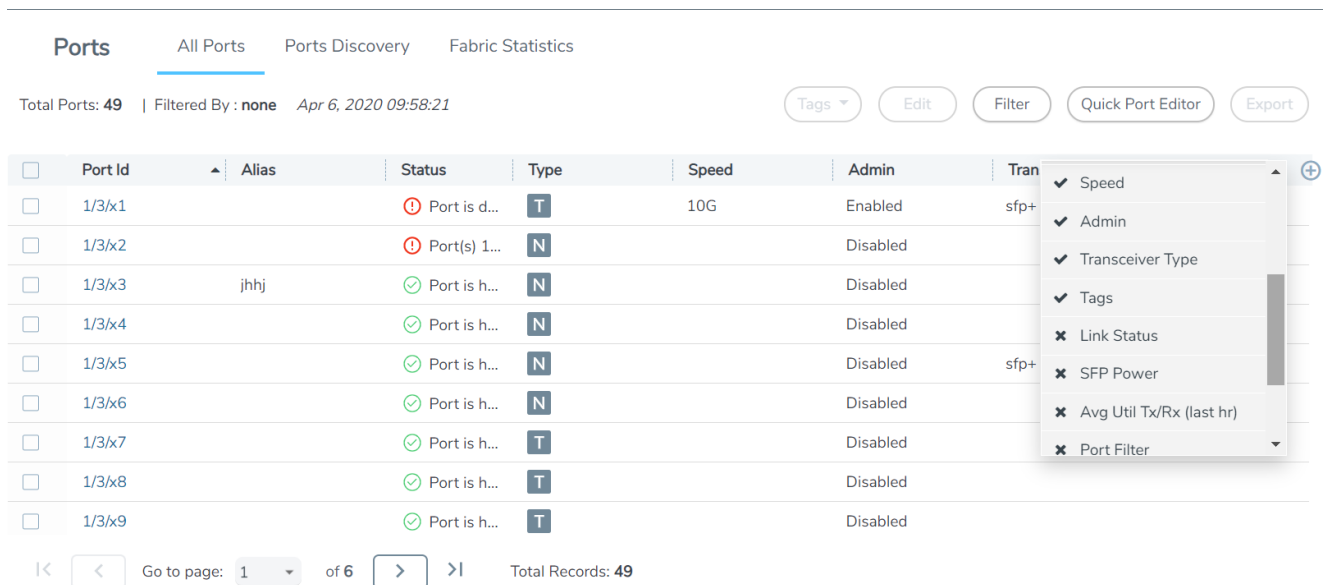
At any time, to return back to the Dashboard, click on the  icon on the top left of GigaVUE-FM GUI. Refer to [Dashboard](#). By default, the Physical & Virtual Dashboard page is displayed.

Table View Customization

GigaVUE-FM enables you to customize the appearance of tables. You can choose the columns you want to show and hide in the table. You can also choose the order in which you want to view the columns in the table.

To customize the columns:

1. Click the '+' icon on the top-right edge of the table.



The screenshot shows the 'Ports' section of the GigaVUE-FM GUI. At the top, there are tabs for 'All Ports', 'Ports Discovery', and 'Fabric Statistics'. Below the tabs, it says 'Total Ports: 49 | Filtered By : none Apr 6, 2020 09:58:21'. To the right of the table are buttons for 'Tags', 'Edit', 'Filter', 'Quick Port Editor', and 'Export'. The table has columns: Port Id, Alias, Status, Type, Speed, Admin, and Tran. A context menu is open on the right side of the table, showing a list of columns with checkboxes to toggle their visibility. The columns in the menu are: Speed (checked), Admin (checked), Transceiver Type (checked), Tags (checked), Link Status (unchecked), SFP Power (unchecked), Avg Util Tx/Rx (last hr) (unchecked), and Port Filter (unchecked). At the bottom of the table, there is a pagination bar showing 'Go to page: 1 of 6' and 'Total Records: 49'.

Port Id	Alias	Status	Type	Speed	Admin	Tran
1/3/x1		Port is d...	T	10G	Enabled	sfp+
1/3/x2		Port(s) 1...	N		Disabled	
1/3/x3	jhhj	Port is h...	N		Disabled	
1/3/x4		Port is h...	N		Disabled	
1/3/x5		Port is h...	N		Disabled	sfp+
1/3/x6		Port is h...	N		Disabled	
1/3/x7		Port is h...	T		Disabled	
1/3/x8		Port is h...	T		Disabled	
1/3/x9		Port is h...	T		Disabled	

Figure 2 Table menu to configure columns

2. Click on a column name to change the show/hide setting. A check mark indicates the columns to show and an X indicates the columns to hide.
3. To rearrange the columns in the table, select a column heading and drag it to the new location. Your customizations are automatically saved.
4. Click on 'Reset columns to default' to reset the columns to the default view.

NOTE: The customized column settings are preserved for the user profile. When you logout and log back in, the tables display the same customized columns.

The pagination option on the bottom-right corner of the page allows you to scroll through long lists of data that span across multiple pages. You can also jump to a specific page by clicking the page number. Each page can show up to 100 rows of data per view.

Click the export option to export the tables either in CSV file format or in XLSX format. You can either export all the records or export only the selected records.

Dashboard

This section describes the Dashboards available in GigaVUE-FM. Refer to the following table for details:

Left Navigation Pane	Description	Reference
Overview		
Physical and Virtual	Provides a quick visual overview of the traffic, health status, inventory and audit logs of the physical and virtual nodes managed by GigaVUE-FM.	Overview of the Physical and Virtual Dashboard
System		
Alarms	Lists the alarms triggered in GigaVUE-FM	Overview of Alarms
Audit Logs	captures audit logs for all users connected to GigaVUE-FM	
Events		
FM Health	Provides an overview of GigaVUE-FM health.	GigaVUE-FM Health Dashboard
Analytics		Analytics

Physical and Virtual Dashboard

This chapter describes the dashboards that provide information about the physical nodes, ports, port links, maps, GigaSMART, audit logs, and events on a single page.

This chapter covers the following topics:

- [Overview of the Physical and Virtual Dashboard](#)
- [Physical Dashboard Profiles](#)
- [Physical Dashboard Quick Views](#)
- [Physical Dashboard Widgets](#)

Overview of the Physical and Virtual Dashboard

The Physical and Virtual Dashboard is a central location to monitor all the physical and virtual nodes and clusters that are managed by GigaVUE-FM. The widgets in the dashboard provides a quick visual overview of inventory and events, GigaSMART traffic, highest and lowest traffic by maps and ports, traffic comparison by tags, most and least utilized traffic, health status, and audit logs.

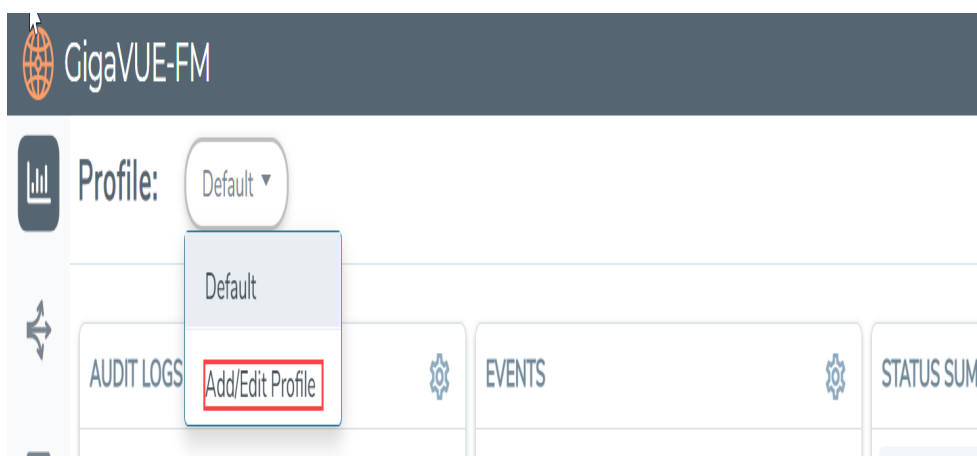
NOTE: You must scroll the individual widgets horizontally to view the invisible information.

Physical Dashboard Profiles

The Physical Dashboard displays a number of default widgets when you first log in. They are displayed with the profile labeled as **Default**. You can create multiple profiles and choose the widgets to be displayed in each profile based on the data you want to proactively monitor and troubleshoot in your Visibility Fabric.

To create a new profile

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile drop-down and click **Add/Edit Profile**.



2. In the **Add/Edit Profile...** box, enter the name of the new profile and click **Enter**.
The new profile name is displayed under Profiles. The new profile page is displayed.

- (Optional) Click the Edit icon and select **Set as Login Profile** if you want the new profile to display as your default Physical Dashboard.

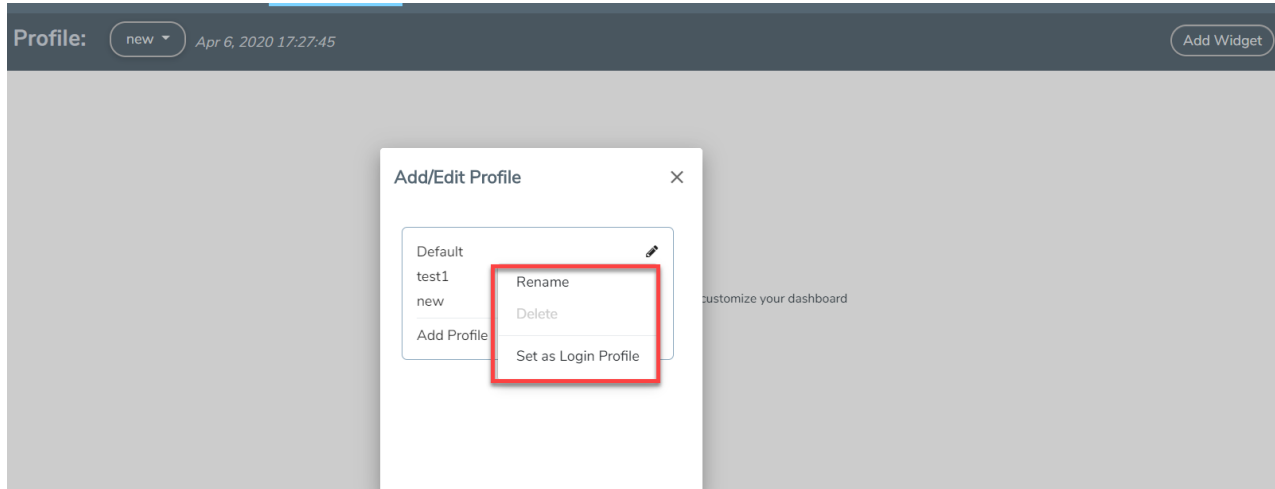


Figure 3 Profile Settings

To change the profile name, click **Rename**, edit the name, and press **Enter**.

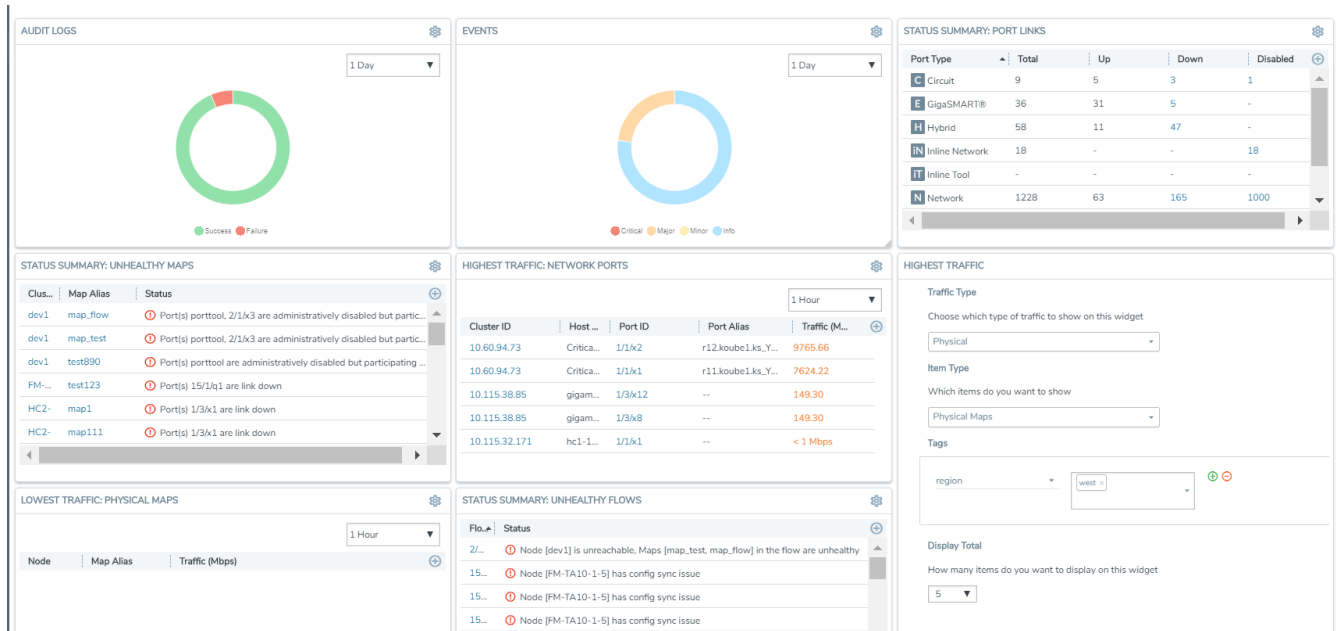
To delete the profile, click **Delete**. If you delete a default profile, then the initial default profile is automatically set as the login profile unless you actively select another one.

Once deleted, there is no option to recover those dashboards.

NOTE: When GigaVUE-FM is upgraded, the profiles created in the previous version are not retained in the latest version.

Keep in mind the following regarding the widgets on the dashboard.

- Widget and trending data is available based on the GigaVUE-FM license purchased. For the base package, the data is not stored for more than 1 day. The prime package users can select any option including 1 month.
- Individual widgets can be resized and saved as part of the profile. Each widget can expand in both horizontal and vertical planes. The other widgets self-adjust when the widgets are manipulated.
- The widgets can also be dragged and dropped to different section of the page. Refer to [Physical Dashboard Profiles](#).
- The data points can be viewed when the mouse is hovered over the graph as shown in [Physical Dashboard Profiles](#).
- The widgets such as Unhealthy Maps opens a quick view when clicked on the cluster info or the map alias. The quick view shows more details relating to that specific map.
- The trending information can also be changed for each widget on the same dashboard.
- The port and map health status changes on the device reflect instantly on the screen.
- The color-coded legends are available at the bottom of each widget.



Note: If the percentage displayed in a pie-chart is negligible or less, then it would be difficult to click on the pie-chart arc and view the details.

Physical Dashboard Quick Views

When reviewing the widgets available on the Physical & Virtual dashboard, clicking on the options in the widgets takes you to the details page relating to the information for that node. For example, on the Nodes by Model or Software Version widget, you click on the node and it takes you to the Physical Nodes page.

For more information about Physical Nodes, refer to [Manage GigaVUE Nodes and Clusters](#).

Telemetry Insights Dashboard

The Telemetry Insight dashboard gives you a single, actionable view of the health, usage, licensing risks, and security posture of your GigaVUE-FM, along with recommended actions.

The Telemetry Insights dashboard has three major sections:

- [Executive Health Summary](#)
- [Operational Summary](#)
- [Recommended actions](#)

Prerequisites

- Enable GigaVUE-FM Connected Experience to populate the Telemetry Insight Dashboard. If you do not enable it, the dashboard shows no data, and GigaVUE-FM does not compute the insight data points.
- Enable SNMP traps on the devices and configure them to send traps to GigaVUE-FM.
- Enable the following trap categories:
 - Packet drops
 - Packet errors
 - Port link status
 - High and low utilization

Executive Health Summary

Once Connected Experience is enabled in GigaVUE-FM, the dashboard is populated with subsequent data at 5 AM UTC.

In the **Executive Health Summary** section, GigaVUE-FM shows a point-in-time health status of:

- Physical nodes such as GigaVUE ® HC Series and TA.
- Virtual nodes such as V Series nodes, and V Series-proxies.
- Universal Cloud Tap (UCT) such as UCT-V Controller, UCT-V, UCT-C, UCT-C Controller.

This section lets you quickly see whether your physical, virtual, and cloud tap components are healthy or need attention.

Operational Summary

In the **Operational Summary** section, GigaVUE-FM highlights the information about:

- **Compliance and Security:** GigaVUE-FM shows operational risks and inefficiencies over the last 7 days, which will help you to understand the performance issues and configuration problems without drilling into multiple device pages. This section helps you to quickly assess whether GigaVUE-FM and its access controls are configured according to internal policies. It also summarizes configuration elements that affect security, including:
 - FIPS Status- Whether GigaVUE-FM is running in FIPS mode.
 - Common Criteria Compliant- GigaVUE-FM checks settings such as FIPS, Crypto Mode, Network Audit Log, CRL Validation, and Lock Users, and ensures they are compliant.
 - Authentication mode (for example, basic authentication vs third-party).
 - API rate-limit exceed counts.
 - About to Expire tokens -Tokens that are expiring (for example, expiring within 7 days).

- **Licenses:** This section helps you to identify where you may soon lose support or entitlements so you can renew or migrate in time. You can view information about:
 - Installed and expired licenses.
 - License SKUs that are approaching End-of-Sale (EOS) or End-of-Life (EOL).
 - License SKUs that are already past EOS or EOL.
 - Volume-based license (VBL) over-usage in the last 7 days.
- **Aggregated Physical Nodes** - This section shows view of health, performance, and configuration-related signals across physical inventory managed by GigaVUE-FM, helping to identify operational risks, underutilized resources, and nodes that need attention. You can infer the following information:
 - Ports with High Packet Drops - Highlights physical ports experiencing sustained packet drops.
 - Admin Enabled Ports with no Traffic - Highlights ports that are administratively enabled but not carrying traffic.
 - Ports With High Utilization - Tracks ports with high utilization.
 - Unused Flow Maps - Shows configured flow maps that are currently not in use.
 - Physical Nodes with Older than LTS Version - Shows physical nodes running software versions older than the supported LTS baseline.
- **Aggregated Cloud Fabrics** - This section summarizes the health of V Series nodes, UCT-V agents. It combines the health signals for those cloud environments into a single cloud-level view so that you can quickly confirm whether there are problems in any of the managed cloud locations. When the aggregated cloud fabrics tile shows issues, you can use the rest of the dashboard and drill-down views to identify which specific cloud nodes or fabrics are affected. You can infer the following information:
 - GigaVUE V Series added and deleted - Shows the count of V Series nodes added to or removed from the environment during the reporting window.
 - UCT-V Inventory Added - Displays newly added UCT-V instances in the environment.
 - Virtual Nodes with outdated Software Version - Highlights virtual nodes running versions behind the supported software baseline.
 - GigaVUE V Series with Status Flaps - Highlights V Series nodes whose status is changing frequently between healthy and unhealthy states.

Recommended actions

In the recommended actions section, you can view the lists of actionable items that are derived from the other sections, such as:

- Expired Licenses
- About to expire License
- End Of Sale/End Of Life SKU
- Unreachable Nodes (Node Healthy) Physical
- Token about to expiry
- Basic Authentication
- GigaVUE-FM Storage Space (/Config /var /root)

This section helps you to decide what to fix first. For example:

-  - Issues marked with this symbol must be treated as Priority 1 (P1).
-  - Issues marked with this symbol must be treated as Priority 2 (P2).
-  - Issues marked with this symbol must be treated as Priority 3 (P3).

View the Telemetry Insight dashboard

To view the Telemetry Insights Dashboard, in GigaVUE-FM, go to Dashboard  > **System** > **Telemetry**. The Telemetry Insights dashboard page appears.

Rules and Notes

- The Telemetry Insight Dashboard shows data only the next day after GigaVUE-FM Connected Experience is enabled. If you do not enable it, the dashboard appears but stays empty.
- Only Super Admin users can view the dashboard. This prevents incomplete views caused by RBAC limits in this release.
- If SNMP traps are not enabled or do not reach GigaVUE-FM, trap-based sections will be empty or partly filled. GigaVUE-FM still shows sections based on inventory and configuration.
- Dashboard time windows are relative (for example, last 7 days). Absolute dates are not supported.
- Configuration-change insights show only the changes made through GigaVUE-FM (GUI, REST API, or other GigaVUE-FM based methods). GigaVUE-FM does not capture changes made directly on devices, such as through the device CLI. This may cause lower reported configuration activity.

Physical Dashboard Widgets

This section describes the widgets that can be created and viewed on the Physical Dashboard.

- [Highest Traffic](#)
- [Lowest Traffic](#)
- [Traffic Comparison By Tags](#)
- [Most Utilized Traffic](#)
- [Least Utilized Traffic](#)
- [Inventory](#)
- [Status Summary](#)

The default profile displays the following widgets:

- Highest Traffic: Network Ports, Tool Ports, and Physical Maps
- Status Summary: Unhealthy Maps and Port Links
- Audit Logs
- Events

You can customize the widgets by modifying the physical dashboard profiles. Refer to [Physical Dashboard Profiles](#) for more information.

Highest Traffic

The Highest Traffic widget can be created for the following:

- Physical
 - Physical maps
 - Fabric maps
 - Network ports
 - Tool ports
 - Stack ports
 - Hybrid ports
 - Inline network ports
 - Inline tool ports
- GigaSMART
 - GigaSMART groups
 - GigaSMART operations

You can create as many Highest Traffic widgets as you want listing up to 5, 10, 15, 20, 50, or 100 items in each widget.

The highest traffic is measured in megabytes per second (Mbps). You can specify the period over which the amount of traffic must be calculated. The period can be 1 hour, 1 day, 1 week, or 1 month.

HIGHEST TRAFFIC: NETWORK PORTS					⚙️
					1 Hour ▼
Cluster ID	Host ...	Port ID	Port Alias	Traffic (Mbps)	⊕
10.60.94.73	Critica...	1/1/x2	r12.koube1.ks_YR0742_DS	9764.35	
10.60.94.73	Critica...	1/1/x1	r11.koube1.ks_YR0741_DS	7623.20	
10.115.38.85	gigam...	1/3/x12	--	149.58	
10.115.38.85	gigam...	1/3/x8	--	149.58	
10.115.32.171	hc1-1...	1/1/x1	--	< 1 Mbps	

Figure 4 Highest Traffic: Example

The physical maps are listed by the node ID, map alias, and the traffic in Mbps.

The ports are listed by the node on which they are used and the port alias. You can create the Highest Traffic widget for the following ports:

- Network ports
- Tool ports
- Stack ports
- Hybrid ports
- Inline network ports
- Inline tool ports

The highest traffic for GigaSMART operations or GigaSMART group can be displayed as shown in [Figure 5 Highest Traffic GigaSMART](#).

HIGHEST TRAFFIC: GIGASmart GROUPS			⚙️
			1 Hour ▼
Node	GS Group ▲	Traffic (Mbps)	⊕
dev6	GS_1		
HC2-	gs_1		
gigamon-...	gsg1		

Figure 5 Highest Traffic GigaSMART

To configure the Highest Traffic widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.

- Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 6Add New Widget](#).

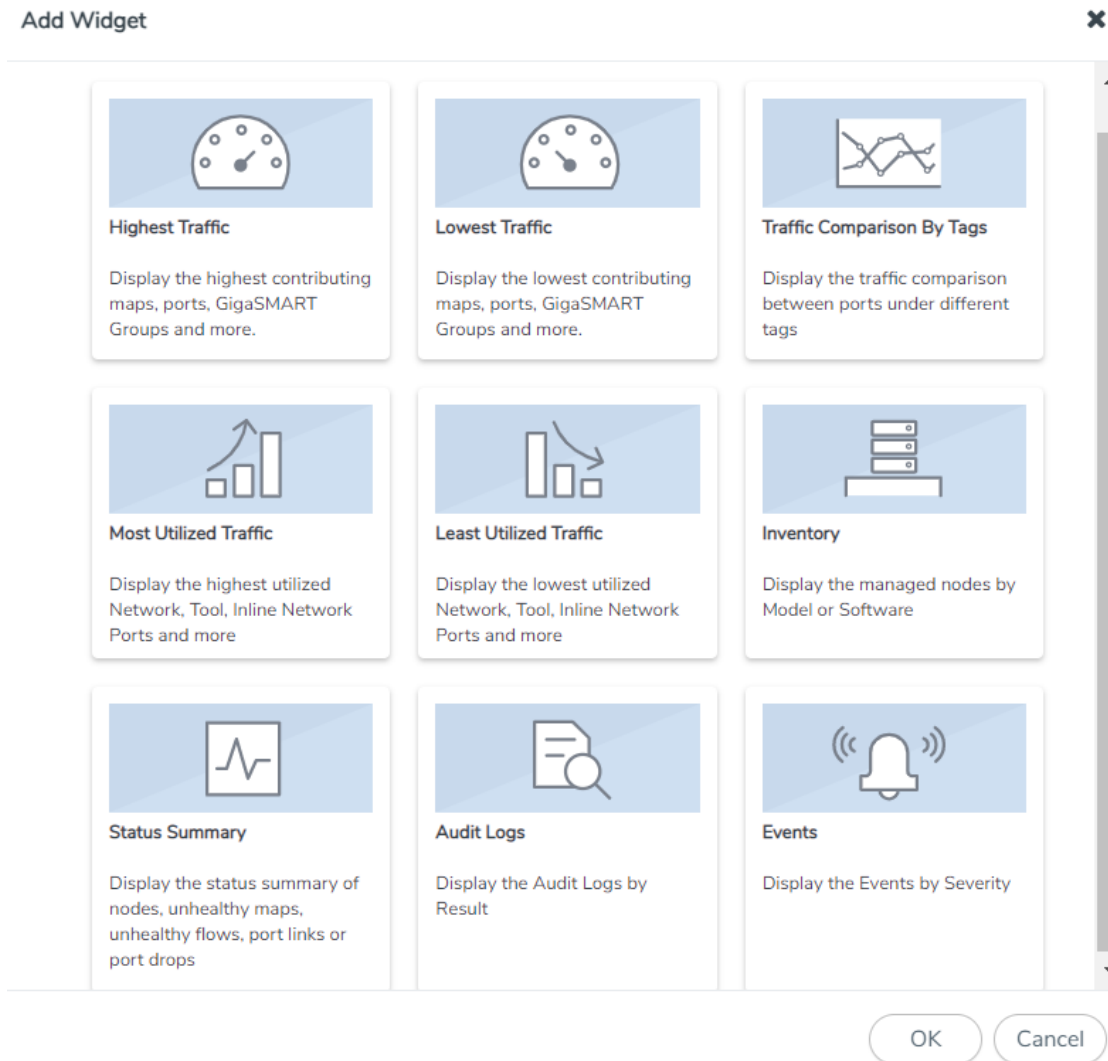
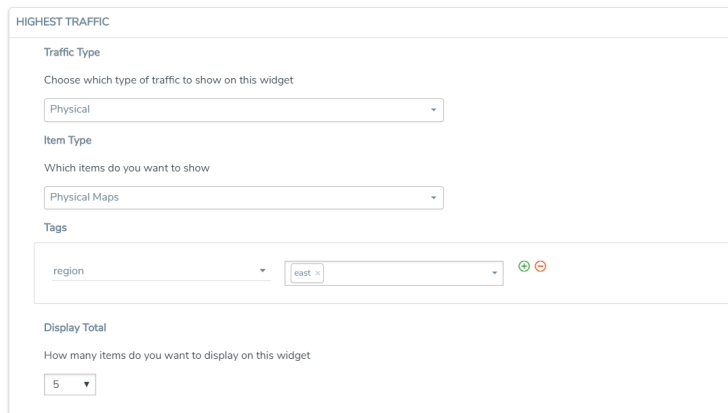


Figure 6 Add New Widget

- In the Add New Widget window, select **Highest Traffic** and click **OK**. The Highest Traffic configuration window is displayed. Refer to [Figure 7Highest Traffic Configuration](#).



HIGHEST TRAFFIC

Traffic Type
Choose which type of traffic to show on this widget
Physical

Item Type
Which items do you want to show
Physical Maps

Tags
region east

Display Total
How many items do you want to display on this widget
5

Figure 7 Highest Traffic Configuration

4. From the **Traffic Type** drop-down list, select one of the following traffic types:
 - Physical—Allows you to view the physical maps and ports that contribute to the highest traffic distribution.
 - GigaSMART—Allows you to view the virtual ports, GigaSMART groups, and GigaSMART operations that contribute to the highest traffic distribution.
5. From the **Item Type** drop-down list, select the item you want to view. The options displayed are based on the traffic type you selected in step 5.
6. Select the required tag key and tag value combination (for example: tag key is 'Site' and tag value is 'East') for which the highest traffic distribution must be displayed. This step is optional.
7. From the **Display Total** drop-down list, select the number of items to be displayed. By default, the number of items selected for display is 5.
8. Click **OK**.

Lowest Traffic

The Lowest Traffic widget lists the physical maps, flow maps, ports, and GigaSMART that contribute to the lowest traffic within a specified time. You can create as many Lowest Traffic widgets as you want listing up to 5, 10, 15, 20, 50, or 100 items in each widget.

The traffic flowing through a port or a map rule is measured in megabytes per second (Mbps). You can specify the period over which the amount of traffic is calculated. The period can be 1 hour, 1 day, 1 week, or 1 month.

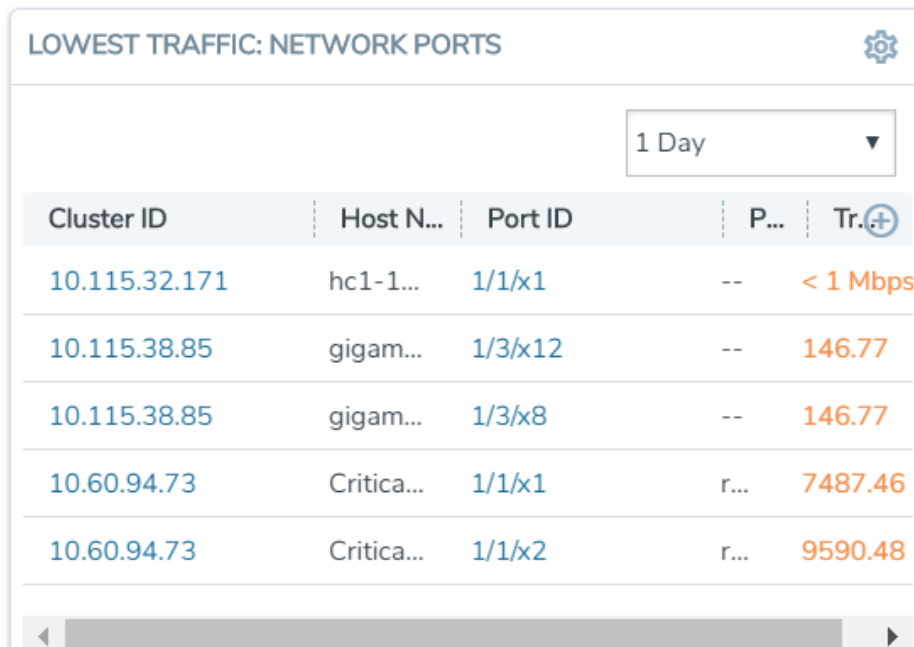


Figure 8 Lowest Traffic

The Lowest Traffic widget is configured exactly the same way as the Highest Traffic widget. To configure the Lowest Traffic widget, refer to the configuration steps provided in [Highest Traffic](#). In **step 4**, select **Lowest Traffic** and click **OK**. The Lowest Traffic configuration window is displayed.

Traffic Comparison By Tags

The Traffic Comparison By Tags widget allows you to compare the aggregated traffic flowing through the list of ports associated to tags. You can choose to view up to four traffic comparisons in a single widget. You can create as many Traffic Comparison By Tags widgets as necessary in the selected profile and provide a customized name for each widget. The customized name helps you to differentiate multiple traffic comparison widgets in a single profile.

In this example, there is traffic flowing from GigaVUE-TA10 to GigaVUE-HC3. You can group the tool ports in GigaVUE-TA10 and create a tag as TA_TOOL. Then, you can group the network ports in GigaVUE-HC3 and create a tag as HC3-NETWORK. Refer to [Figure 9Example for Traffic Comparison By Tags Widget](#).

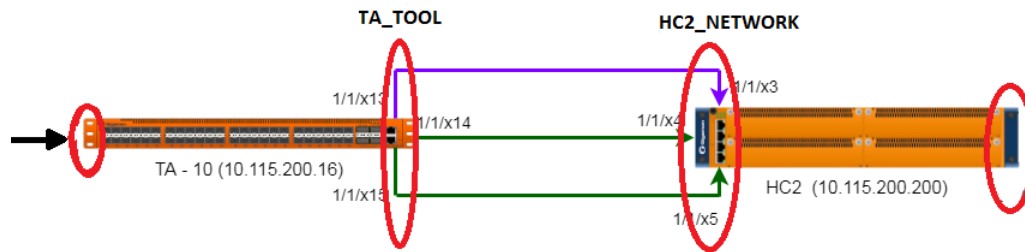


Figure 9 Example for Traffic Comparison By Tags Widget

Using the Traffic Comparison By Tags widget, you can compare the egress traffic passing through the ports associated with T A_TOOL with the ingress traffic passing through the ports associated with HC3-NETWORK, and quickly analyze if there is any packet loss associated. Refer to [Figure 10Traffic Comparison By Tags](#)

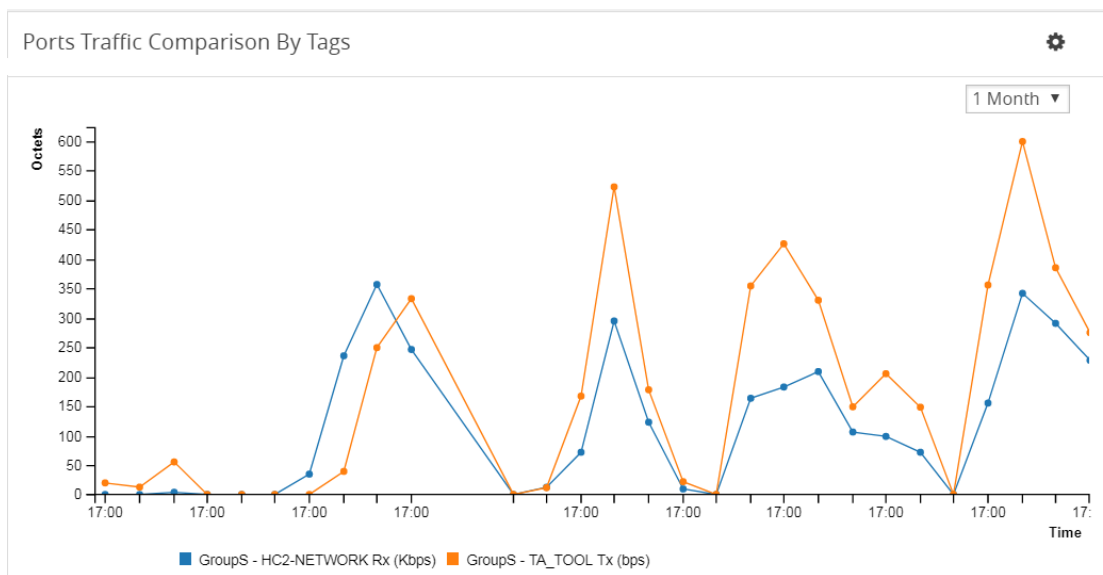


Figure 10 *Traffic Comparison By Tags*

The Traffic Comparison By Tags widget also allows you to choose just the egress traffic passing through the ports associated with T A_TOOL and view the graph.

The following statistics can be viewed for physical ports and GigaSMART:

Traffic Type	Statistics
Physical Ports	Data Rate
	Packet Rate
	Packet Errors
	Packet Discards
	Packet Drops

Traffic Type	Statistics
	Port Utilization
GigaSMART	Data Rate Packet Rate Packet Drops Packet Errors Packet Buffer Packet Terminated

The aggregated traffic comparison is displayed as a graph. You can choose to display the data over a day, an hour, a week, or a month. However, when you select a week or a month, the time period is not persisted. The data is defaulted to 1 day when you navigate away from the Physical Dashboards page and then return to the page. Click the notification icon at the top of the window and view the alarms and notifications displayed (refer to [Figure 11 Notifications](#)):

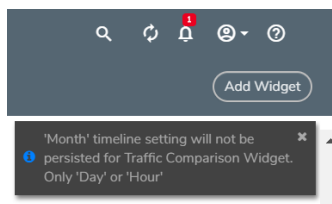


Figure 11 Notifications

Hovering the mouse over the lines in the graph displays the tag name, traffic direction, and traffic flow (Mbps).

To configure the Traffic Comparison By Tags widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
2. Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 6 Add New Widget](#).

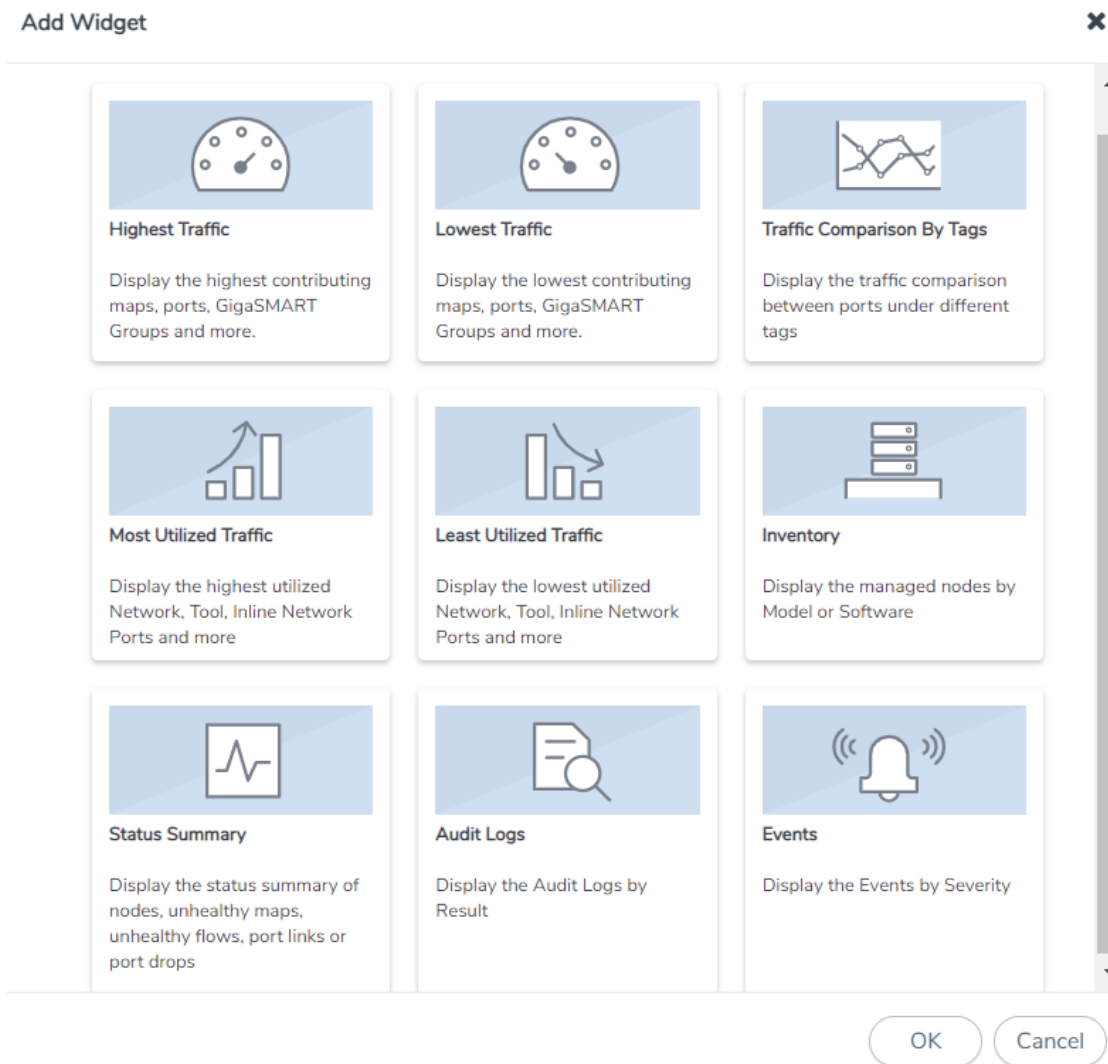


Figure 12 Add New Widget

3. In the Add New Widget window, select **Traffic Comparison By Tags** widget and click **OK**. The Traffic Comparison by Tags configuration window is displayed. Refer to [Figure 13Traffic Comparison By Tags Configuration](#).

Figure 13 *Traffic Comparison By Tags Configuration*

4. (Optional) In the **Widget Name** box, enter a customized name for the widget. Customized name helps to differentiate multiple traffic comparison widgets in the same profile.
5. From the **Traffic Type** drop-down list, select one of the following traffic types:
 - o Physical Ports
 - o GigaSMART
6. From the **Statistics** drop-down list, select the type of statistic to view in the comparison graph.
7. Select **Sum** or **Average** to determine the way to display the statistics.
8. In Tag Items, select two or more tags to compare.
 - a. For Traffic 1, select the tag name and tag value from the drop-down lists.
 - b. Select **Ingress (Rx)** or **Egress (Tx)** to determine the traffic direction.
 - c. Repeat step a and step b to select the next traffic for comparison.
9. Click **OK**.

Most Utilized Traffic

The Most Utilized Traffic widget allows you to view the ports with highest percentage utilization. The highest percentage utilization is displayed over the selected period. The period can be 1 hour, 1 day, 1 week, or 1 month to view the utilization percentage.

The Most Utilized Traffic widget lists the ports with the cluster ID, port Id, port alias, and the utilization percentage.



Figure 14 *Most Utilized Traffic Widget*

To configure the Most Utilized Traffic widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
2. Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 15Add New Widget](#).

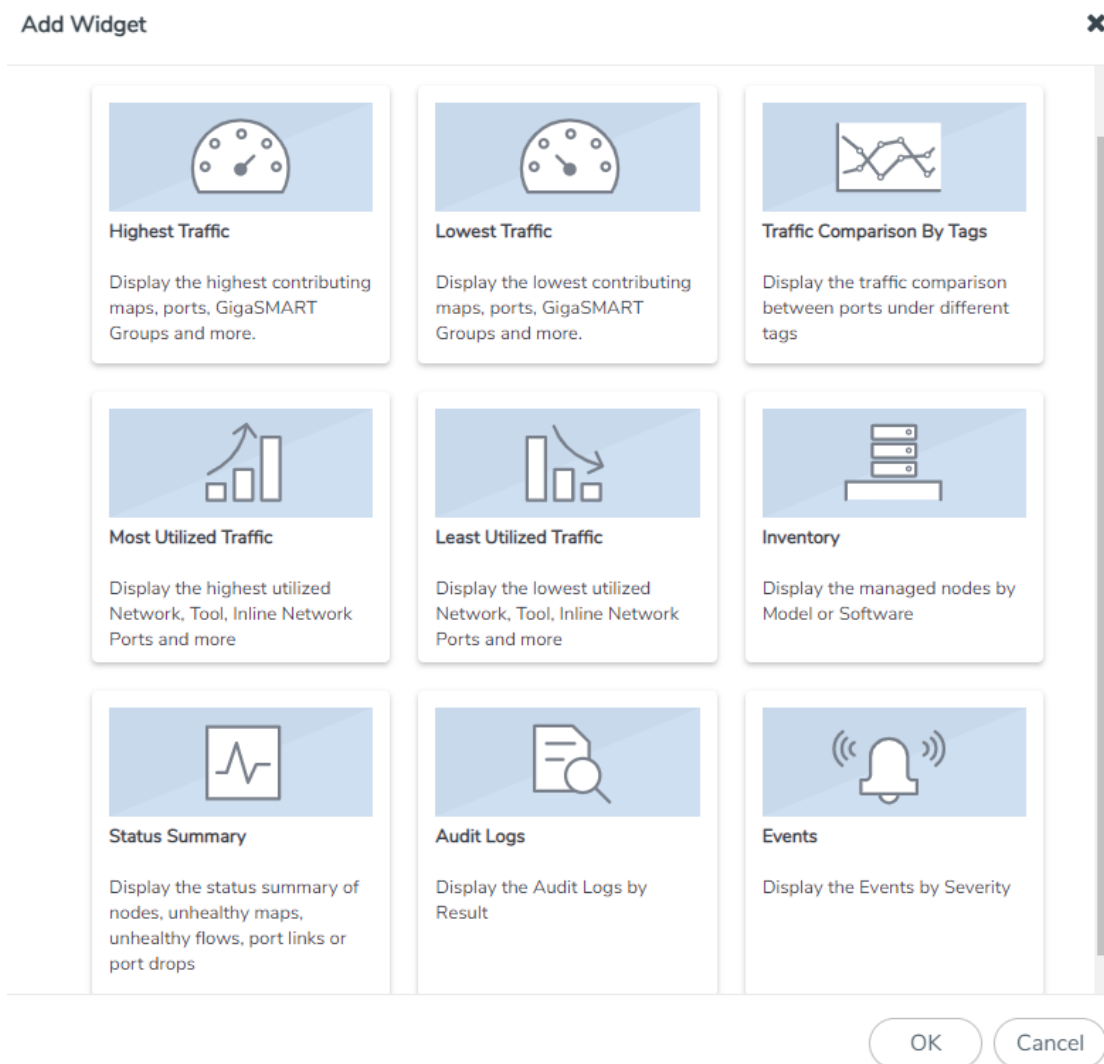
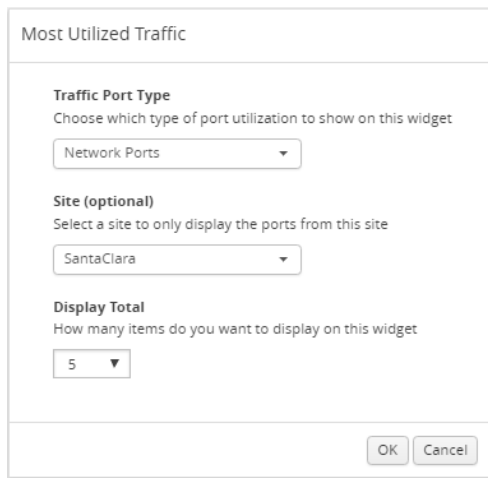


Figure 15 Add New Widget

- In the Add New Widget window, select **Most Utilized Traffic** and click **OK**. The Most Utilized Traffic configuration window is displayed. Refer to [Figure 16 Most Utilized Traffic Configuration](#).



The image shows a configuration dialog box titled "Most Utilized Traffic". It contains three sections: "Traffic Port Type" with a dropdown menu set to "Network Ports", "Site (optional)" with a dropdown menu set to "SantaClara", and "Display Total" with a dropdown menu set to "5". At the bottom right are "OK" and "Cancel" buttons.

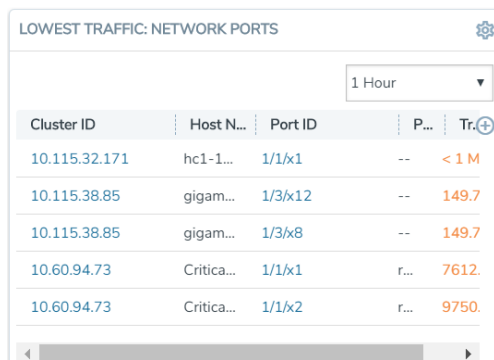
Figure 16 *Most Utilized Traffic Configuration*

4. From the **Traffic Port Type** drop-down list, select one of the following port types:
 - Network Ports
 - Tool Ports
 - Stack Ports
 - Hybrid Ports
 - Inline Network Ports
 - Inline Tool Ports
5. Select the required tag key and tag value combination (for example: tag key is 'Site' and tag value is 'East') for which the most utilized traffic configuration must be displayed. This step is optional.
6. From the **Display Total** drop-down list, select the number of items to be displayed. By default, the number of items selected for display is 5.
7. Click **OK**.

Least Utilized Traffic

The Least Utilized Traffic widget allows you to view the lowest percentage utilization for all the ports. The lowest percentage utilization is displayed over the selected period. You can choose 1 hour, 1 day, 1 week, or 1 month to view the utilization percentage.

The Least Utilized Traffic widget lists the ports with the cluster ID, host name, port number, port alias, and the utilization percentage.



LOWEST TRAFFIC: NETWORK PORTS

1 Hour

Cluster ID	Host N...	Port ID	P...	Tr.+
10.115.32.171	hc1-1...	1/1/x1	--	< 1 M
10.115.38.85	gigam...	1/3/x12	--	149.7
10.115.38.85	gigam...	1/3/x8	--	149.7
10.60.94.73	Critica...	1/1/x1	r...	7612.
10.60.94.73	Critica...	1/1/x2	r...	9750.

Figure 17 Least Utilized Traffic

The Least Utilized Traffic widget is configured exactly the same way as the Most Utilized Traffic widget. To configure the Least Utilized Traffic widget, refer to the configuration steps provided in [Most Utilized Traffic](#). In **step 4**, select **Least Utilized Traffic** and click **OK**.

Inventory

The Inventory widget provides information about the physical nodes by model and software.

Nodes by Model

The Nodes by Model widget displays the number of nodes managed by the current instance of GigaVUE-FM as a bar graph. Each bar in the graph indicates the number of each device model managed. Hovering the mouse over a bar in the graph displays the model name and the total number. [Figure 18](#) [Nodes by Model](#) shows a Node by Model widget displaying six different nodes managed by GigaVUE-FM. Hover the mouse over the bar to view the number of devices in each node.

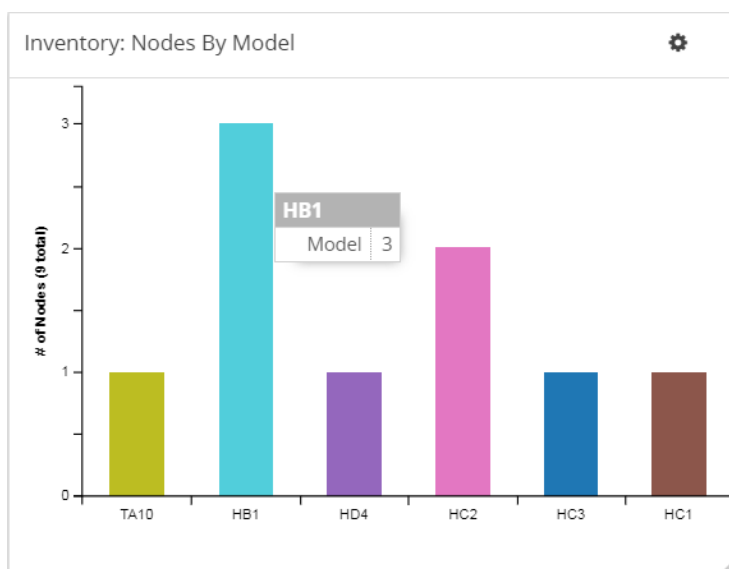
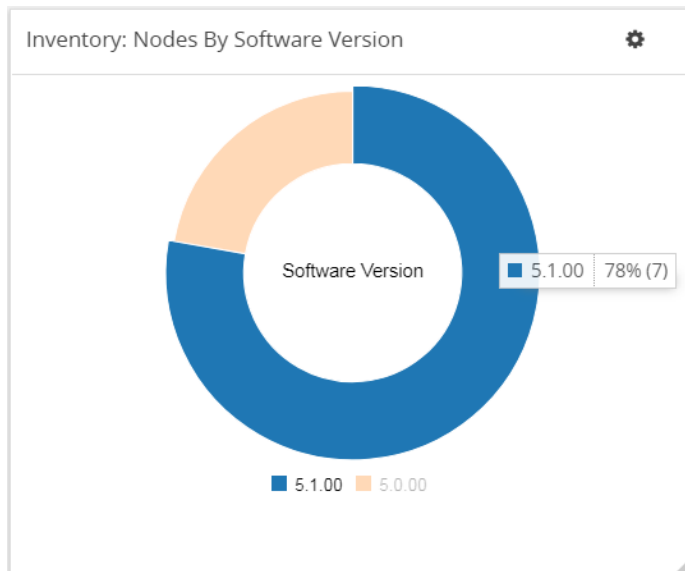


Figure 18 *Nodes by Model*

Nodes by Software Version

The Nodes by Software Version widget presents a graph that helps you to quickly view the software versions of the nodes that GigaVUE-FM is managing and the total percentage of each version. Each software version is assigned a color in the graph, which is specified by the legend. Hovering the mouse over an area in the graph displays the total number of software version used as a percentage. In [Figure 19 Nodes by Software Version](#), the Nodes by Software Version widget shows that there are 7 instances of version 5.1 and 2 instances of version 5.0, which is 22 percent of the total versions installed.

**Figure 19** *Nodes by Software Version*

To configure the Inventory widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
2. Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 20 Add New Widget](#).

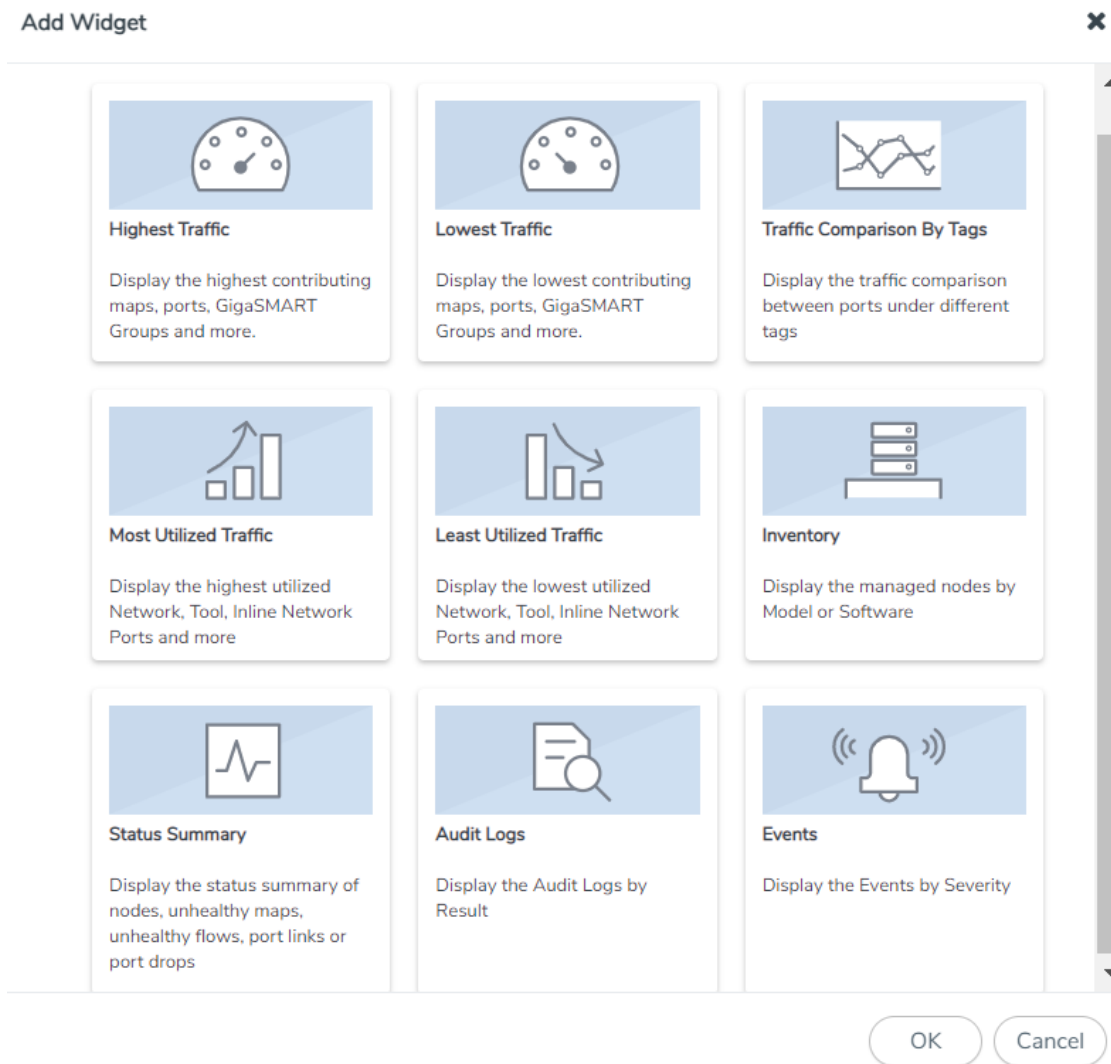
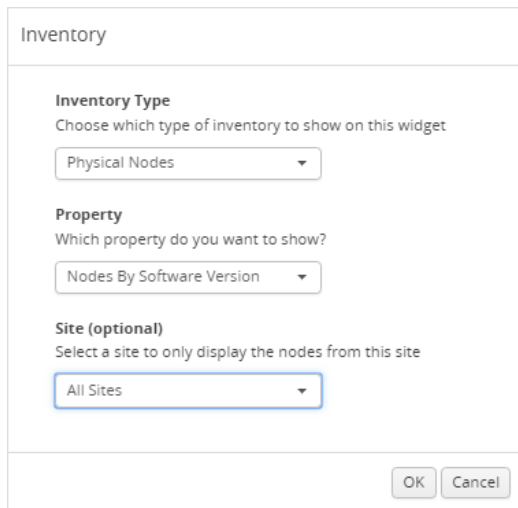


Figure 20 Add New Widget

- In the Add New Widget window, select **Inventory** and click **OK**. The Inventory configuration window is displayed. Refer to [Figure 16Most Utilized Traffic Configuration](#).



The image shows a dialog box titled "Inventory". It contains three sections: "Inventory Type" with a dropdown menu set to "Physical Nodes"; "Property" with a dropdown menu set to "Nodes By Software Version"; and "Site (optional)" with a dropdown menu set to "All Sites". At the bottom right are "OK" and "Cancel" buttons.

Figure 21 *Inventory Configuration*

4. From the **Inventory Type** drop-down list, select the Physical Nodes.
5. From the **Property** drop-down list, select one of the following:
 - Nodes by Model
 - Nodes by Software Version
6. Select the required tag key and tag value combination (for example: tag key is 'Site' and tag value is 'East') for which the inventory type details must be displayed. This step is optional.
7. Click **OK**.

Status Summary

Refer to the following section for the Status Summary widget details:

- [Nodes' Status Summary](#)
- [Port Link Status Summary](#)
- [Unhealthy Maps](#)
- [Unhealthy Flows](#)
- [Port Drops and Errors](#)
- [Unhealthy Fabric Maps](#)

Nodes' Status Summary

The nodes' status summary widget presents a graph that allows you to quickly view the current status of the physical nodes that GigaVUE-FM is managing and the number of nodes in a particular status, which is indicated by a color in the graph. The possible statuses

are:

- Normal (green)
- Warning (yellow)
- Error (orange)
- Critical (red)

For information about how the device status is computed, refer to [Node Health Status](#).

Hovering the mouse over an area in the graph displays the percentage of nodes in that status. In [Figure 22 Nodes' Status Widget](#), the widget shows that there are 5 nodes in Normal status, 4 nodes in Warning status, and 5 nodes in Critical status. There are no nodes in Error status.

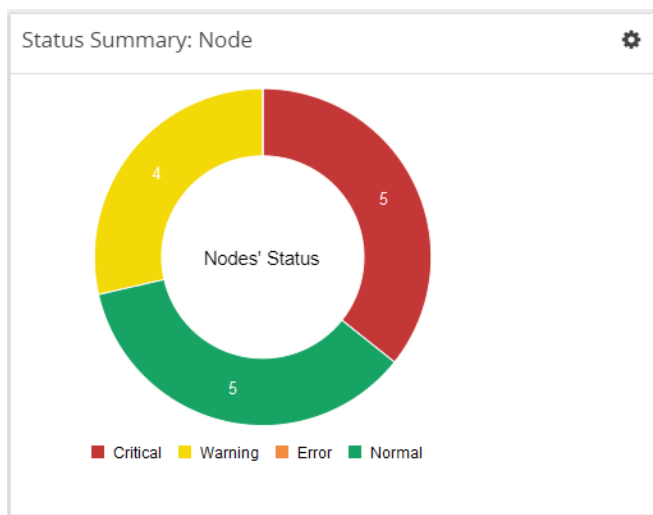
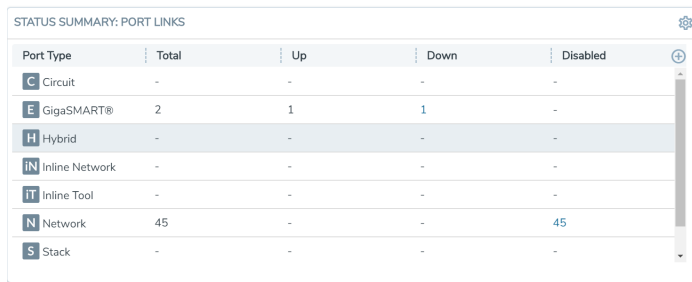


Figure 22 Nodes' Status Widget

Port Link Status Summary

The Port Link status summary widget allows you to view the current link status of all the ports available in the physical nodes currently managed by GigaVUE-FM. Optionally, the Port Link status can be displayed for the required combination of tag key and tag value (for example: tag key is 'Site' and tag value is 'East'). When a particular site tag is selected, the port link status of all the ports available in the nodes associated to that site are displayed in the Port Link Status Summary dashboard.

Refer to [Figure 23 Status Summary: Port Links Widget](#) for Status Summary: Port Links dashboard.



Port Type	Total	Up	Down	Disabled
C Circuit	-	-	-	-
E GigaSMART®	2	1	1	-
H Hybrid	-	-	-	-
IN Inline Network	-	-	-	-
IT Inline Tool	-	-	-	-
N Network	45	-	-	45
S Stack	-	-	-	-

Figure 23 Status Summary: Port Links Widget

The Status Summary: Port Links widget lists the following:

- Ports type
- Total number of ports in each type
- Total number of ports in the up, down, or disabled state

Click the numbers in the down or disabled column. A quick view provides detailed information with the cluster ID, device host name, port ID, and port alias of all the ports in the down or disabled state. If the port status is down, the quick view also provides information about the time since when the port has been in down state. The down time is displayed in minutes, hours, days, or months.

Click the port ID link for a detailed view of the packet errors, packet drops, data rate transmitted or received, packet transmitted or received, and so on occurring on an hourly, daily, weekly, or monthly basis. You can also view the related maps, transceiver type, speed, and other detailed information about the port.

NOTE: All gateway ports on GigaVUE TA Series nodes are tool ports.

Unhealthy Maps

The Unhealthy Maps status summary widget lists the maps that are in unhealthy state. The health of a map is determined by the health status of its associated components such as ports, port groups, port pairs, GigaStream, tool port, GigaSMART group, tunneled port, virtual port, inline network, inline tool, inline tool group, inline serial tool group, inline network group, and GigaSMART operations. If the status of any one of the component is down, the corresponding map is also considered unhealthy.

The Unhealthy Maps widget shows the cluster ID, map alias, and current status of the unhealthy map. The possible statuses are:

- Critical (red)
- Warning (amber)
- Unknown (gray)

The health status of a map is shown as gray when the traffic health is still being computed. The status will be updated eventually.

Click on the ID to go directly to the node. Click on the map alias to display the quick view for the map. Hovering the mouse over the status bubble for the map displays the port or ports related to the map that is in an unhealthy state.

Unhealthy Flows

The Unhealthy Flows status summary widget lists the flows that are in unhealthy state. The health of a flow is determined by the health status of the pass-all maps and the priority maps involved in the flow.

A priority map group consists of one or more maps configured with the same source ports. The health of a priority map group is determined by the aggregated health of the constituted maps. The health of the maps is determined by its associated components such as ports, port groups, port pairs, GigaStream, and so on. If any one of the maps in the priority map group is unhealthy, the corresponding priority map group is also considered unhealthy. But, the overall health status of a flow is determined by the aggregated health of the maps that are involved in the flow.

The Unhealthy Flows widget shows the names of the flows that are in unhealthy state and the names of the maps that are unhealthy in the flow. Click the Flow Name to open the flow view page.

For more information about Flows, refer to [Flows](#).

Port Drops and Errors

The Port Drops and Errors status summary widget helps in identifying the ports with packet drops or packet errors in the network. When a particular site value is selected, the status summary widget lists the port types associated to that site and the number of ports having packet drops, transmitting errors, or receiving errors in the site. You can view the number of ports with packet drops or packet errors occurring on a daily or an hourly basis.

NOTE: To view the unhealthy ports for GigaSMART, the GigaVUE-OS node must have Software version 5.0.

To view detailed information about the port drops and errors, click the number in the Pkt Drops, Rx Errors, or Tx Errors column. A quick view displays the cluster ID, host name, port ID, port alias, and the number of packet drops or errors for the list of unhealthy ports in the port

type. If there are too many ports, click the Filter icon and filter the ports based on the cluster ID, host name, port ID, or port alias. To clear the filters, click **Clear Filters** in the filter dialog box.

In the Unhealthy Ports quick view, click the port ID for a detailed view of the type of packet errors or packet drops occurring on a daily or an hourly basis. You can also view the related maps, transceiver type, speed, and other detailed information about the port, which helps to investigate the reason for the packet drops or packet errors. To return to the Ports quick view, click **Back**.

To configure the Inventory widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
2. Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 6Add New Widget](#).

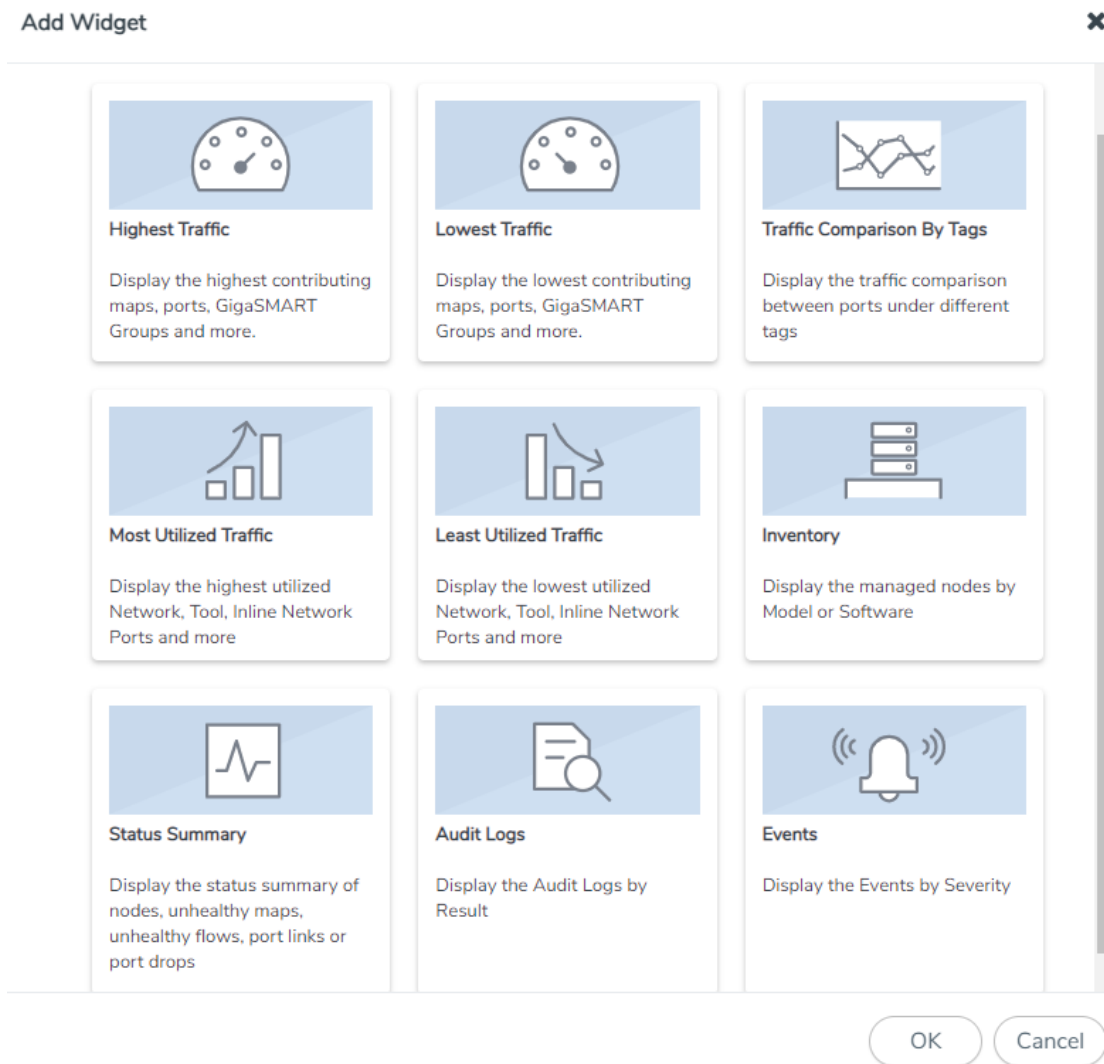


Figure 24 Add New Widget

- In the Add New Widget window, select **Status Summary** and click **OK**. The Status Summary configuration window is displayed.

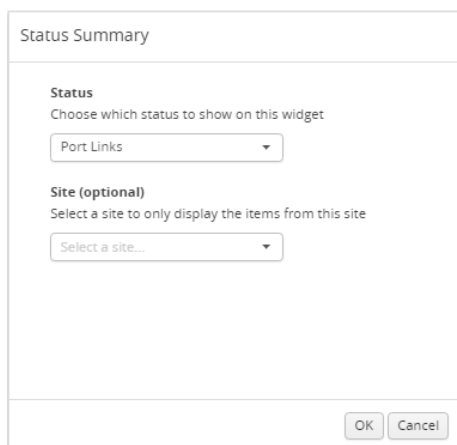


Figure 25 Status Summary Configuration

4. From the **Status** drop-down list, select one of the following:
 - Node—For information, refer to [Nodes' Status Summary](#).
 - Port Links—For information, refer to [Port Link Status Summary](#).
 - Unhealthy Maps—For information, refer to [Unhealthy Maps](#).
 - Port Drops & Errors—For information, refer to [Port Drops and Errors](#).
5. Select the required tag key and tag value combination for which the highest traffic distribution must be displayed. This step is optional.
6. Click **OK**.

Unhealthy Fabric Maps

The unhealthy flow maps widget displays the list of unhealthy flow maps.

The Unhealthy Fabric Maps status summary widget lists the maps that are in unhealthy state. The health of a fabric map is determined by the health status of its associated components such as maps, ports, port groups, port pairs, GigaStream, tool port, GigaSMART group, virtual port and GigaSMART operations. If the status of any one of the component is down, the corresponding fabric map is also considered unhealthy.

The Unhealthy Maps widget shows the fabric map alias and the current status of the unhealthy fabric map. The possible statuses are:

- Critical (red)
- Warning (amber)
- Unknown (gray): The health status of a map is shown as gray when the traffic health is still being computed. The status will be updated eventually.

Audit Logs

The Audit Logs widget shows the audit logs of successful and failed events. Optionally, the audit logs can be displayed for a specified site. When a particular site tag is selected, the audit logs pertaining to the clusters and nodes associated to that site are displayed in the Audit Logs dashboard.

The Audit Logs widget presents a graph that allows you to quickly view the number of logs in successful or failure state. In the graph, the state is indicated by color. The possible log results are:

- Success (green)
- Failure (red)

Hovering the mouse over an area in the graph displays the percentage of audit logs in that result. You can also specify the audit log statuses that have occurred over the past hour, day, week, or month. [Figure 26 Audit Logs by Result](#) shows the audit log results over each of the time periods.

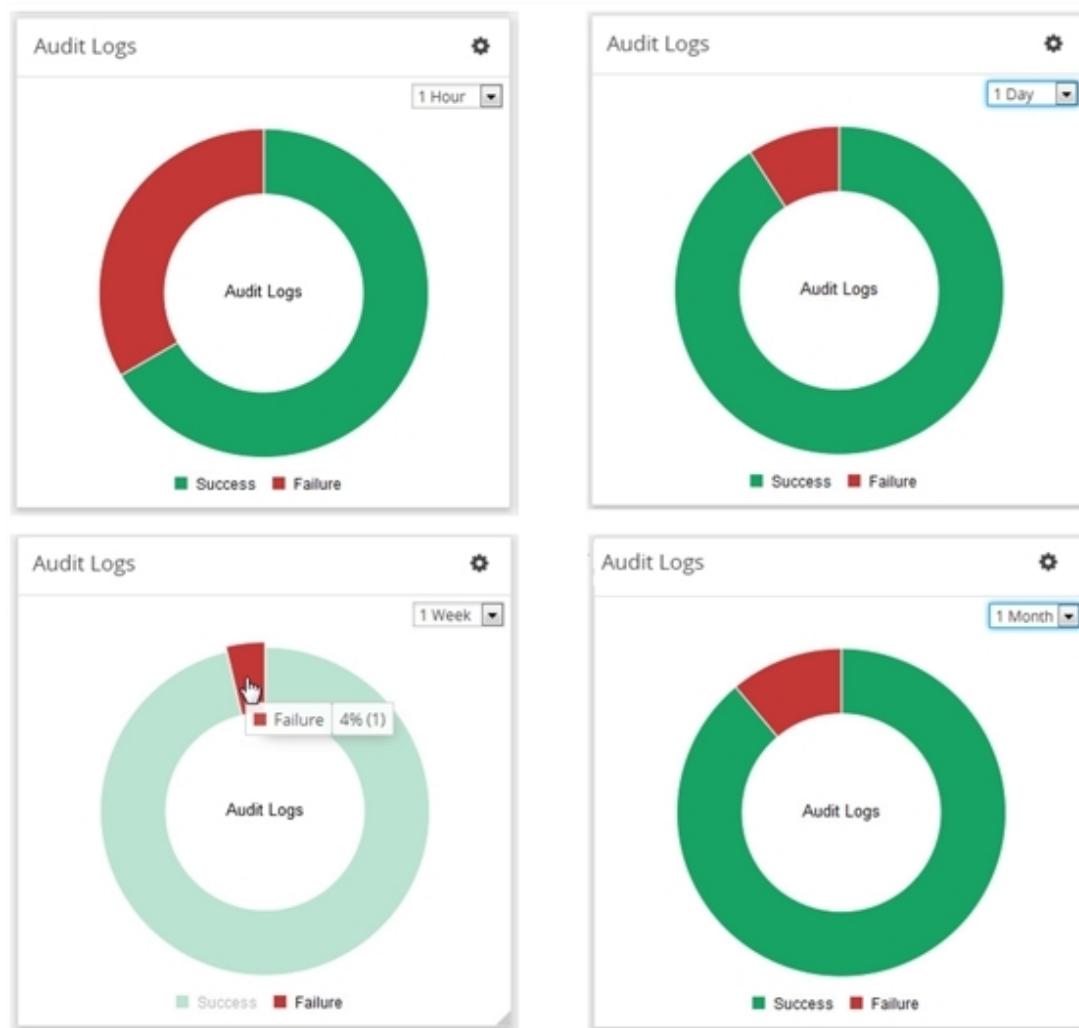


Figure 26 *Audit Logs by Result*

In this example, the Audit Logs widget shows that there is a log with the failure status that has occurred in the last hour. When you go to the audit logs page, you can see the entries, which matches with the information displayed in Audit Logs widget: two successes and one failure due to an incorrect log in.

To configure the Audit Logs widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
2. Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 6Add New Widget](#).

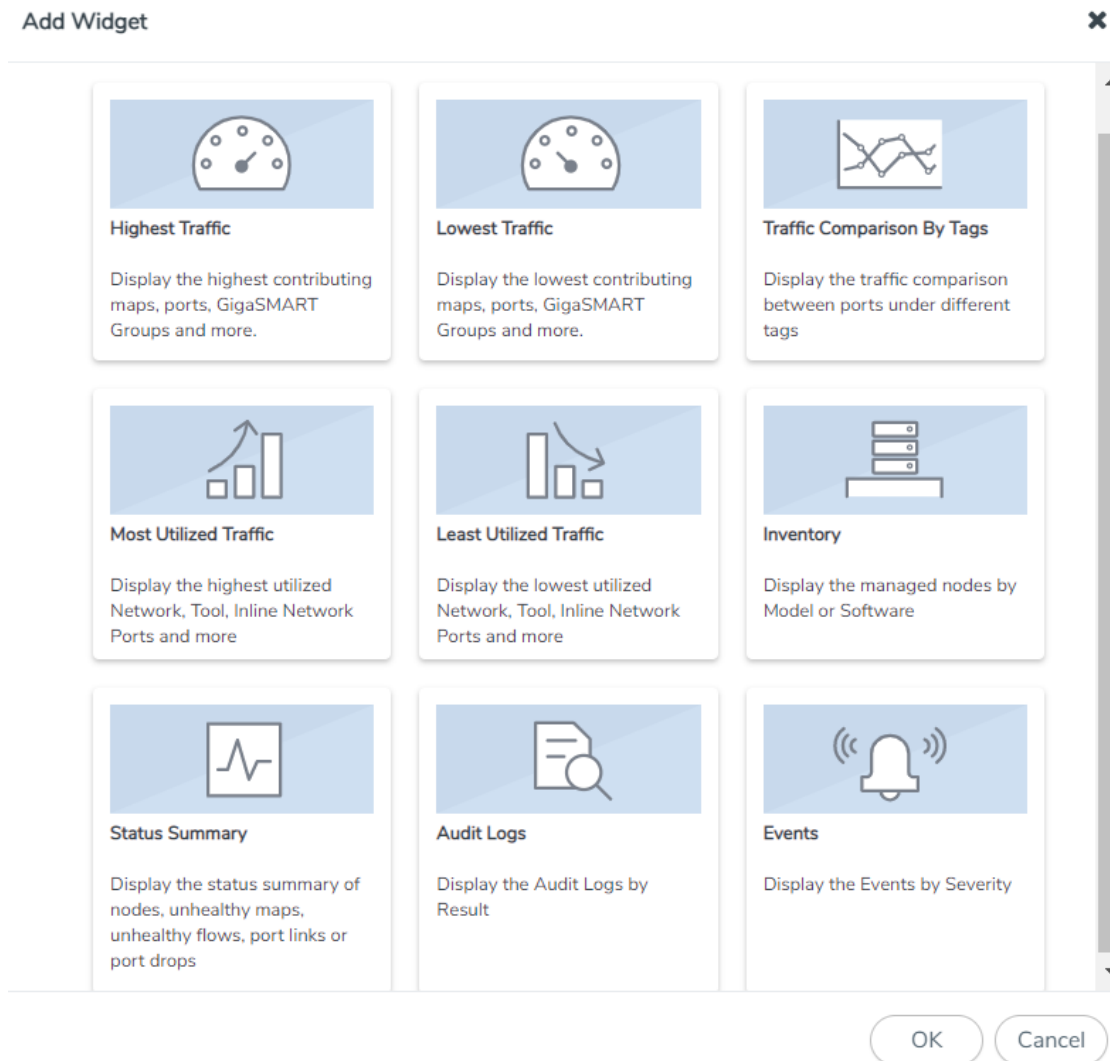


Figure 27 Add New Widget

3. In the Add New Widget window, select **Audit Logs** and click **OK**. The Audit Logs configuration window is displayed. Refer to [Figure 16Most Utilized Traffic Configuration](#).

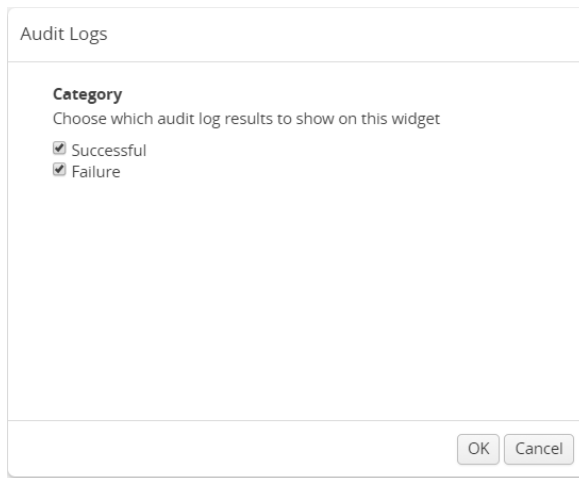


Figure 28 *Status Summary Configuration*

4. Choose the category of audit log results you want to view:
 - Successful
 - Failure
5. Click **OK**.

Events

The Events widget presents a graph that shows the number of events that have occurred within a particular severity level, which is indicated by a color in the graph. Optionally, the events can be displayed for a specified site. When a particular site tag is selected, only the events pertaining to the clusters and standalone nodes associated to that site are displayed in the Events dashboard.

The possible severity levels are:

- Information (blue)
- Major (orange)
- Minor (yellow)
- Critical (red)

Hovering the mouse over an area in the graph displays the percentage and the number of events that have occurred within the selected severity level. You can also select the time period to view the number of events that have occurred over the past hour, day, week, or month.

[Figure 29 Events Widget](#) shows the number of events that have occurred in the past week in each severity level for all sites. If you want more detail about the events, select **Events** in the Physical page.

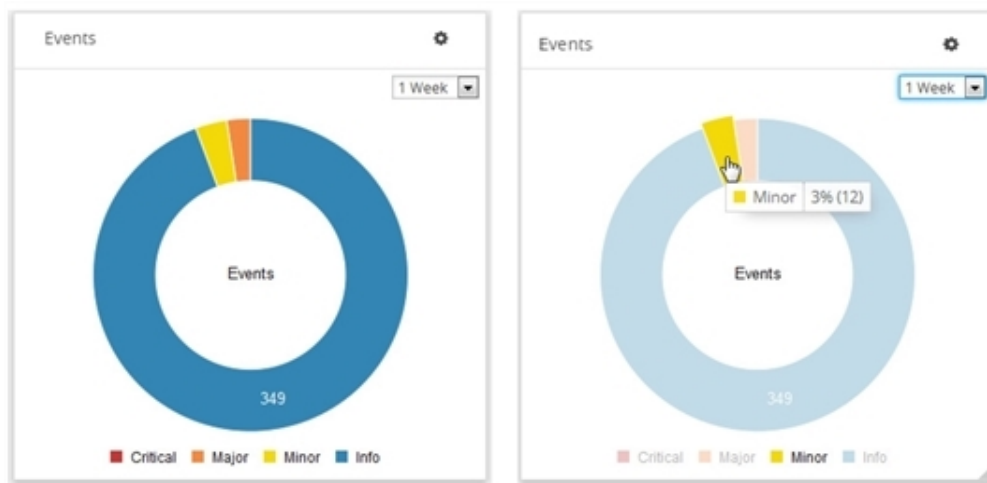


Figure 29 Events Widget

Figure 29 Events Widget shows the number of events that have occurred in the past week in each severity level for the tag Santa Clara site.

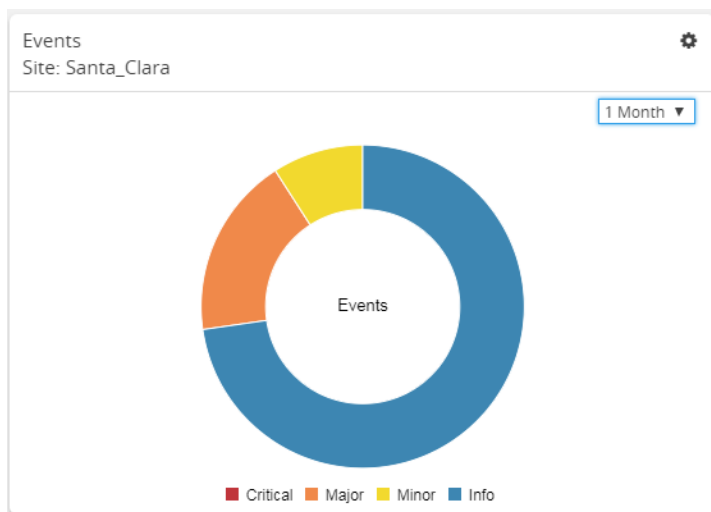


Figure 30 Events Widget for Santa Clara

To configure the Events widget:

1. On the left navigation pane, click on  and from the Physical & Virtual dashboard page, select the profile in which you want to add the widget.
2. Click **Add New Widget**. The Add New Widget window is displayed. Refer to [Figure 6Add New Widget](#).

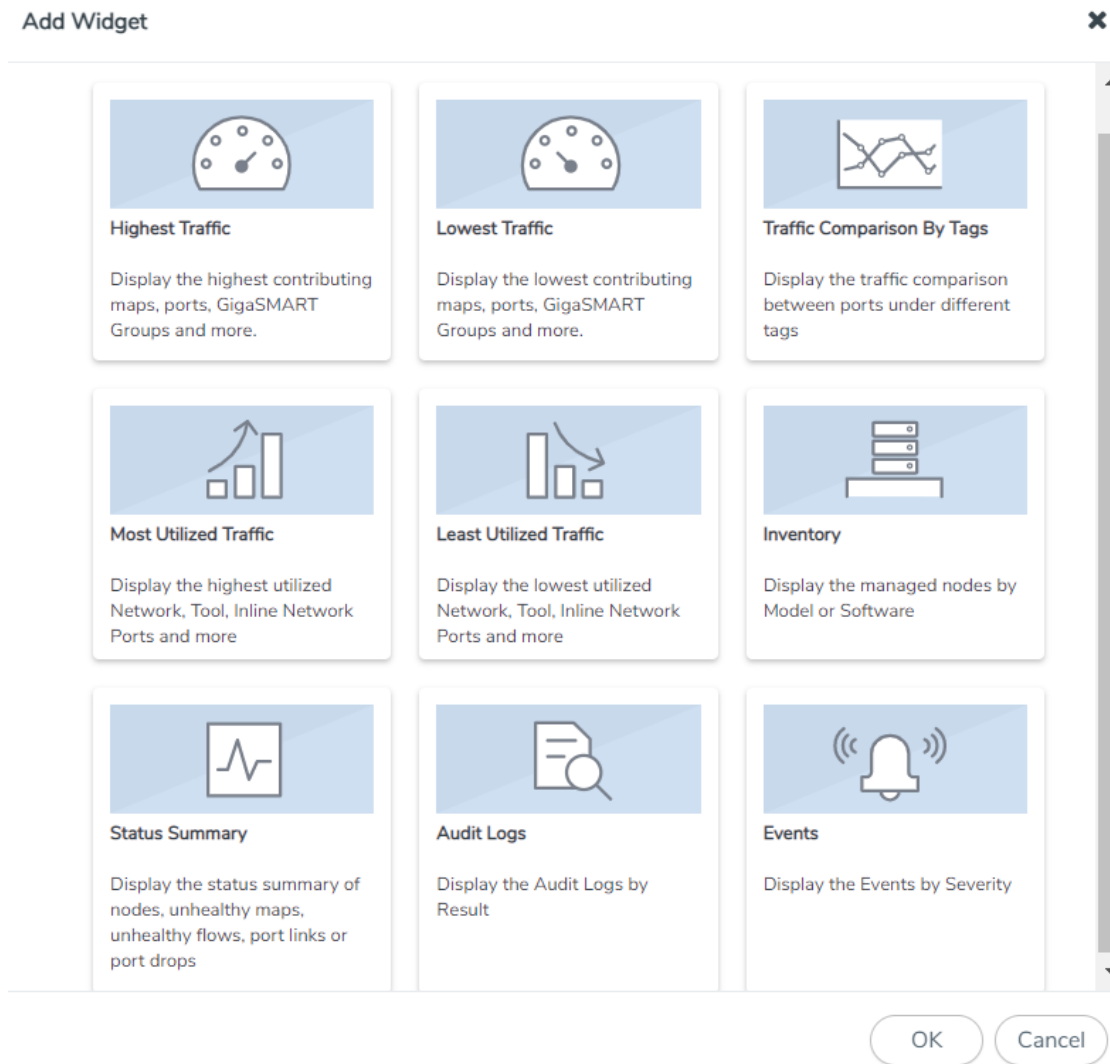
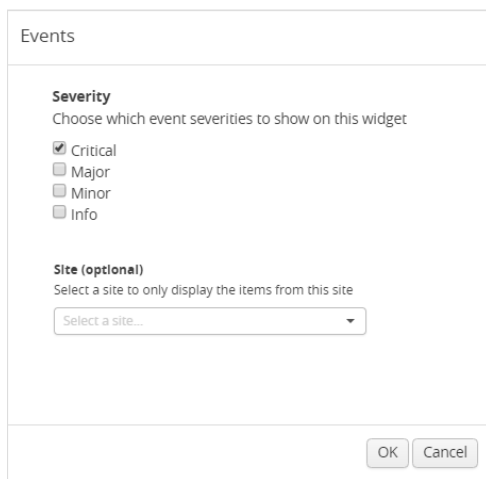


Figure 31 Add New Widget

3. In the Add New Widget window, select **Events** and click **OK**. The Events configuration window is displayed. Refer to [Figure 16Most Utilized Traffic Configuration](#).



The image shows a configuration window titled "Events". Inside, there is a section labeled "Severity" with the instruction "Choose which event severities to show on this widget". Below this are four checkboxes: "Critical" (checked), "Major", "Minor", and "Info". There is also a section labeled "Site (optional)" with the instruction "Select a site to only display the items from this site". Below this is a dropdown menu with the text "Select a site...". At the bottom right of the window are "OK" and "Cancel" buttons.

Figure 32 Status Summary Configuration

4. Choose the event you want to view in the widget:
 - o Critical
 - o Major
 - o Minor
 - o Info
5. Select the required tag key and tag value combination for which the events must be displayed. This step is optional.
6. Click **OK**.

GigaVUE-FM Health Dashboard

This chapter describes the Health Monitor Dashboard of GigaVUE-FM.

This chapter covers the following topics:

- [Overview of GigaVUE-FM Health Dashboard](#)
- [Alarm Thresholds and Notifications](#)

You can access the Health Monitor Dashboard and view the current system performances such as CPU, Memory and Disk Usage without being authenticated in to GigaVUE-FM. Type `<fmip>/fmHealth` in your browser to view the Health Monitor Dashboard.

Overview of GigaVUE-FM Health Dashboard

GigaVUE-FM is the central management appliance for the visibility fabric. Therefore, knowing its current health is important in order to maximize the availability of the appliance. The Health Monitor dashboard provides health information about GigaVUE-FM and makes it possible to do the following:

- Detect problems with GigaVUE-FM so that they can be responded to in a timely fashion.
- Provide alerts about issues that could impact the performance, such as CPU or disk over-utilization.

The Health Monitor provides the following monitors:

- CPU utilization
- Memory utilization
- Disk utilization



Figure 33 Health Monitor Dashboards

Note: If the percentage displayed in a pie-chart is negligible or less, then it would be difficult to click on the pie-chart arc and view the details.

CPU Utilization

The CPU Utilization Monitor displays overall CPU usage over time, providing information about peak CPU usage. This indicates whether there is sufficient CPU processing power for the currently deployed GigaVUE-FM appliance deployment. For example, peak CPU usage above a high-utilization mark of 90 for a long period for more than 30 minutes could indicate that the CPU power of the server is not adequate for GigaVUE-FM to manage the size of the deployed visibility fabric.

The CPU Utilization Monitor displays utilization as donut and time charts. The donut chart shows the percentage of utilized and available CPU. The time chart shows utilization at specific intervals. By clicking on a point in the time chart, you can see the utilization at a specific point in time. In [Figure 34 CPU Utilization Monitor](#), the CPU utilization at 10:49:55 AM is 1.0 percent.

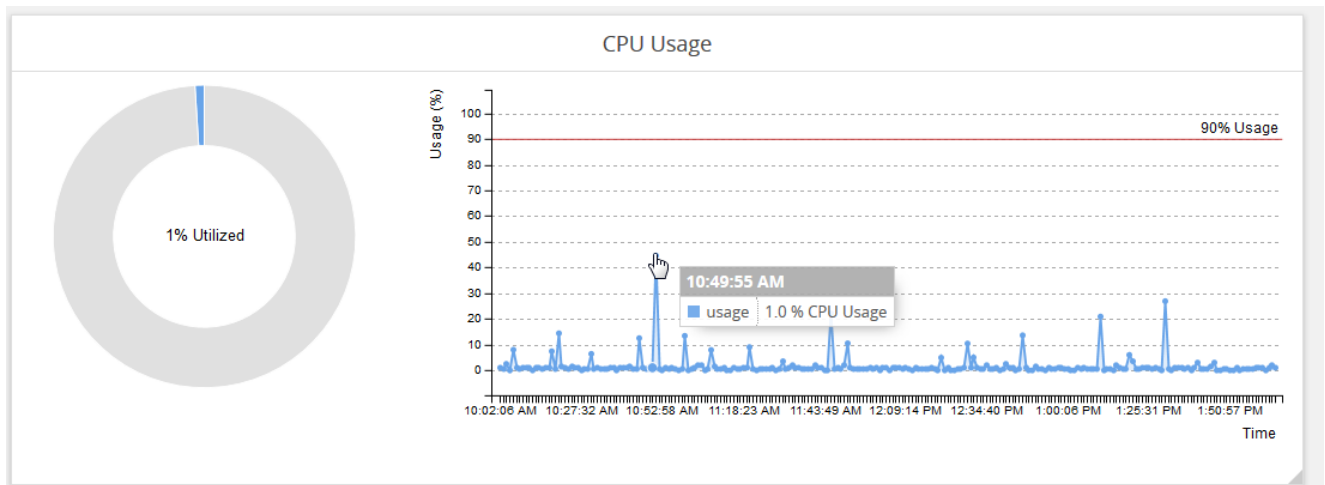


Figure 34 CPU Utilization Monitor

Memory Utilization

The Memory Utilization Monitor displays overall memory usage over time, providing information about peak memory usage. This indicates whether there is sufficient memory to handle the size of the visibility fabric managed by GigaVUE-FM. For example, memory usage above a high-utilization mark over a period for more than 30 minutes could indicate that the amount of memory supplied to GigaVUE-FM is insufficient.

The Memory Utilization Monitor displays utilization as dough nut and time charts. The dough nut chart shows the percentage of utilized and available memory. The time chart

shows utilization as specific intervals. By clicking on a point in the time chart, you can see the utilization at a specific point in time. In the following figure, the memory utilization at 11:48:49 AM is 17 percent.

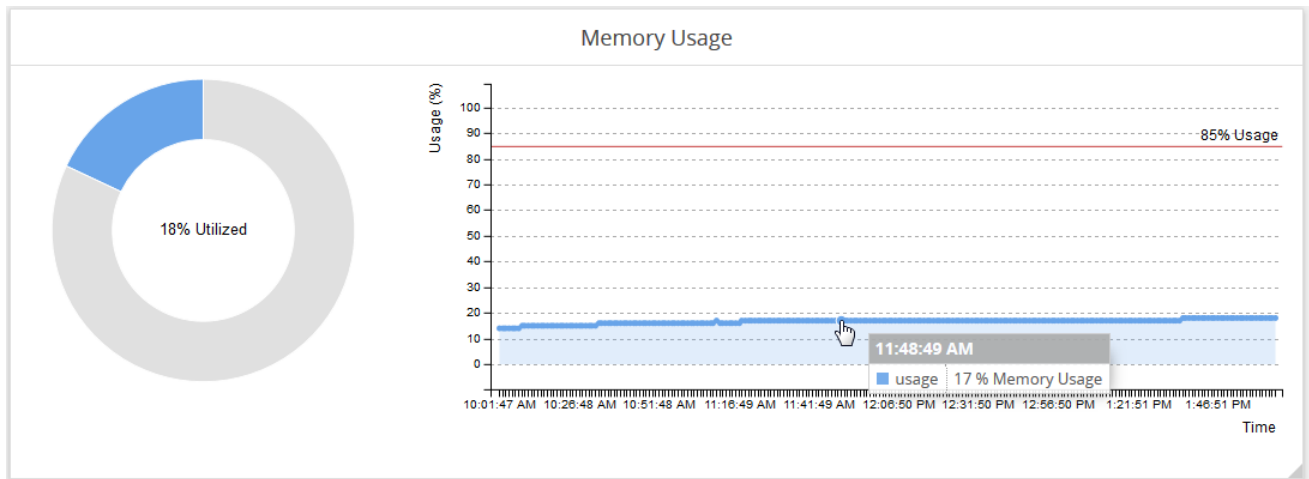


Figure 35 Memory Utilization Monitor

NOTE: When GigaVUE-FM starts up, the Memory Utilization Monitor displays around 60-65%. The utilization slowly increases up to 85% with the back end operations running and the memory gets stabilized at this point. A spike in memory is also observed when syslogs are more than usual.

Storage Utilization

The Storage Utilization Monitor displays disk usage levels over time for individual partitions, providing information about peak disk usage for GigaVUE-FM logs. This provides information that can help prevent outages due to disk out-of-space issues.

The Storage Utilization Monitor displays utilization for GigaVUE-FM logs. The bar charts show the percentage of disk utilization in the partitions for GigaVUE-FM logs. The time chart shows utilization as specific intervals for both partition. By clicking on a point in the time chart, you can see the utilization at a specific point in time. In [Memory Utilization](#), the disk usage at 11:16:01 AM for GigaVUE-FM logs is 18.5 percent and the disk usage for GigaVUE-FM data is 12%.

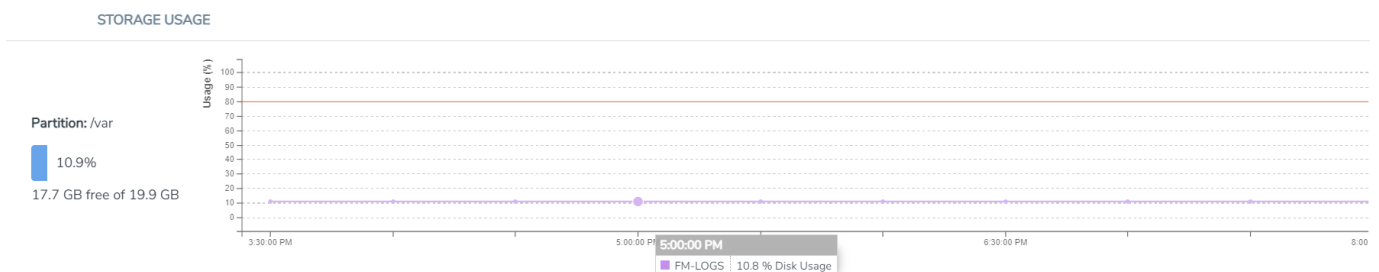


Figure 36 *Storage Utilization Monitor*

Alarm Thresholds and Notifications

For CPU, memory, and disk utilization monitoring, an alarm is triggered in the Alarms page if the following threshold levels are exceeded:

- CPU Utilization - 80%
- Memory Utilization- 90%
- File System (/var) - 80%
- File System (/config) - 80%

What Next?

Using Analytics you can create visual elements such as charts that are embedded as visualizations. To learn more about the data visualization capabilities in GigaVUE-FM, refer to [Analytics](#).

To learn about the administrative task in GigaVUE-FM such as User Management, Creating Roles and User Groups, Authentication and security, refer to [Administer GigaVUE-FM](#).

How to Add the GigaVUE-FM Instance Name

The default name of the GigaVUE-FM instance is GigaVUE-FM, and it is displayed on the footer.

When you have multiple GigaVUE-FM Instances running in your system, it becomes difficult to differentiate the instances and switch between tabs.

To customize the GigaVUE-FM instance name:

1. Go to **Settings** and select **System > Preferences**.
2. Click **Edit**.
3. In the **FM Instance Name** box, enter a name for the GigaVUE-FM instance.
4. Click **Save**.

The customized GigaVUE-FM instance name is displayed in the footer.

Notifications Panel

The Notifications icon in the top navigation bar displays a number if there are any system alerts. Immediate alerts appear on the left side of the page as individual pop-ups.

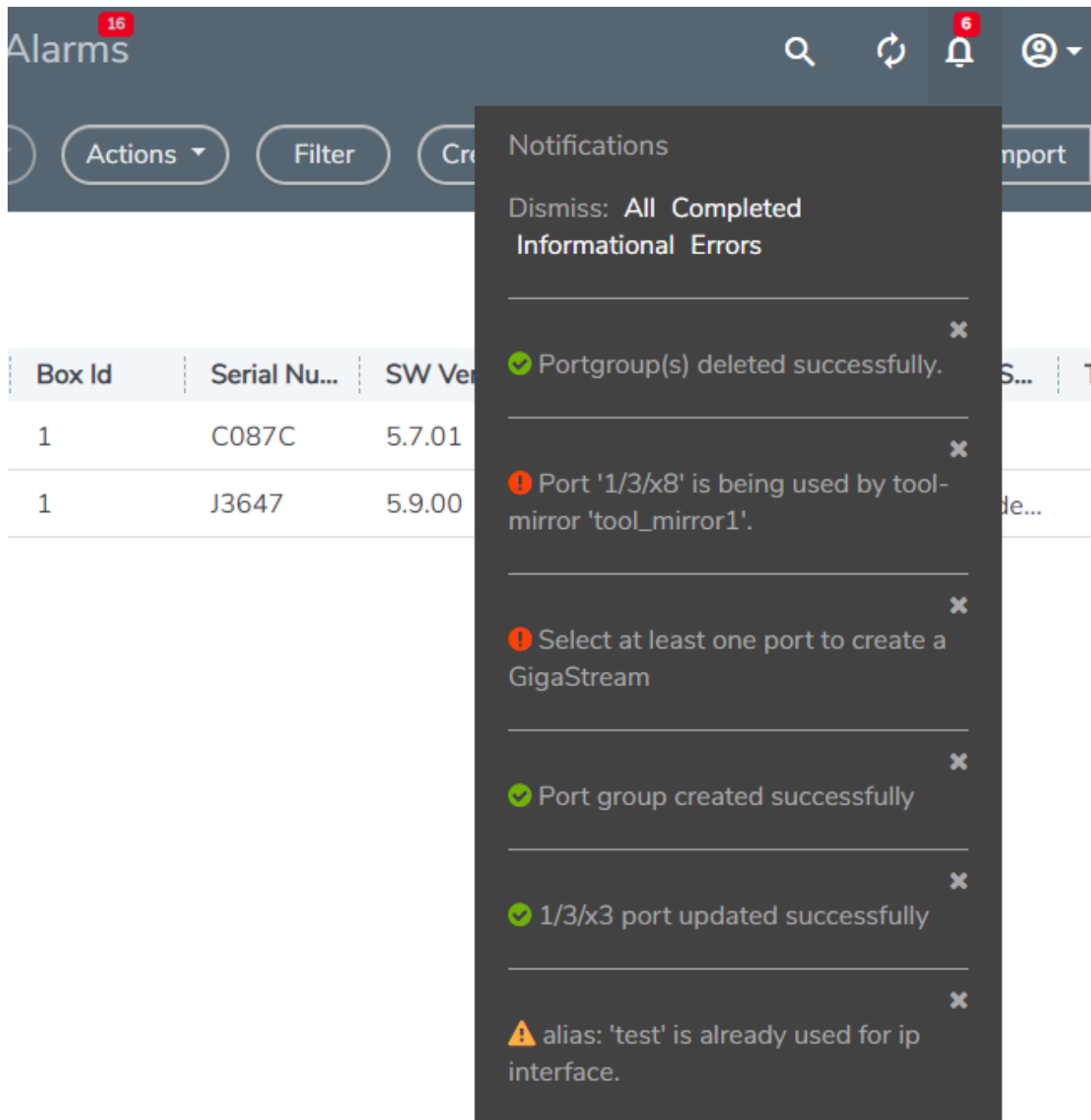


Figure 37 Pop-up messages

Long-term Notifications

Click on the Notifications icon to display a Notifications Panel listing long-term alert messages. If the list is long, a scroll bar appears on the left so you can scroll through the list.

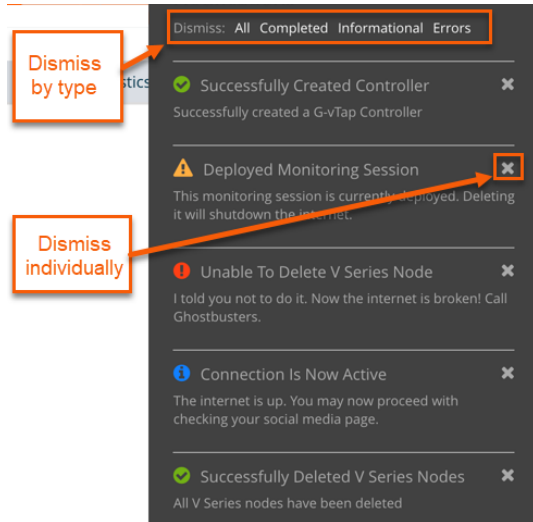


Figure 38 Long-term messages

Messages are updated as more information is received from packets. You can dismiss the individual messages or by type.

Notification Type Icons

Notification messages include a summary and a notification-type icon indicating the severity level of the alert. Some notifications have titles as well.

	Process Completed (green circle with a check mark)
	Warning (yellow triangle with an exclamation point)
	Error (red circle with an exclamation point)
	Information (blue circle with an "i")
	Alert being processed (gray spinner)

Notification Banners

Notification banners are displayed in the GigaVUE-FM GUI to alert users of critical or warning situations that require immediate user attention, such as the following:

- when disk space exceeds a predefined threshold limit.
- when the licenses are in expired state
- when Volume-based License (VBL) usage exceeds the daily usage allowance limit

Refer to the GigaVUE Licensing guide for banners related to licenses.

NOTE: You must be a read-only user to view the notification banners.

Notification Banners for Disk Space Utilization

The disk space in GigaVUE-FM is used to store statistical data and syslogs. External log files, sysdumps, and device image files also take up disk space. It is important to monitor the disk space, as increased usage beyond a threshold level results in system slowness, system instability, and UI inaccessibility. If appropriate action is not taken GigaVUE-FM will stop functioning.

GigaVUE-FM monitors the disk space utilization of the /config directory. Whenever the disk space usage exceeds a pre-defined threshold level, GigaVUE-FM performs the following steps sequentially:

1. Cleans the statistical data.
2. Disables syslog and stats collection services if the disk usage is still above the threshold. Corresponding alarms are triggered and displayed in the Alarms page. Email notifications are also sent to notify about the critical disk usage levels (if configured).
3. Sends SNMP traps

To alert the users immediately about the critical disk usage levels, starting from software version 6.2.00, notification banners are displayed when disk space usage level exceeds a specific threshold limit. Notification banners are displayed in the following cases:

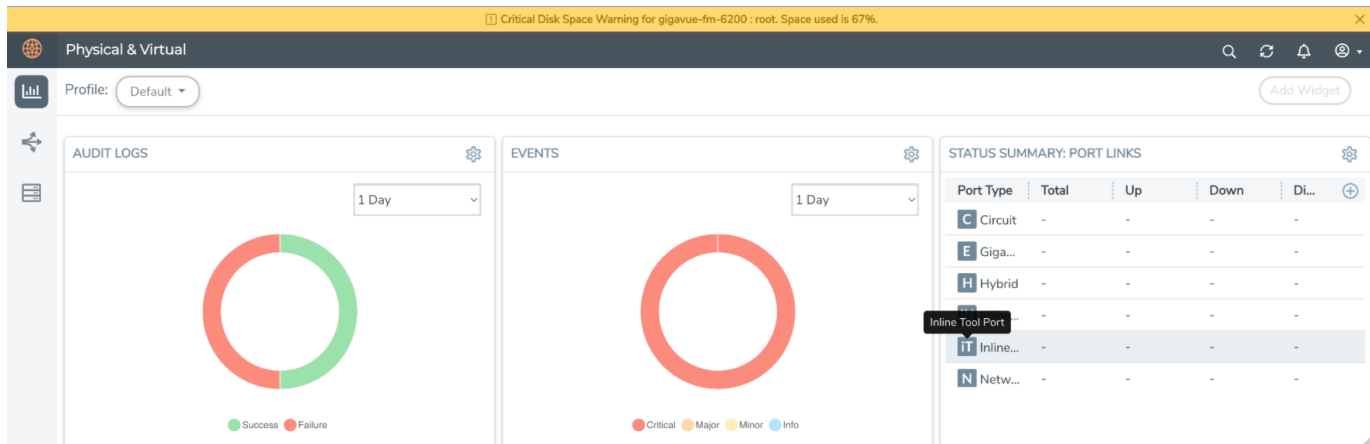
- When you login to a GigaVUE-FM instance.
- Near Real-time notifications also get displayed at the time when the disk usage exceeds the configured threshold value.

NOTE: Notification banners for disk space utilization alerts users about critical disk usage levels in all three partitions (/config, /var, /) of GigaVUE-FM.

Depending on the severity, the color of the banner varies:

- **Warning - Yellow-colored banner:** If disk space utilization has reached 60%.
- **Critical - Red-colored banner:** If disk space utilization has exceeded 75%

If the severity of the disk space utilization varies across the partitions, then the color of the banner is determined based on the highest severity level.



The screenshot shows the 'Preferences' page. A red banner at the top reads: 'Critical Disk Space Error for multiple partitions. Space used is 75% for atleast one partition.' The page includes a sidebar with navigation options like 'Node Details', 'IP Resolver', 'Backup/Restore', 'Images', 'Certificates', 'Event Notificat...', 'External Data ...', 'Licenses', 'Logs', 'Storage Mana...', 'Reports', and 'Tasks'. The main content area is titled 'My Profile' and contains form fields for 'Username' (admin), 'Password' (masked with asterisks), 'Email', and 'Group *' (Super Admin Group). A 'Change Password' link is next to the password field. A notification box at the top of the form states: 'Form elements marked with * are mandatory.'

If you click on the notification banner ribbon, a pop-up with details about the disk space utilization is displayed. See the following example:

Critical Disk Space Error



Please free up disk space on the partition(s) below as soon as possible or GigaVUE-FM will become slow, unresponsive or terminate. You can purge logs, delete uploaded images and backups to free up space.

Host Name	Partition	Space Remaining (GB)
gigavue-fm-6200	root	1.98 / 9
gigavue-fm-6200	config	8.80 / 40

OK

You may experience a slight delay while the notification banner pops-up and clears.

Disk utilization monitoring is also applicable in dynamic GigaVUE-FM High Availability setups. The details of the GigaVUE-FM HA host names are displayed in the pop-up.

NOTE: For information about how to free-up disk space refer to [How to Clean up Disk Space on a GigaVUE-FM Instance](#) for details.

How to Search in GigaVUE-FM

When searching for items, GigaVUE-FM performs a full search across multiple categories and displays the categories as part of the results. A Filter option is also available, which displays as a quick view, making it possible to quickly refine the search results.

GigaVUE-FM has an global search feature that allows you to search for information in GigaVUE-FM as well all the devices and device configurations managed by GigaVUE-FM. Essentially, if it is part of the GigaVUE-FM UI or managed by GigaVUE-FM, you can search for items based on keywords because almost all items are indexed for global search.

GigaVUE-FM enhances port alias search, allowing you to enter full or partial aliases to instantly find the corresponding port and all directly associated resources including maps, GigaStreams, inline components, port groups, and interfaces consolidated in a single result set for faster troubleshooting and impact analysis. Refer to the [Search Examples](#).

The search feature allows you to search for items across the following:

- Maps
- Roles and Users
- GigaSMART
 - GigaSMART Operations
 - GigaSMART Groups
 - Virtual Ports
 - NetFlow/IPFIX Generation
 - SSL Decryption
 - GTP Whitelists
 - Application Session Filtering (ASF)
- Ports
 - Port Groups
 - Port Pairs
 - Tool Mirrors
 - Stack Links
 - Tunnel Endpoints
 - IP Interfaces
 - Circuit Tunnels
 - GigaStreams
 - Port Alias
- Chassis and port inventory
- Node Clusters
- VMs
- IP, DNS, and MAC address

The following are not currently searchable: audit logs, events, NetFlow data, RBAC, IP ranges, or statistics.

Categories are another important component of Elastic Search. When you provide a keyword, the search system displays the matching category or categories related to the keyword search. This provides an automatic filtering of the keyword, helping to narrow your search. Some of the general categories are:

- Cluster
- GigaSMART
- Inline Bypass

- Maps
- NSX-V
- Ports
- Users
- VMware

You can refine the search categories by using the Filter feature (refer to [Filtering Search Results](#)) to further narrow the search results. For example, if the search keyword falls into the GigaSMART category, you can narrow the search further to NetFlow Records.

Performing a Search

To find an item in GigaVUE-FM, do the following:

1. Click the **Search** icon in the GigaVUE-FM top menu to open the Keyword field.
2. Type a keyword in the text field.

As you enter the keyword, the system displays the categories in which the keyword appears and the total matches in that category along with the specific instances. For example, as shown in [Figure 39GigaVUE-FM Search](#), you start to enter an IP address. The search shows that 10.115 occurs in the Cluster category 29 times, Ports 1 time, and IP Interfaces 2 times.

NOTE: You can type up to 128 characters in the **Keyword** field. This is because you cannot create a component with alias more than 128 characters (Map aliases, Port aliases and other such aliases).

The Search results start appearing when you type a minimum of three characters in the search pane.

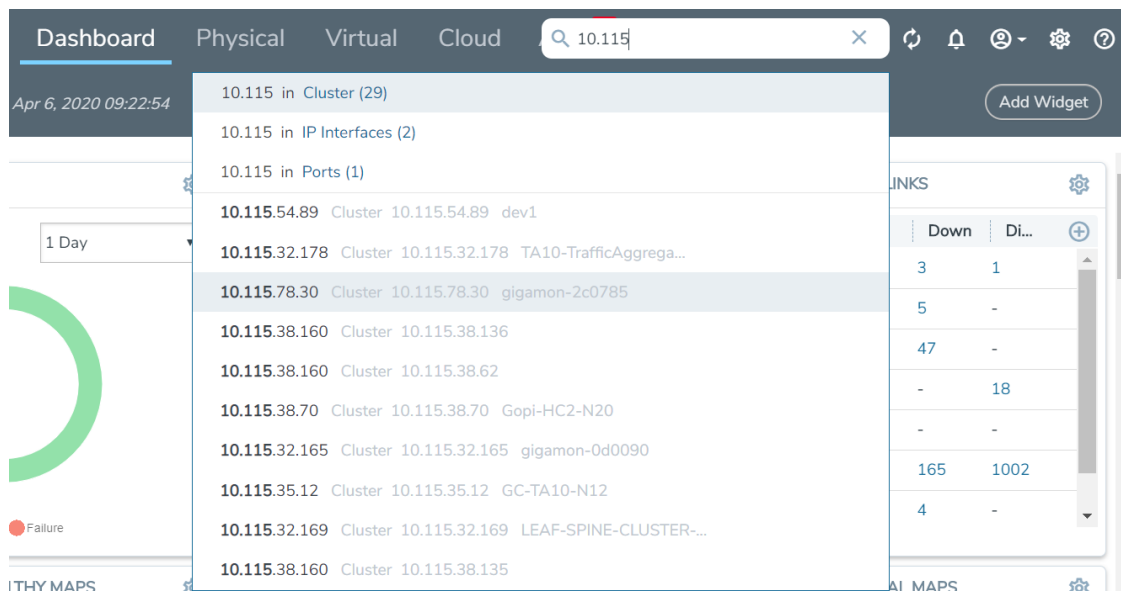


Figure 39 GigaVUE-FM Search

3. Once you are done entering the keyword, you can scroll through the list by using the up and down keys on the keyboard. Select an item by pressing the Enter key.
 - o Selecting a category, displays all the results in that category, using the category as a filter. You can further refine the results by clicking the **Filter** button. For details on filtering, refer to [Filtering Search Results](#).
 - o Selecting a specific result opens the page for that item.

If the search result is a cluster or standalone node, clicking the results takes you to the Overview page of that node and the Keywords field displays the node's ID as shown in the following figure. When the node ID is displayed in the Keywords field, it indicates that the scope of searches is narrowed to the current node or cluster.

Search Examples

This section provides few examples to show how to use the global search feature. The examples cover the following:

- [Search Maps](#)
- [Search for Roles and Users](#)
- [Search Ports](#)

Search Maps

You can search for maps based on the map alias, IP address associated with maps, MAC address, port status and so on. Click on the **Filter by Cluster** icon  in the search results page to refine the search results based on the cluster ID.

This section provides several examples of searching Maps:

- [Example 1: Search for a Map by Alias](#)
- [Example 2: Search for a Map with an IP Address](#)
- [Example 3: Search for a Map with a MAC Address](#)
- [Example 4: Search for Maps with Down Ports](#)

Example 1: Search for a Map by Alias

In this example, you are looking for a map where you remember the map's alias but are not sure which node or cluster it is on.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and start typing the map alias. In this example, Up.

As you type, the search displays the categories and items that match the keyword.

[Figure 40 Searching by Map Alias](#) shows the search results and you can see that the map with Alias Up is on node 10.60.94.73 without typing the entire string.



Figure 40 Searching by Map Alias

2. In the search results, click on Up-1.

GigaVUE-FM opens the Map page as shown in [Figure 41Map Page](#).

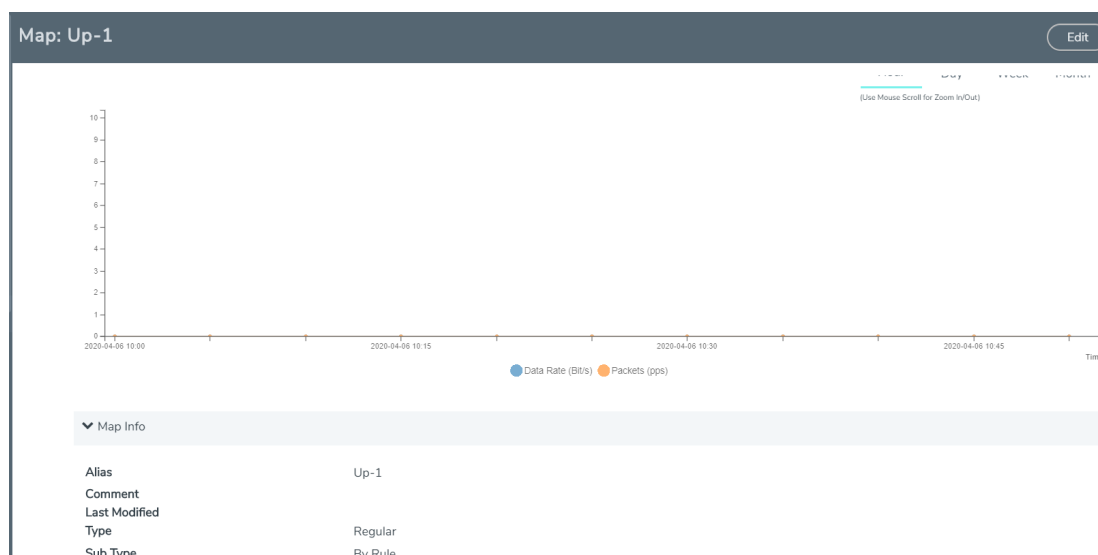


Figure 41 Map Page

Example 2: Search for a Map with an IP Address

In this example, you are searching for a map or maps that contain a specific IP address.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and start typing an IP address. In this example, the IP address is 10.60.94.73.

As you type the search displays the categories and items that match the keyword.
[Figure 42Search for IP Address](#) shows the search results.

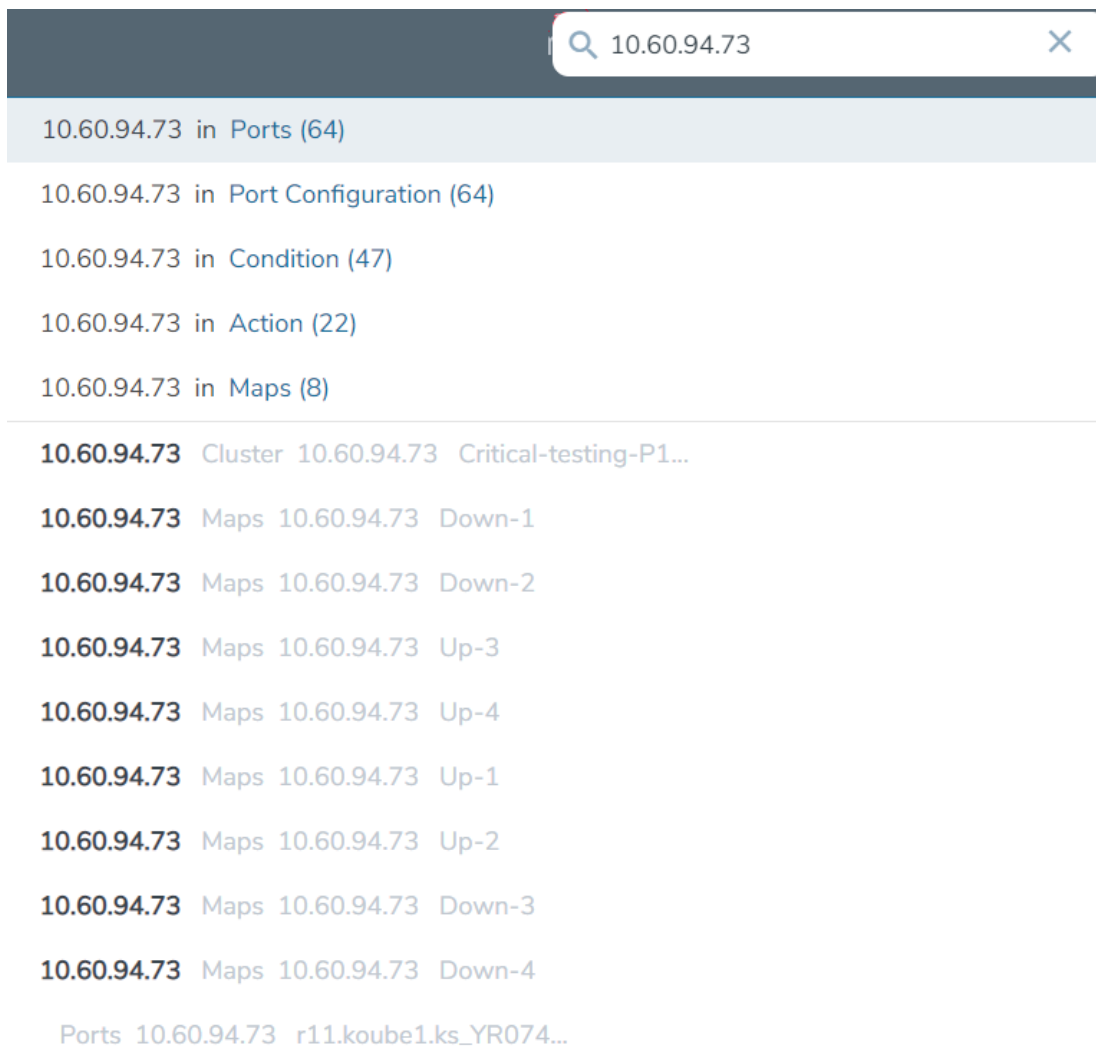


Figure 42 Search for IP Address

- Click on Maps in the categories section of the search results.

The Filter page opens. [Figure 43 Search Result Filter Page](#) shows the results with maps that contain the IP address. In this scenario, the item of interest is Down-1, so you click on the cluster name.

Search Results for "10.60.94.73"							Filter
Filtered By: none							
Alias	Cluster ID/Device IP	Type	Source ports	Destination Ports	Map Status	Number of Rules	
Down-1	10.60.94.73	regular	1/1/x1,1/1/x2	1/1/x57	Port(s) r11.koube1...	28	
Down-2	10.60.94.73	regular	1/1/x3,1/1/x4	1/1/x59	Map is Healthy	28	
Up-3	10.60.94.73	regular	1/1/x29,1/1/x30,1/1/x3...	1/1/x62	Multiple ports are L...	28	
Up-4	10.60.94.73	regular	1/1/x39,1/1/x40,1/1/x4...	1/1/x64	Multiple ports are L...	28	
Up-1	10.60.94.73	regular	1/1/x9,1/1/x10,1/1/x11...	1/1/x58	Multiple ports are L...	28	
Up-2	10.60.94.73	regular	1/1/x19,1/1/x20,1/1/x2...	1/1/x60	Multiple ports are L...	28	
Down-3	10.60.94.73	regular	1/1/x5,1/1/x6	1/1/x61	Map is Healthy	28	
Down-4	10.60.94.73	regular	1/1/x7,1/1/x8	1/1/x63	Map is Healthy	28	

Figure 43 Search Result Filter Page

A Map quick view opens, showing the information for the map.

Example 3: Search for a Map with a MAC Address

In this example, you are searching for a map or maps that contain a specific MAC address.

1. Click the **Search** icon in the GigaVUE-FM header to open the Keyword field and start typing an IP address. In this example, the IP address is 11:11:11:11:11.

After entering the MAC address in the Keyword field, only one map is found as shown in [Figure 44Search for MAC Address](#).

**Figure 44** Search for MAC Address

2. Click on the result with the map named MacSrcMap to view the map details.

Example 4: Search for Maps with Down Ports

In this example, you are looking for maps that have a port that is in the “down” state.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and type down.

As shown in [Figure 45Search Results for down Keyword](#), the keyword occurs in several categories.

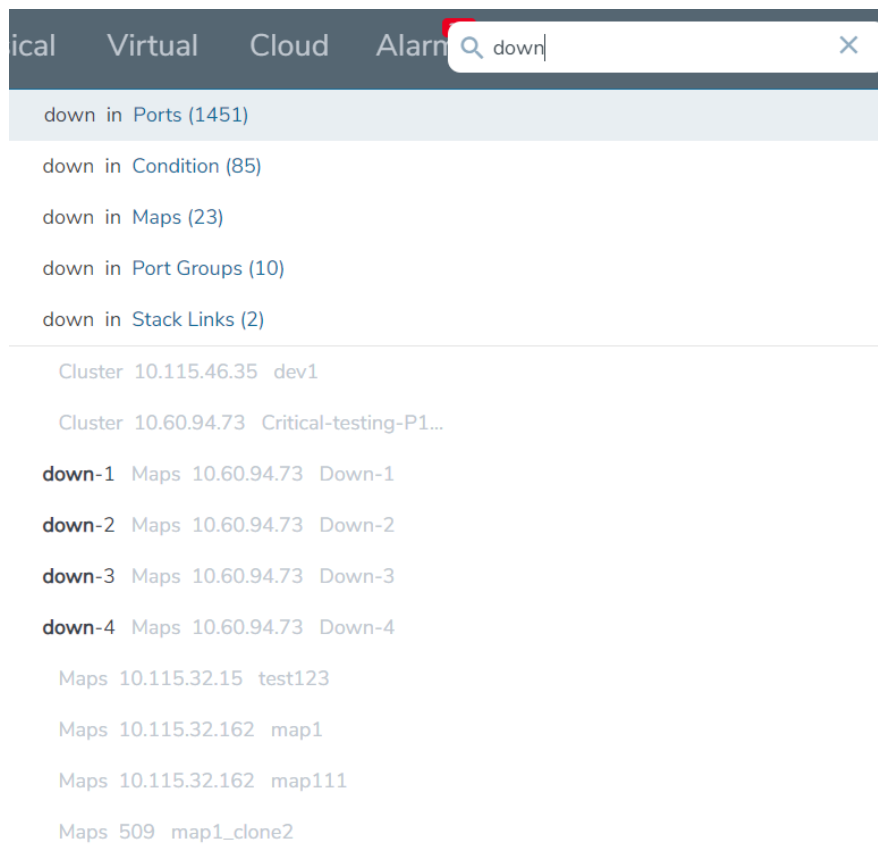


Figure 45 Search Results for down Keyword

2. Because you are searching for Maps, you click on the Maps category.

Search for Roles and Users

This section provides examples of searching for a role and for a user:

- [Example 1: Search for Monitor Role](#)
- [Example 2: Search for a User](#)

Example 1: Search for Monitor Role

In this example, you are looking for where the fm_User role is applied.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and type Monitor.

As shown in [Figure 46Categories for Monitor.](#), the keyword occurs in the several categories.

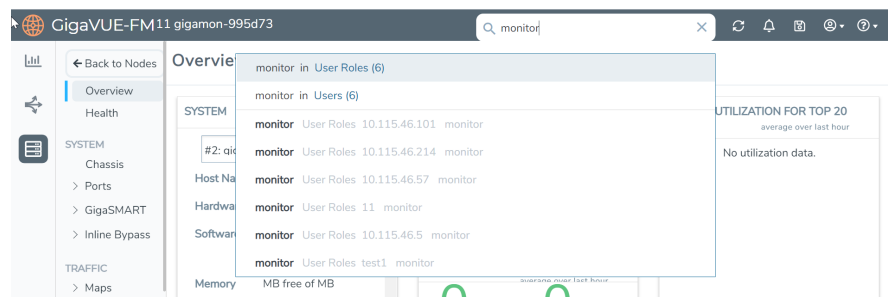


Figure 46 Categories for Monitor.

- 2. Select the User Roles category. The search results shows the nodes where the Monitor role is used.

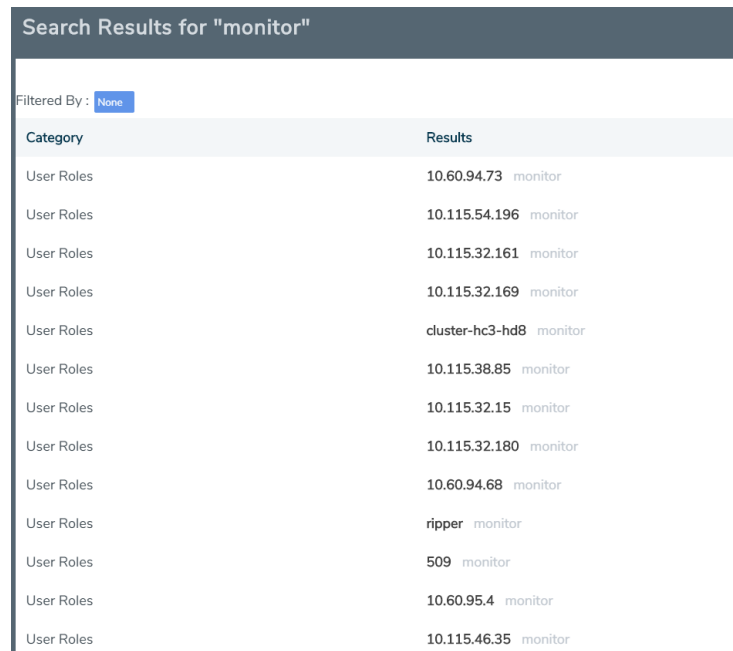


Figure 47 Search Results for Monitor.

- 3. From the search results, drill down further by selecting one of the results.
GigaVUE-FM takes you to the User Setup page for the selected cluster as shown in [Figure 48Role From Search Result](#) and indicates in the Keywords field that further searches are restricted to the cluster.

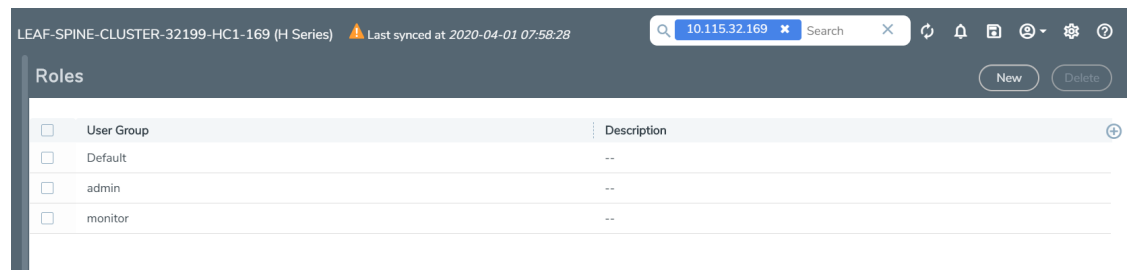
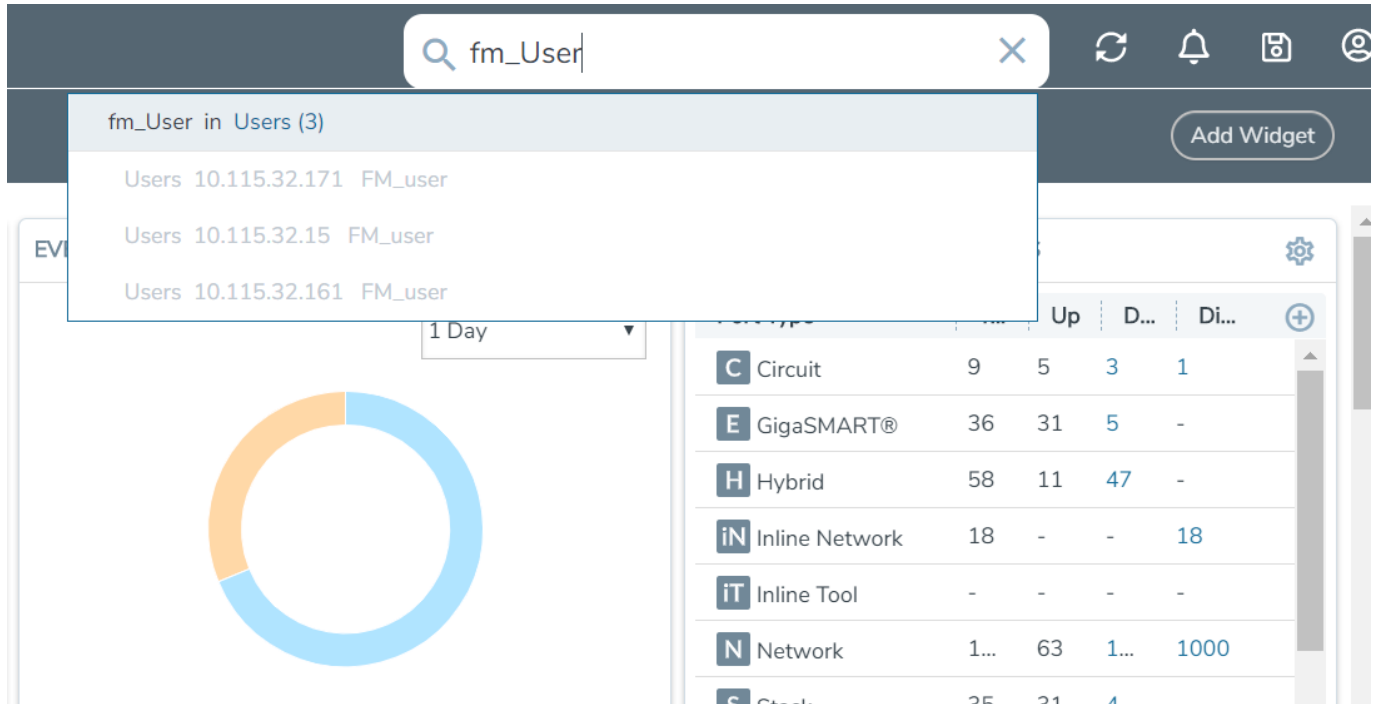


Figure 48 Role From Search Result

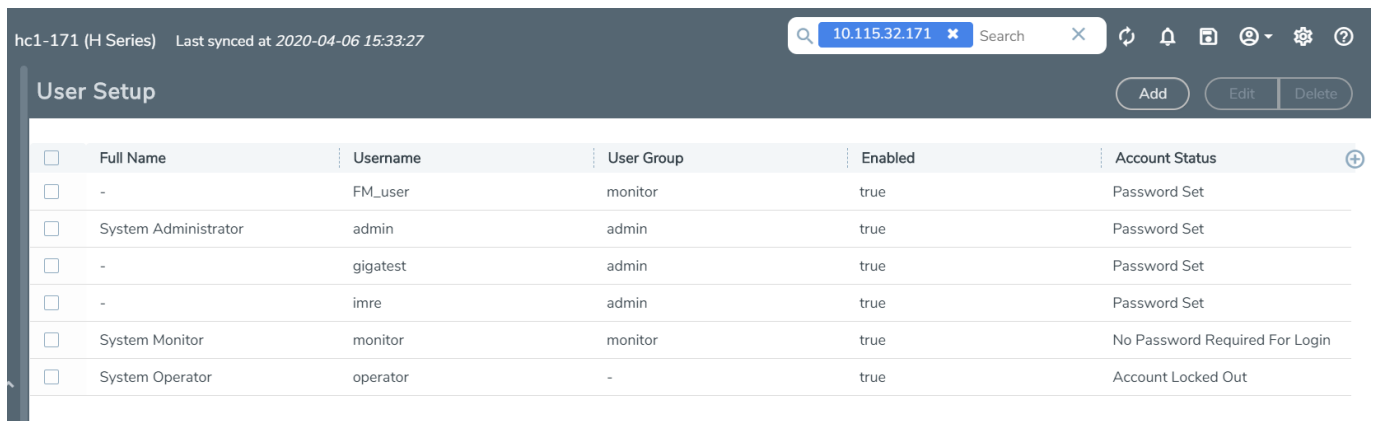
Example 2: Search for a User

In this example, you are looking for a specific user.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and type the user name for the user. In this example, the user is *fm_User*.



2. Click on *fm_User* in the categories and items list. The User page on the node with the *fm_User* opens a shown in the following figure. The Keywords field also indicates further searches are restricted to the current node.



Search Ports

NOTE: You can search for ports based on the port id, port alias, cluster ID/Device IP and so on. You can also view the neighboring ports information from the port search

results page. Click on the **Filter by Cluster** icon  in the search results page to refine the search results based on the cluster ID.

This section provides few examples related to searching for ports:

- [Example 1: Search for Down Ports](#)
- [Example 2: Search for Port Details of Devices Managed by GigaVUE-FM](#)
- [Example 3: Search for Port and Linked Resources Using a Port Alias](#)

Example 1: Search for Down Ports

In this example, you are searching for a particular port by its ID. This example also shows how to combine keywords.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and type the port ID 1/1/x5 followed by the keyword *down*.

As shown in [Figure 49 Categories Returned for Port ID and Down](#), the 1/1/x5 and down occur 60 times in the Port category.

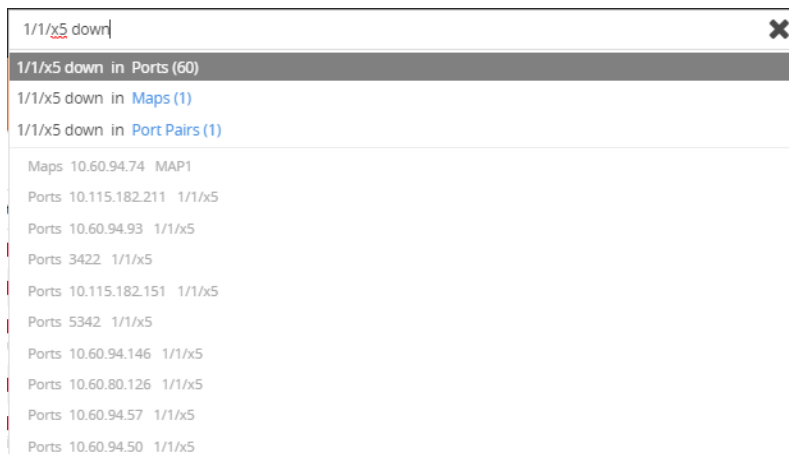


Figure 49 Categories Returned for Port ID and Down

2. Click on the Ports category to view the results.
3. Click on an item search results to see the port information. A Port quick view displays for the selected port as shown in [Figure 50 Port Quick View for Search Results](#).

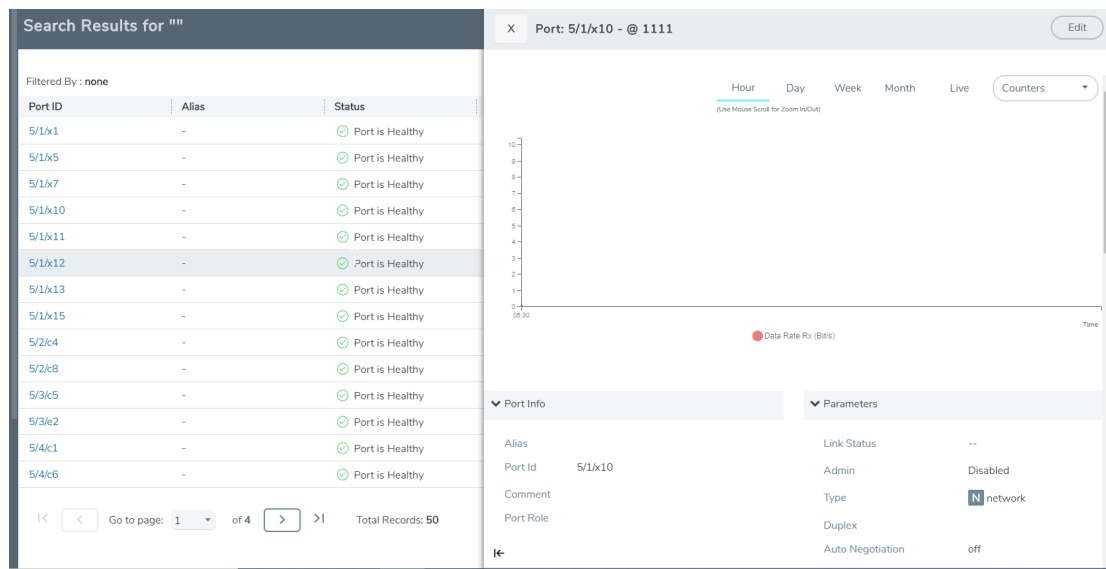


Figure 50 Port Quick View for Search Results

Example 2: Search for Port Details of Devices Managed by GigaVUE-FM

In this example, you want to retrieve port information from all the devices managed by GigaVUE-FM and that are up. This example also shows the use of a non-alphabetic character as the keyword.

1. Click the Search icon in the GigaVUE-FM header to open the Keyword field and type the back-slash character (/) and up.

As shown in [Figure 51 Categories Returned for Port Details of All Devices and up](#), the search returns results in several categories.

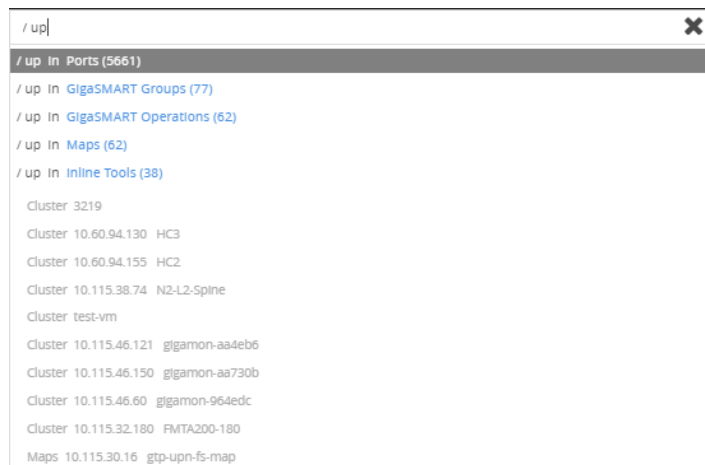


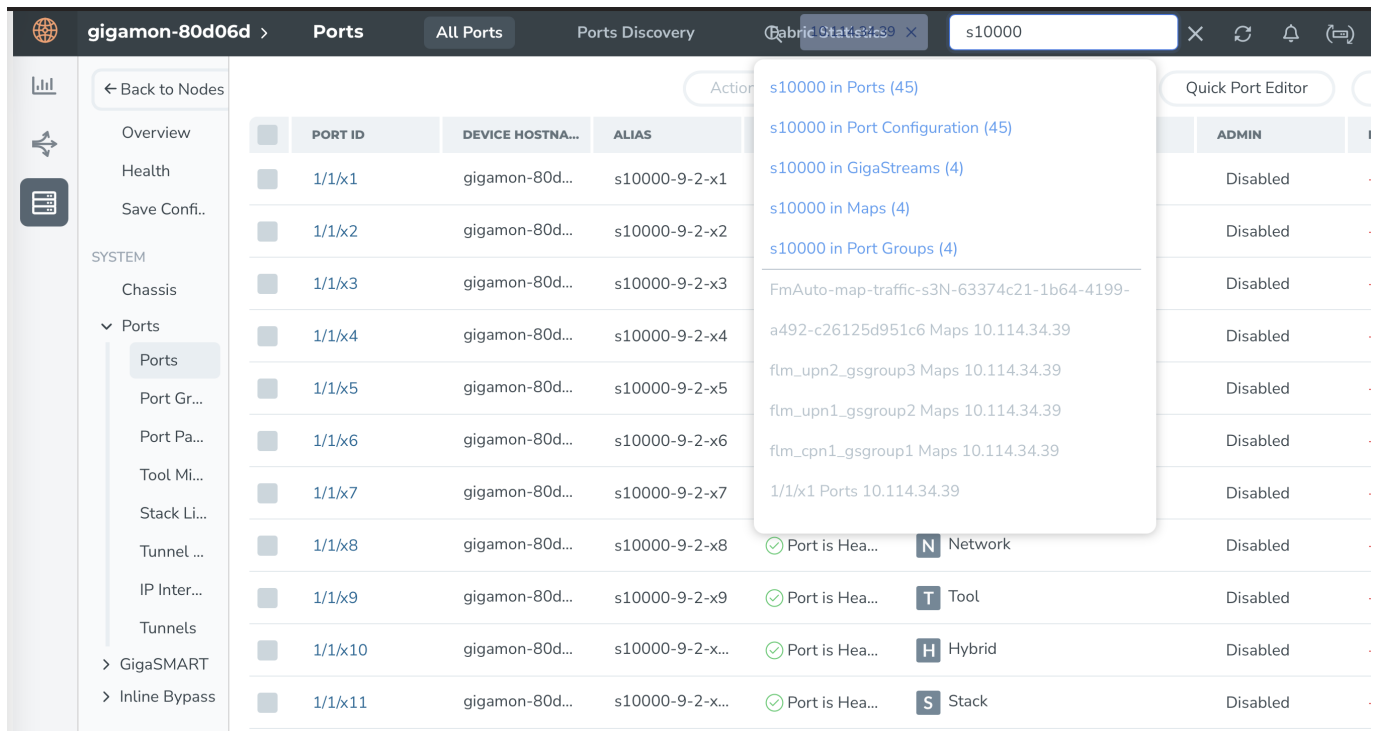
Figure 51 Categories Returned for Port Details of All Devices and up

2. Click on the Ports category to view the results.
3. Click on an item search results to see the port information.

Example 3: Search for Port and Linked Resources Using a Port Alias

In this example, to search using a port alias, perform the following steps:

1. Log in to GigaVUE-FM.
2. Click **Inventory > Physical > Nodes**.
3. Select the node.
4. Select **System > Ports > Ports**.
5. In the global search, searching by port alias returns the corresponding port and all directly associated resources, including maps, GigaStreams, inline components, port groups, and interfaces.



Filtering Search Results

When selecting a search result for a category, GigaVUE-FM opens a page that lists the results for that category.

To change the filter, do the following:

1. Click **Filter**.
The Filter quick view displays.
2. Add or remove filters by selecting items from the Filter quick view.

How to Apply Filters

The filter functionality allows you to search and narrow down the options you want to display on a particular page.

To use the filter functionality, do the following:

1. Click on the **Filter** button.
2. The **Filter quick view** dialog is displayed.
3. Specify the parameters to be filtered.

The filter selection appears above the list for reference. To remove a particular filter, click on the 'x' icon next to the filtered item.

4. Click the 'x' icon to exit the Filter quick view dialog.

The following figure shows how the applied filters are displayed on the GigaVUE-FM instance page:

The screenshot shows the GigaVUE-FM interface with the 'Ports' tab selected. The top navigation bar includes 'All Ports', 'Ports Discovery', 'Fabric Statistics', and 'Header Stripping Statistics'. The left sidebar shows a tree view with 'Ports' selected. The main area displays a table of ports with columns: Port Id, Devic..., Alias, Status, Type, Speed, Admin, Link S..., Trans..., SFP P..., Avg U..., Port F..., Disco..., Giga..., Rx On..., and T... The table lists 12 ports, with the first 10 visible. Above the table, a row of filter buttons is shown: 'Box ID : 10/1 X', 'Box ID : 10/2 X', 'Box ID : 10/3 X', 'Box ID : 10/4 X', 'Box ID : 2/5 X', 'Box ID : 2/3 X', 'Box ID : 2/4 X', and 'Box ID : 23/2 X'. An arrow points from the 'Box ID : 23/2 X' button to the 'Applied filters' label. The bottom of the interface shows pagination controls: 'Go to page: 1 of 12' and 'Total Records: 122'. The footer includes 'FM Instance: GigaVUE-FM', 'Node Sync Time: Jul 14, 2021 17:33:33', and 'Last Updated At: Jul 14, 2021 17:39:07'.

Port Id	Devic...	Alias	Status	Type	Speed	Admin	Link S...	Trans...	SFP P...	Avg U...	Port F...	Disco...	Giga...	Rx On...	T...
2/3/e1	ST-Inf...		✓ P...	E Gi...		Enabl...	up			—	—	none	Disabl...	N/A	COUNT...
2/3/x1	ST-Inf...		✓ P...	N N...	10G	Enabl...	up	sfp+ sr	-2.64 ...	0 / 46	—	none	Enabl...	N/A	COUNT...
2/3/x2	ST-Inf...		✓ P...	N N...	10G	Enabl...	up	sfp+ sr	-1.84 ...	0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x3	ST-Inf...			N N...		Disabl...	--			0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x4	ST-Inf...			N N...		Disabl...	--			0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x5	ST-Inf...	ESXi-...	✓ P...	C Ci...	1G	Enabl...	up	sfp cu		0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x6	ST-Inf...		✓ P...	T T...	10G	Enabl...	up	sfp+ sr	-2.34 ...	0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x7	ST-Inf...		✓ P...	N N...	10G	Enabl...	up	sfp+ sr	-2.21 ...	0 / 46	—	none	Enabl...	N/A	COUNT...
2/3/x8	ST-Inf...			N N...		Disabl...	--	sfp+ sr	-40 / -...	0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x9	ST-Inf...		✓ P...	T T...	10G	Enabl...	up	sfp+ sr	-2.37 ...	0 / 0	—	none	Enabl...	N/A	COUNT...
2/3/x10	ST-Inf...		✓ P...	T T...	10G	Enabl...	up	sfp+ sr	-2.34 ...	46 / 0	—	none	Enabl...	N/A	COUNT...

Analytics

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities for the following entities in GigaVUE-FM:

- Physical resources, specifically the nodes and the ports
- Virtual resources
- Alarm Management services
- GigaVUE-FM CPU, Memory and Disk Storage services

Using Analytics¹ you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects.

Analytics provides the following advantages:

- Real-time data for visualization as the required data is taken from GigaVUE-FM.
- Data to be analyzed and visualized is fetched based on the access control rights of the user.
- Trending Analysis: Visualize the trends in the traffic using pre-defined widgets.
- Capacity Planning: Utilization of resources based on health and inventory summary data.
- Generation of reports based on the available data.

Rules, Notes, and Limitations for Analytics

- All GigaVUE-FM users can create, edit and delete Analytics objects². However, you can perform these operations only on the objects created by you. You cannot delete or edit system-defined objects such as dashboards and visualizations.
- You can only view the Analytics objects created by other users, but you cannot edit them.
- There is no limit on the number of dashboards per user.
- The data available in dashboard is controlled by Role Based Access Control. That is, the data fetched depends on the accessibility rights of the user based on the user role and user-defined tags.

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

²Analytics objects include Dashboards, Visualizations and Saved Search Objects.

- The GigaVUE-FM backup/restore operation preserves both default and custom dashboards and visualization. This allows the dashboards and visualizations created in the earlier software versions to be restored in software version 5.13.00. This enables rapid resumption of GigaVUE-FM services and also provides the users the ability to operate and monitor the visualizations in GigaVUE-FM.
- Statistical dashboards display data in the following two tabs.
 - **Metric:** Displays maximum and average values of statistical counters for a specific time period, example Rx Ports Aggregated Max Traffic, Rx Ports Aggregated Average Drop Traffic.
 - **Trends:** Displays trend of statistical counters for a specific time period, example Rx Port Statistics (bps), Tx Port Statistics (bps), Tool GigaStream Maximum Rx Rate (bps) by member port Alias.
- The Inbound and Outbound Port Statistics dashboards display metric values for the top 1000 port elements in visualizations (as the total count it set to 1000).
- By default, all statistical dashboards display data based on a pre-selected cluster ID to avoid performance issues in a scaled environment.
- When browsing the Analytics page with 5 minute granularity, you can observe visual gaps in the displayed results. This is because stats collection happen in GigaVUE-FM with 5 minute granularity and a small delay of few seconds in stats collection can result in such gaps over time.
- For custom dashboards, enable the resource type filter to generate faster search results.
- For rate-based visualizations in the default system dashboards and cloned system dashboards, the axis-min setting (under panel option) is set to zero (0). An empty graph is therefore displayed when the data point values are zero. However, for visualizations in the dashboards created using the **Create Dashboard** option, you must manually change the axis-min setting to '0' for an empty graph to be displayed.
- For gauge-based visualizations "no data to display" message is received in case of the following scenarios:
 - GigaVUE-FM or the device is down during a particular time interval.
 - No traffic in the device and the axis-min panel option is set to value > 0.
- For rate-based visualizations, "no data to display" message is received in case of the following scenarios:
 - With *Drop Last Bucket* set to 'Yes' and time interval range < 15 minutes or time range has less than three data points.
 - With *Drop Last Bucket* set to 'No' and time interval range < 10 minutes or time range has less than two data points.
 - When a large time range is selected, the chart uses a larger data interval for rendering. If the selected range has insufficient data points, the visualization may appear empty. Select a smaller time range to improve trend visibility.

GigaVUE-FM Statistics and Data Roll-up

Until software version 6.0.00, the statistical dashboards of the physical and logical resources display data collected for a period of 30 days with 5 minute granularity (considered as the base index). Starting from software version 6.1.00, the statistical dashboards display data collected for a period of 35 days.

Resource	Related Statistical Dashboards
Ports	- Inbound Port Statistics - Outbound Port Statistics
Maps	Map Statistics
Nodes	Inventory Statistics
GigaStreams	- Circuit and Stack GigaStream Statistics - Tool GigaStream Statistics
GigaSMART	GS Group Statistics

With Data Rollup, GigaVUE-FM allows you to collect, summarize and display historical data up to 120 days with hourly granularity. Refer to the following notes:

- Starting from software version 6.1.00, Rollup is enabled by default. To disable Data Rollup, navigate to the Storage Management page. Refer to the GigaVUE Administration Guide for details.
- Rollup is applicable only for ports, maps, and map rules. You can search and analyze port statistics for a duration of up to 120 days. GigaVUE-FM collects statistical data from the day you upgrade to software version 6.1.00 or higher. Complete 120 days of data will be visible only from 121st day (and not backwards from the day GigaVUE-FM was upgraded).

NOTE: Associated Map Rule Visualization will only show the latest map rule count of 35 days.

- On upgrading to software version 6.1.00, ensure to have increased disk space for data roll-up. Refer to the [Recommended Resource Requirements for Scaled Environments](#) section in the GigaVUE-FM Installation Guide for detailed information.

Control Filters in Analytics Dashboards

You can use control filters in your dashboards to filter and display the data you want to explore:

- To filter data in the visualizations based on the required tag keys and tag values, clone the required statistical dashboard and edit the *Sample - Tags* option in the Control Filters. Refer to [Filter Data Using Tags in Control Filters](#)

- Starting from software version 6.2.00, Cluster ID is a mandatory control filter field in the statistical dashboards. When cloning the dashboards and visualizations, you must use at least one of the following control filter fields to filter the data:
 - Cluster ID
 - Tag
- To optimize the performance of GigaVUE-FM, starting from software version 6.3.00, the data listed in the following control filter fields in Analytics dashboards is fetched from fminventory index (instead of fmstats index):
 - Cluster ID
 - Tags
- As data is fetched from fminventory index, you cannot view the details of devices that are no longer managed by GigaVUE-FM (as they will not be available in the fminventory index).

You can disable this behavior by logging in to the GigaVUE-FM CLI and performing the following steps:

1. Log in to the command line prompt:

```
sudo su -
```

2. Navigate to the folder where the .json file is located

```
cd /var/lib/fabricHealth/conf
```

3. Open the file using vi editor.

```
vi custom_settings.json
```

4. Set the **load_legacy** attribute value to "true".

5. Restart Analytics service.

```
systemctl restart fabricHealth.service
```

Reference Topics

Refer to the following sections for details:

- [Get Started with Analytics UI](#)
- [Work with the Analytics User Interface](#)

Get Started with Analytics UI

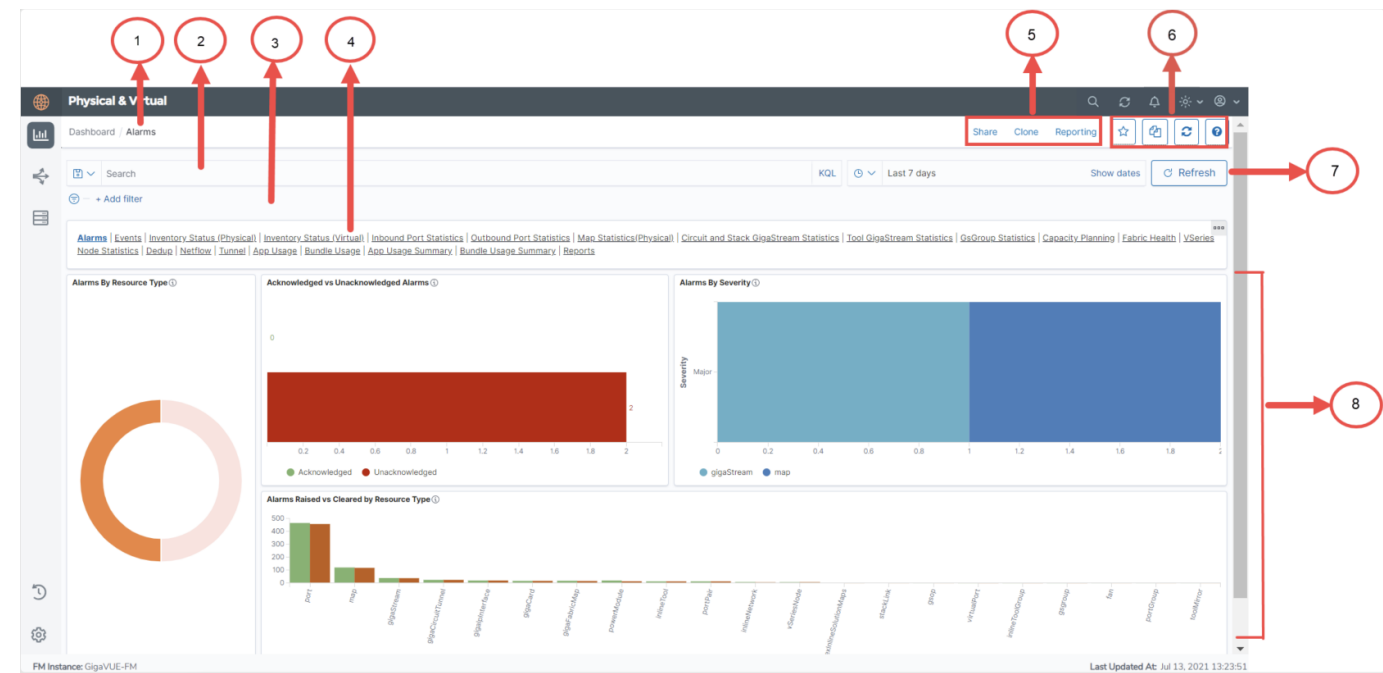
The Analytics option is listed under the Dashboards. To access the Analytics UI:

1. On the left navigation pane, click on .
2. Select **Analytics**. The following options are listed:
 - **Dashboards:** Refer to the [Dashboards](#) section for details.
 - **Visualization:** Refer to the [Visualizations](#) section for details.
 - **Discover:** Refer to the [Discover](#) section for details.
 - **Reports:** Refer to the [Reports](#) section for details.

GigaVUE-FM allows you to view the Fabric Health Analytics (FHA) Dashboard with data points having granularity levels for less than 48 hours in Trend Line Dashboards.

GigaVUE-FM provides granularity to all the custom FHA Dashboards or Visualizations.

The following figure shows the available options in the Analytics Dashboard page.



Refer to the following table for details:

S.No	Description	
1	Name of the Dashboard: Example Alarms.	Dashboards
2	Search box	Filter Data in Visualizations
3	Add Filter	In the Dashboard, refrain from using multiple filters in the global filter for better results.
4	Dashboard Navigation bar	Copy Dashboard Path
5,6	Working with the GUI	Work with the Analytics User Interface
7	Refresh	Use to manually refresh visualizations
8	Visualizations	Visualizations

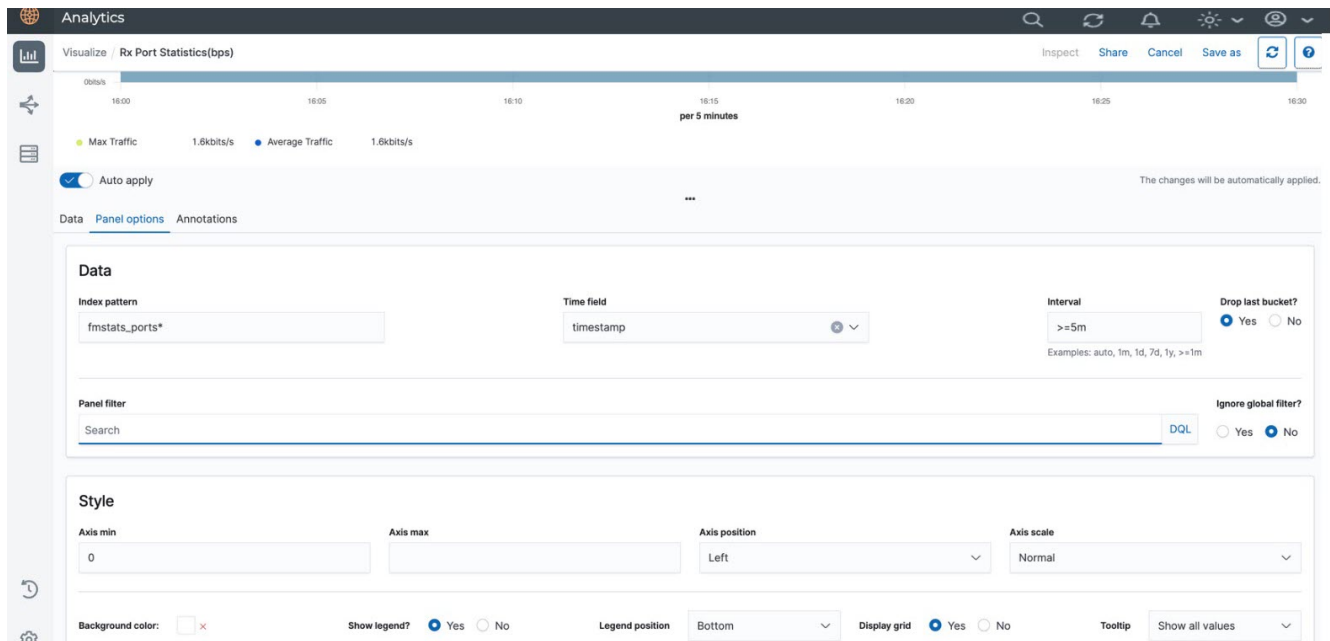
NOTE: When you cannot view the theme changes applied in Fabric Health Analytics (FHA), clear the browser cache and reload to view the updated changes.

The following table provides the granularity level at which the data is shown in the FHA Dashboard:

Interval	Granularity level at which data is shown
Up to 14 hours	5 minute granularity
15 to 48 hours	10 minute granularity

For intervals > 48 hours, 12 data points are displayed, is an expected behavior.

NOTE: If the analytics are available for < 30 minutes, it is recommended to select 5-minute granularity.



Work with the Analytics User Interface

GigaVUE-FM allows you to share the dashboard, clone the dashboard, generate the report, copy the dashboard, search data, etc., To know more about the user interface, refer to following sections:

Share

Use to share Dashboard pages with other users. To share a dashboard:

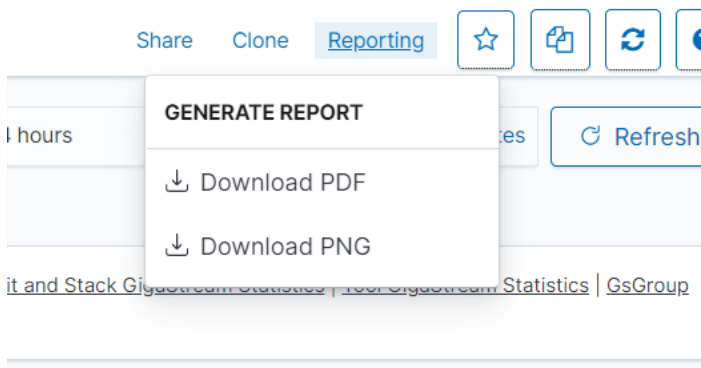
1. Navigate to the Dashboard page that you want to share.
2. From the top navigation bar, click **Share**.
3. The following options are available:
 - **Embed Code:** Use to share the dashboard in an iFrame Embed URL.
 - **Permalinks:** Use to share the permalink URL of the dashboard page.

Clone

Use to clone the system dashboard pages. Refer to the [Clone Dashboard](#) section for the details.

Reporting

Use to generate the report in PDF or in PNG format that can be downloaded instantly. The generated report is also listed in the Reports page. Refer to the [Reports](#) section for details.



Set as Default

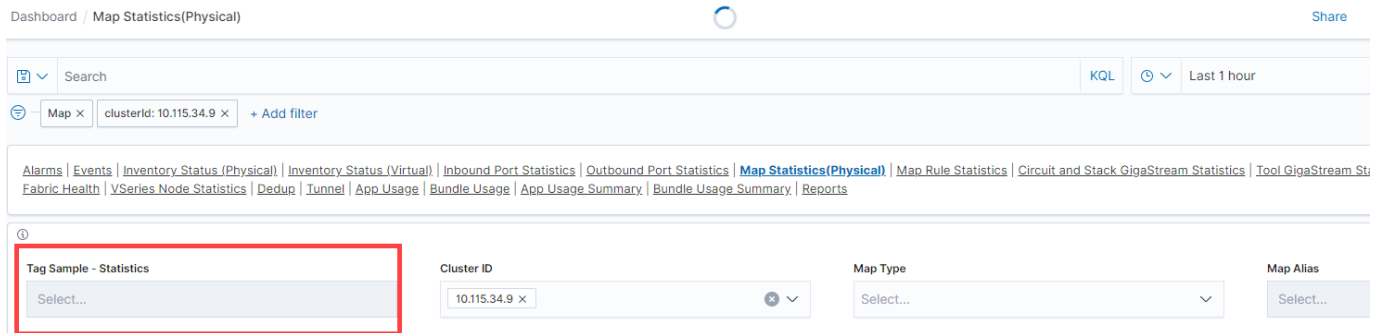
Use to change the default dashboard page:

- Navigate to the specific dashboard page.
- Click  to set this dashboard page as default.

(missing or bad snippet)(missing or bad snippet)

Filter Data Using Tags in Control Filters

Customize the **Tag Sample - Statistics** option available in some of the Statistical Dashboards to filter the data based on the required tags.



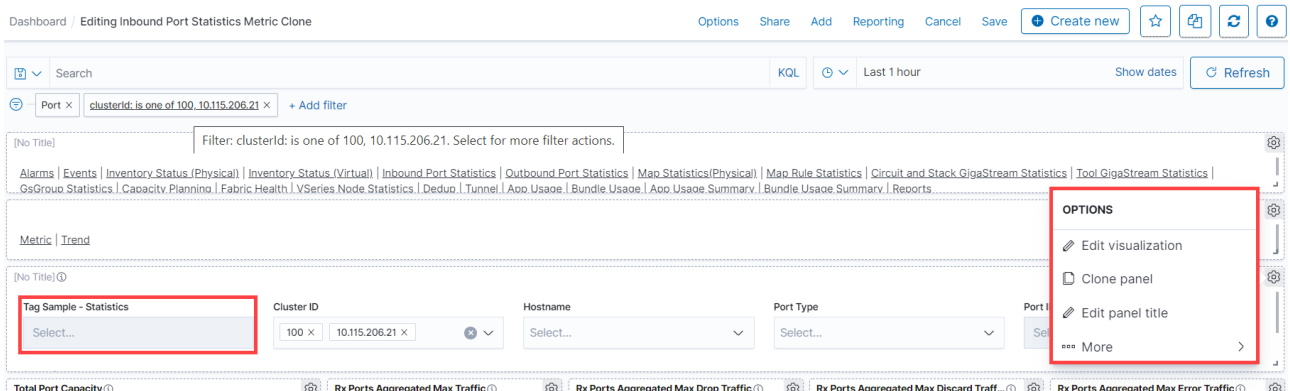
Pre-requisites

- Ensure to add the required tag keys and tag values to the tags page, and associate the tag values to the resources.
- Use the  Refresh Index Pattern icon for the newly added tags to get reflected in the Analytics page.

Consider a scenario in which you want to filter the inventory details in GigaVUE-FM based on a newly created tag key called SITE:

To do this:

1. Clone the required statistical dashboard.
2. Click **Edit**.
3. Scroll to the Control Visualization panel. Click **Options** and select **Edit Visualization**.



4. In the **Control** tab, configure the following. This is for filtering the data based on the tag value SITE.

Control Label	Site
Index Pattern	fmstats*
Field	tag.site

The screenshot shows the 'Controls' tab in the GigaVUE-FM interface. A red box highlights the configuration for a control named 'SITE'. The configuration includes:

- Control Label:** SITE
- Index Pattern:** fmstats*
- Field:** tag.SITE
- Parent control:** Cluster ID
- Multiselect:** Enabled (checked)
- Dynamic Options:** Enabled (checked)

Below the 'SITE' control, there is a section for the 'Cluster ID' control, which has a 'Control Label' of 'Cluster ID'. At the bottom of the interface, there are 'Discard' and 'Update' buttons.

5. Configure the existing tags as required:

Parent Control	Use to configure a specific field as a parent based on which the other fields are filtered
Multiselect	Use to select multiple variables within a field
Dynamic Options	Use to update the dashboards and visualizations dynamically based on this criteria.

6. In the **Option** tab, configure the following:

Update Kibana filters on each change	
Use time filter	To update the data based on the time filter configured in the dashboard.
Pin filters for all applications	

7. Click **Update** to update the changes.

8. Customize the panel title or remove it, as required. Move the control visualization to the top.

You can also create a new control visualization using the steps described above.

Search Data

To search your data:

- Enter the search criteria in the Query bar.
- Press Enter or click Update/Refresh button to submit the request.
- Click the Saved Queries icon to save the current query.

You can use Kibana's standard query language (KQL).

NOTE: When you submit a search request, the histogram, Documents table, Fields list and all the widgets in the dashboard are updated to reflect the search results.

(missing or bad snippet)

Visualizations

Visualization refers to the visual representation of data in various forms such as pie charts, time series graphs and other visual elements.

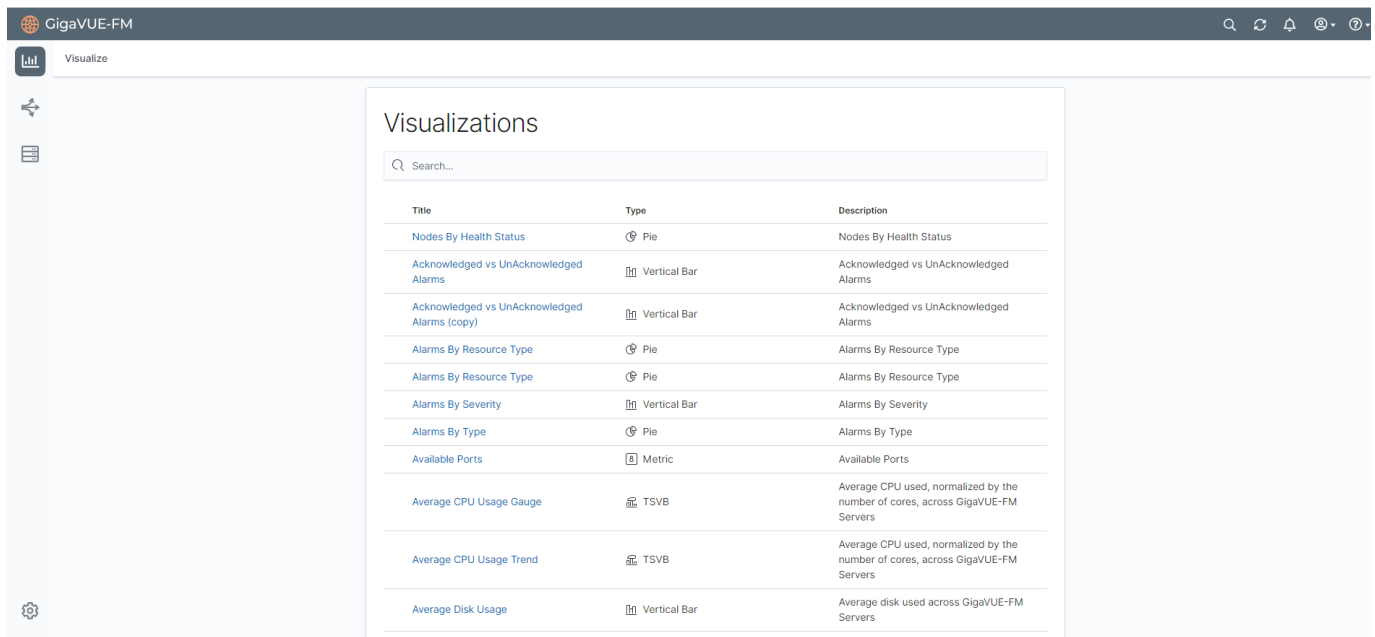
Using Analytics you can:

- View System Visualizations
- Create Custom Visualizations

View System Visualization

System visualizations are pre-defined visualizations that are available by default in GigaVUE-FM. To view the system visualization:

1. Click the Dashboard icon on the left navigation pane.
2. Select **Analytics > Visualizations**.
3. Choose the required system visualizations.



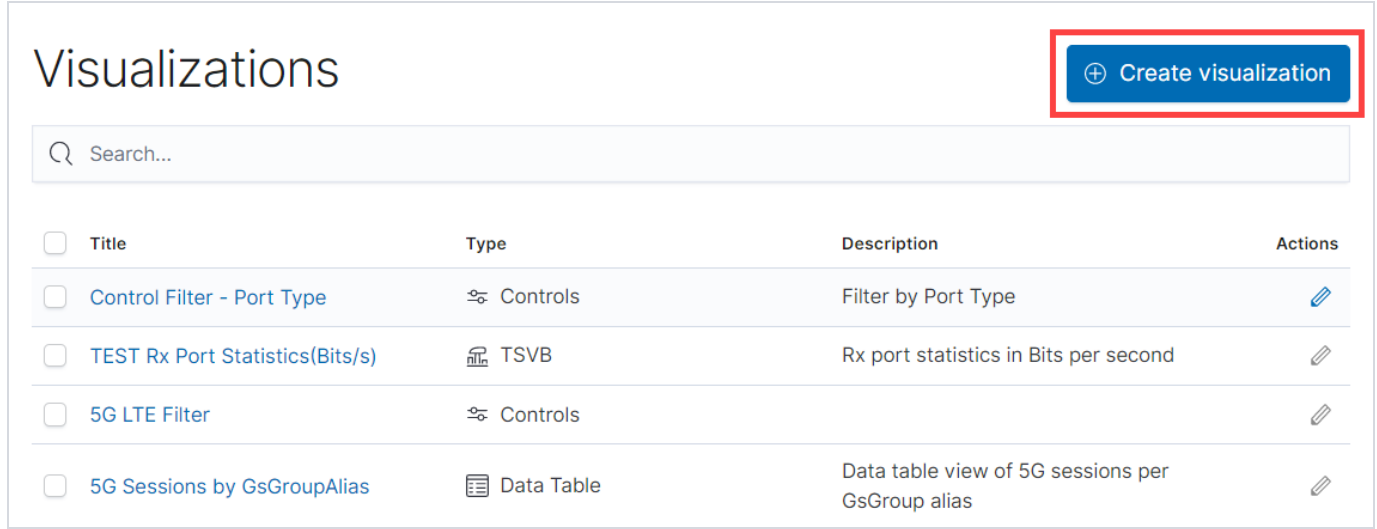
Create Custom Visualizations

You can create custom visualizations by cloning the existing system visualizations or creating a new visualization.

Create a Visualization

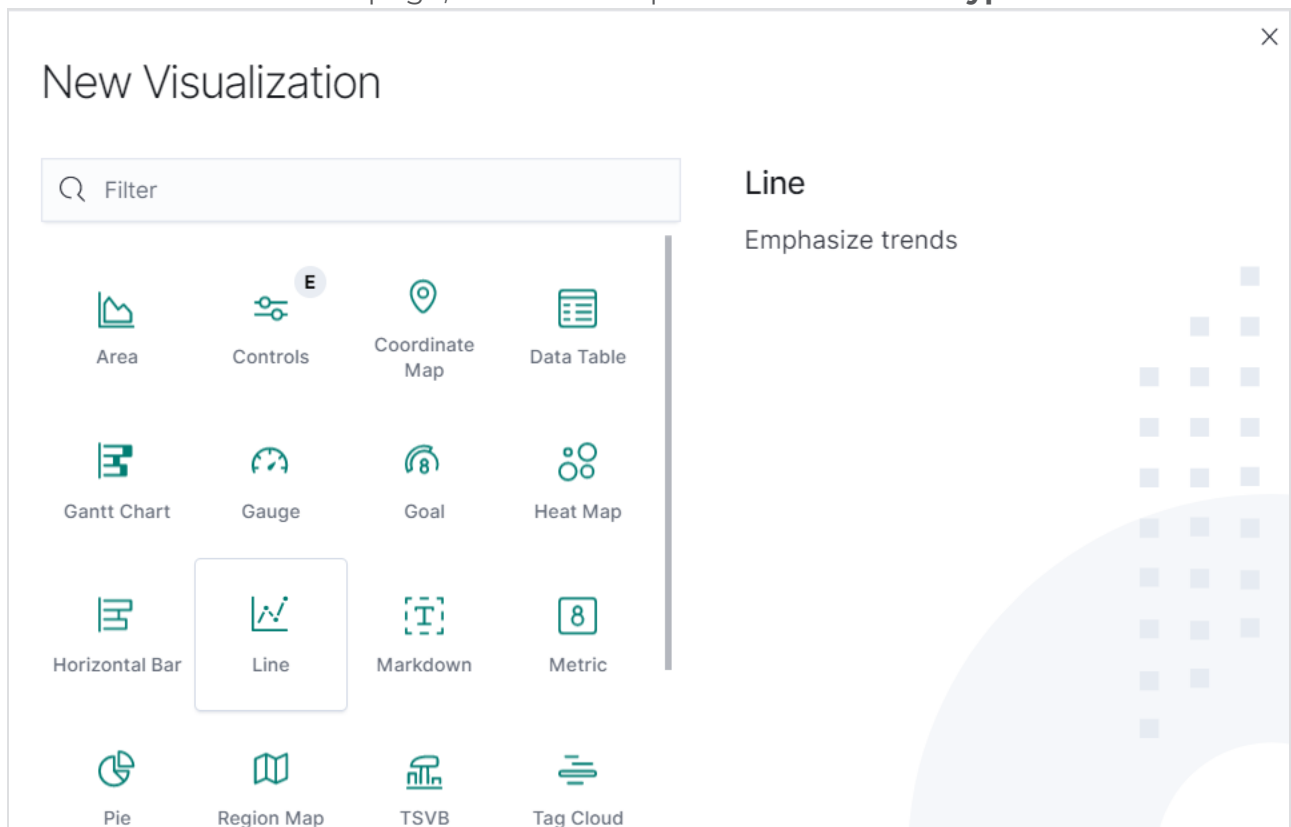
To create a new visualization:

1. On the left navigation pane, click on . Select **Analytics > Visualization**.
2. Click **Create Visualization**.



Title	Type	Description	Actions
Control Filter - Port Type	Controls	Filter by Port Type	
TEST Rx Port Statistics(Bits/s)	TSVB	Rx port statistics in Bits per second	
5G LTE Filter	Controls		
5G Sessions by GsGroupAlias	Data Table	Data table view of 5G sessions per GsGroup alias	

3. In the New Visualization page, select the required **Visualization Type**.



New Visualization

Filter

Line
Emphasize trends

Area, Controls, Coordinate Map, Data Table, Gantt Chart, Gauge, Goal, Heat Map, Horizontal Bar, **Line**, Markdown, Metric, Pie, Region Map, TSVB, Tag Cloud

4. Select the data source for the visualization.

New Metric / Choose a source **4**

Q Search...

Sort ▾ Types 2 ▾

✓ Ascending
Descending

Q Alarm Events

Q Alarm Summary

Q Card/Slot Summary Search

Q Cloud Connection Summary

Q Cluster Summary Search

Q Filter Resource

fmalarms*

fmevents*

< 1 2 3 4 >

- Enter the required details for the type of visualization selected. Refer to the table below for more details.
- Click **Save**.
- In the **Save Visualization** dialog enter the Title and Description for the visualization and click **Save**.

Type of Visualization	Description
Metric	Displays a single number for the selected aggregation.
Data table	Displays the raw data of a composed aggregation.
Pie Chart	Display each source's contribution to a total.
TSVB	Combines an infinite number of aggregations and pipeline aggregations to display complex data in a meaningful way
Line Chart, Area Chart, Horizontal and Vertical Bar charts	Compares different series in X/Y charts.
Heat maps	Shade cells within a matrix.
Markdown widget	Display free-form information or instructions.
Goal and Gauge	Displays a gauge
Coordinate map	Associate the results of an aggregation with geographic locations.
Region map	Thematic maps where a shape's color intensity corresponds to a metric's value.

NOTE:

1. When creating TSVB visualizations using derivative aggregation, you have the option to utilize the 'ignore' keyword in the unit field. This can be particularly beneficial when working with counter metrics and aiming to display only the difference instead of the rate per time unit in the graphical representation. Due to OpenSearch's limitation, the visualization's maximum search results will be limited to 10,000 entries. It is recommended to use filters for refined search results.
2. In the OpenSearch dashboards, you can only change the bucket priority by dragging fields if your screen resolution is set to 100 percent.

Clone a Visualization

To clone a visualization:

1. On the left navigation pane, click on . Select **Analytics > Visualization**.
2. Select the visualization for which you need to create a clone.
3. Make the required changes.
4. Click **Save As**.
5. Enter a name for the new Visualization.
6. Click **Save As**. The new visualization will be added to the list page.

Visualizations - Example Work Flows

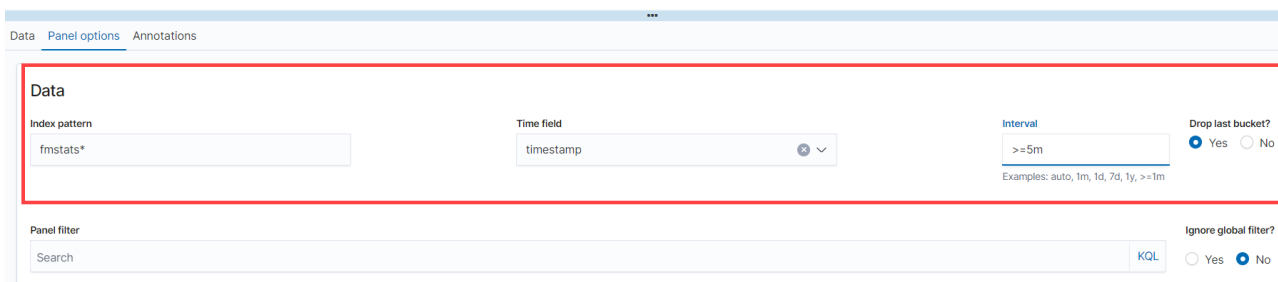
This section includes examples for configuring the visualizations:

- [TSVB Chart Displaying Traffic Trend](#)
- [Pie Chart Displaying Alarms Summary](#)
- [Metric Displaying Card Count](#)
- [Bar Chart for Alarms by Severity](#)

TSVB Chart Displaying Traffic Trend

To create a TSVB chart that shows traffic trend for every five minutes:

1. Click **Create Visualization**. In the New Visualization page, select **TSVB**.
2. Click **Panel Options**.



Data

Index pattern: fmstats*

Time field: timestamp

Interval: >=5m
Examples: auto, 1m, 1d, 7d, 1y, >=1m

Drop last bucket? ☒ Yes ☐ No

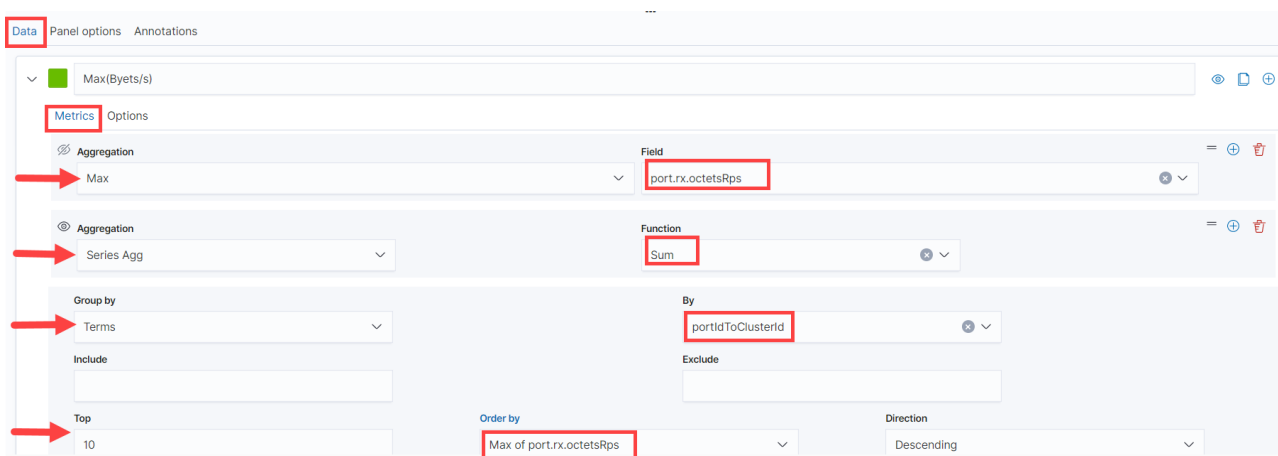
Panel filter: Search

Ignore global filter? ☐ Yes ☒ No

3. Select or enter the following details under Data:

Index Pattern	<i>fmstats*</i>
Time field	<i>Timestamp</i>
Interval	<i>Must be >=5 minutes</i>
Drop last bucket	<i>Must be checked</i>

4. Click **Data** and Select **Metrics**.



Data Panel options Annotations

Max(Bytes/s)

Metrics Options

Aggregation: Max

Field: port.rx.octetsRps

Function: Sum

Group by: Terms

By: portIdToClusterId

Include:

Exclude:

Top: 10

Order by: Max of port.rx.octetsRps

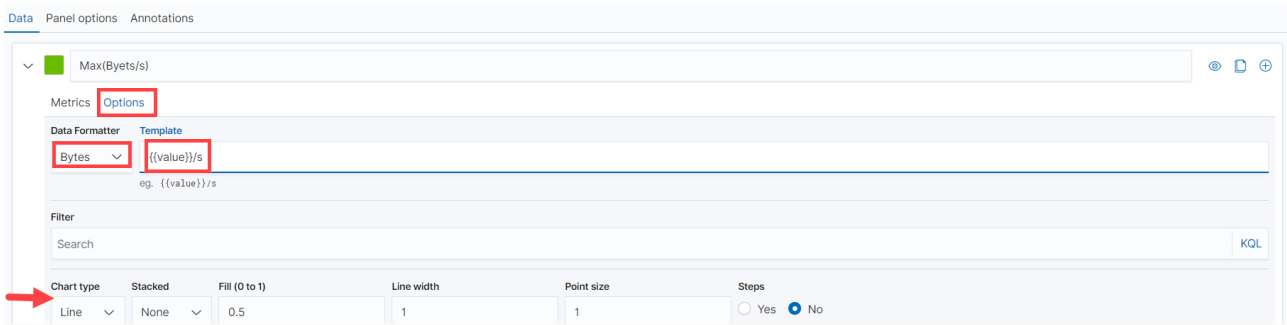
Direction: Descending

Select or enter the following details:

Label: Configure the label as Max Rate (Bytes/s)	
Aggregation	<i>Max</i>
Field	<i>port.rx.octets.Rps</i>
Create another aggregation	

Aggregation	Series Agg
Function	Sum
Group By	Terms
By	PortIdToClusterId
Top	10
Order by	Max of port.rx.octets.Rps

5. Select **Options**.



Data Formatter	Bytes
Template	Values/s

5. Click **Save** to save the visualization.

NOTE: Use the chart type option allows you to configure the chart.

Pie Chart Displaying Alarms Summary

To create a pie chart that shows alarm summary:

1. Click **Create Visualization**. In the New Visualization page, select Pie.
2. Select the data source for the visualization. It can be either an index pattern or a saved search object. *In this example, Alarm Summary is selected as the data source.*

3. Click **Data**. Configure the Metrics and Buckets as shown in the following figure.

The screenshot shows the 'Alarm Summary' configuration page with the 'Data' tab selected. The 'Metrics' section has 'Aggregation' set to 'Unique Count' and 'Field' set to '_id'. The 'Buckets' section has 'Split slices' checked, 'Aggregation' set to 'Terms', 'Field' set to 'type', and 'Order by' set to 'Metric: Alarms'. Red boxes highlight the 'Aggregation' and 'Split slices' settings, and red arrows point to the 'Field' settings.

- **Aggregation function:** Select Unique Count. This returns the number of unique values in a field.
- **Field values:** _Id and Type can be changed as per your requirements
 - **Field value _Id:** The field that you want to visualize (in the example, id is being used because it is unique for each node)
 - **Field value Type:** The Field that you want to use to split the pie chart (in the example, type is being used to slice the chart)

4. Click **Update** to update the visualization.

NOTE: Use the **Options** tab to configure the required visual effects such as configuring the pie chart as a donut, adjusting the position of the legend, and so on.

The screenshot shows a configuration panel titled "Alarm Summary" with a search icon and a menu icon. Below the title are two tabs: "Data" and "Options", with "Options" being the active tab. The panel is divided into two sections: "Pie settings" and "Labels settings".

Pie settings

- ☒ Donut
- Legend position: Right (dropdown menu)
- ☒ Show tooltip

Labels settings

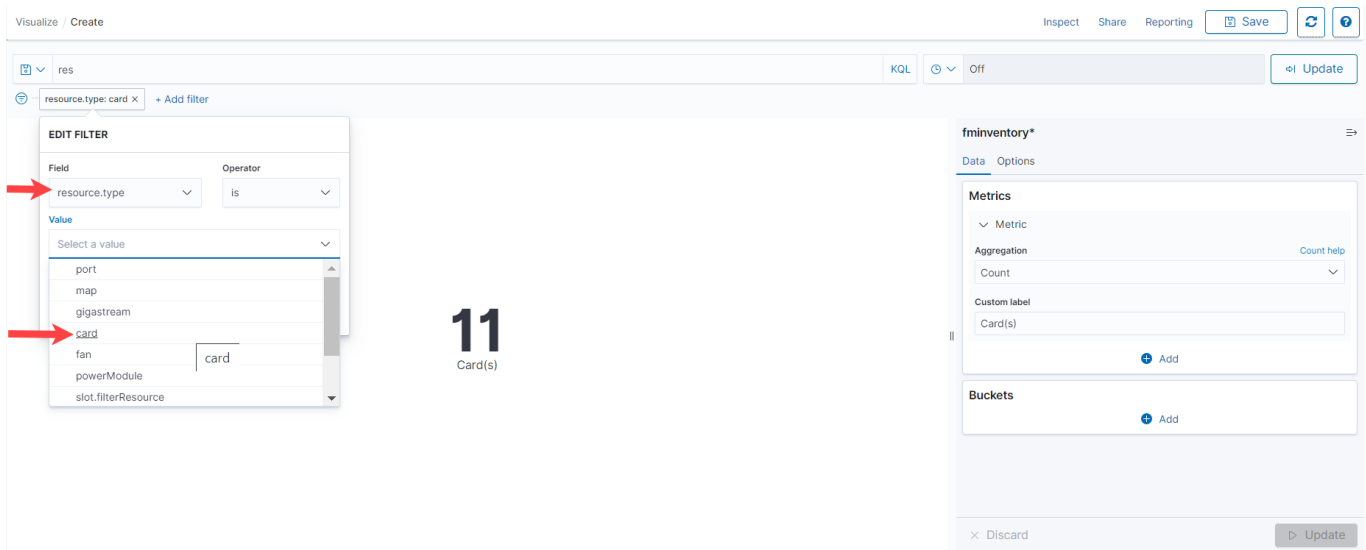
- ☐ Show labels
- ☒ Show top level only
- ☒ Show values
- Truncate: 100 (input field)

Metric Displaying Card Count

To create a Metric visualization that shows the number of cards:

1. Click **Create Visualization**. In the New Visualization page, select **Metric**.
2. Select the data source for the visualization. It can be either an index pattern or a saved search object.
3. Configure the **Aggregation** as **Count**.
4. In the Add Filter option, configure the following:
 - **Filter:** *resource.type*
 - **Operator:** **is**
 - **Value:** *Card*
5. Click **Update**.

Refer to the following image:



NOTE: Use the **Options** tab to configure the required visual effects such as adjusting the font size.

Bar Chart for Alarms by Severity

To create a bar chart that shows the number of alarms based on severity:

1. Click **Create Visualization**. In the New Visualization page, select **Vertical Bar**.
2. Select the data source for the visualization. It can be either an index pattern or a saved search object. In this example, *fmalarms* is selected as the data source.
3. Click **Data**. Configure the **Metrics** and **Buckets** as shown in the following figure.
 - Metrics
 - Aggregation: Count
 - Bucket
 - Aggregation: Terms
 - Field: Severity
 - Order by: Metric Count

fmalarms*

Data Metrics & axes Panel settings

Metrics

Y-axis

Aggregation [Count help](#)

Count

Custom label

+ Add

Buckets

X-axis [Terms help](#)

Aggregation

Terms

Field

severity

Order by

Metric: Count

Order

Descending

Size

100

☐ Group other values in separate bucket

☐ Show missing values

Custom label

Severity

☒ [Advanced](#)

Exclude

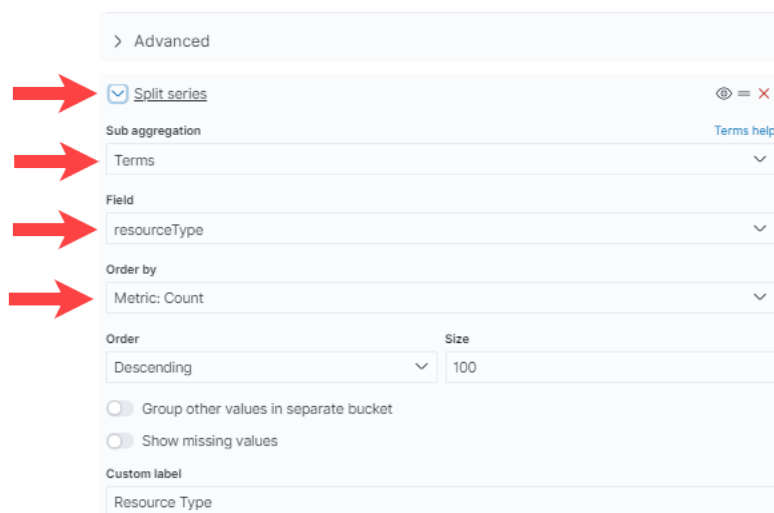
Include

JSON input ⓘ

1

× Discard Update

- Under **Advanced**, select **Split series** and configure the following:
 - *Sub aggregation*: Terms
 - *Field*: resourceType
 - *Order by*: Metric Count



> Advanced

☒ Split series 🔍 = ✕

Sub aggregation Terms help

Terms ▼

Field ▼

resourceType

Order by ▼

Metric: Count

Order ▼ Size

Descending 100

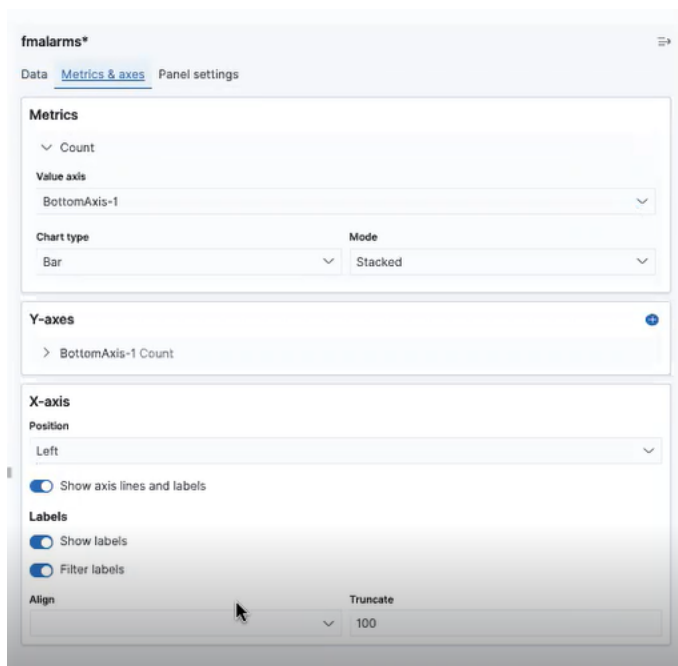
☐ Group other values in separate bucket

☐ Show missing values

Custom label

Resource Type

2. Under Metrics & Axes, configure the following:



fmalarms*

Data Metrics & axes Panel settings

Metrics

▼ Count

Value axis

BottomAxis-1 ▼

Chart type ▼ Mode ▼

Bar Stacked

Y-axes +

> BottomAxis-1 Count

X-axis

Position ▼

Left

☒ Show axis lines and labels

Labels

☒ Show labels

☒ Filter labels

Align ▼ Truncate

100

3. Click **Update**.

Dashboards

A dashboard is a collection of visualizations. Click on **Analytics** > **Dashboard**. The Alarms dashboard page appears.

Click the **Dashboards** menu on the top navigation bar of the Analytics page to view all the dashboards.

From the Dashboards page, you can:

- View Default Dashboards
- Create Custom Dashboards by cloning existing system dashboards or creating new dashboards.

View Default Dashboards

The Default dashboards is the list of pre-defined dashboards created in GigaVUE-FM. Refer to the [Default Dashboards](#) section for the list of default dashboards and the associated visualizations.



Notes:

- You cannot edit or delete the default dashboards. However, you can create your own personalized dashboards as per your requirements.
- GigaVUE-FM displays default static description text for each of the default dashboards.

You can perform the following operations:

- Share** Use to share the Dashboard page. The following options are available:
Embed Code: To share the code either as a snapshot or saved object.
Permalinks: To copy the permalink of the dashboard page.
- Clone** Use to clone the default dashboard page. Refer to the [Clone Dashboard](#) for more details
- Reporting** Use to generate the report in PDF or in PNG format.

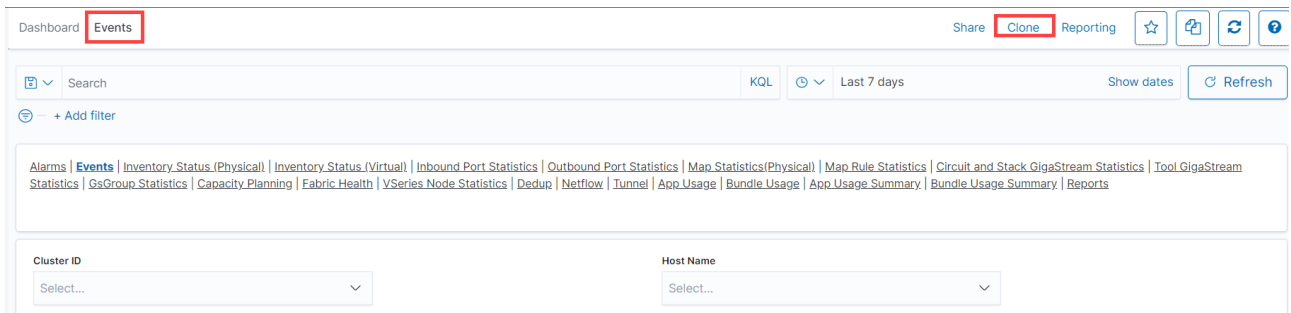
Clone Dashboard

GigaVUE-FM does not allow you to edit the default dashboards. However, you can clone the system dashboard and make changes to the new dashboard.

To clone a dashboard:

1. On the left navigation pane, click on . Select **Analytics > Dashboards**.
2. Navigate to the dashboard page for which you need to create a clone.
3. Click the **Clone** button on the submenu bar.
4. Enter a name for the new dashboard and click **Confirm Clone**. The new dashboard is

created.



Refer to the [Edit Dashboard](#) section for details on editing the dashboard.

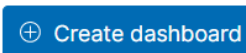
Create New Dashboard

To create a new dashboard:

1. Go to Dashboards -> **Analytics** -> **Dashboards**.
2. Click the **Dashboards** menu on the top navigation bar of the Analytics page.
3. Click **Create Dashboard**.

Dashboards

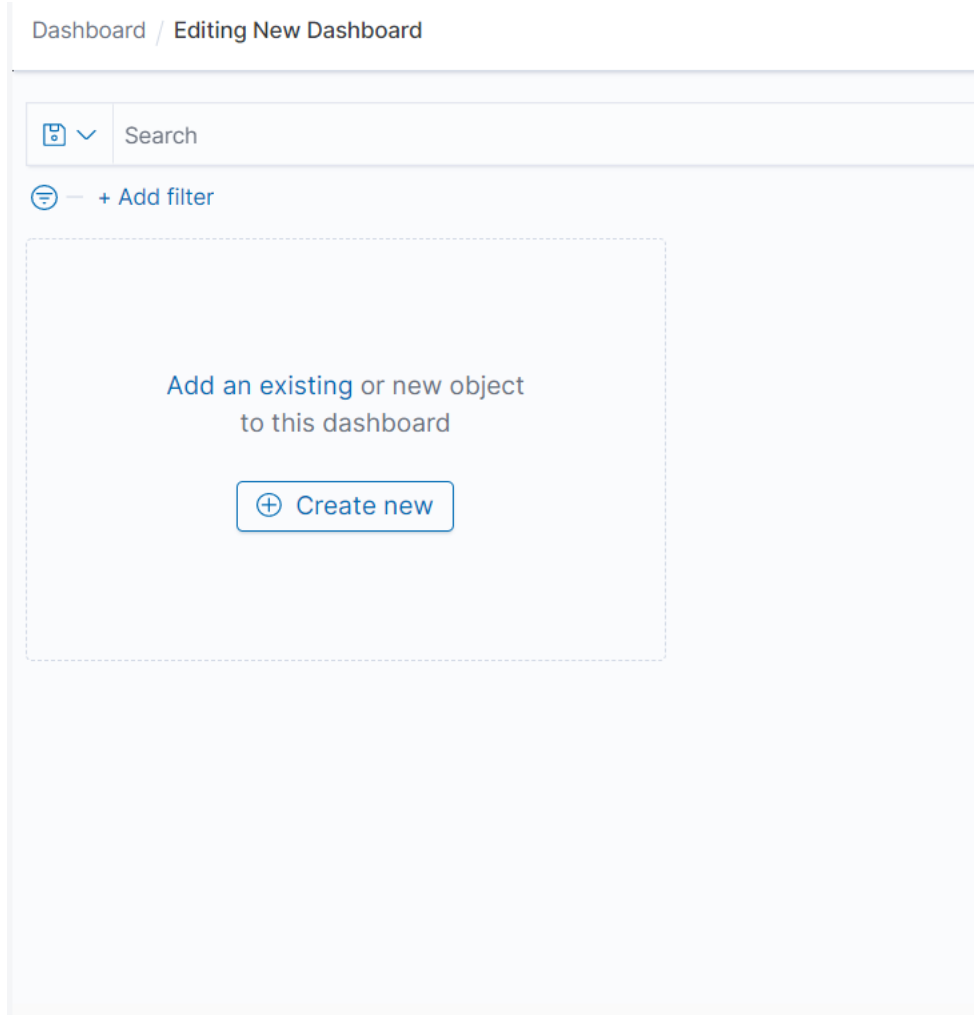
 Search...



 Title	Description	Actions
 5G LTE Sessions	GigaVUE-FM Analytics dashboard: 5G LTE Sessions	
 Alarms	GigaVUE-FM Analytics dashboard: Alarms	
 App (Virtual)	GigaVUE-FM Analytics dashboard: App (Virtual)	
 App Usage Summary	GigaVUE-FM Analytics dashboard: App Usage Summary	
 Application Performance		
 Bundle Usage Summary	GigaVUE-FM Analytics dashboard: Bundle Usage Summary	
 Capacity Planning	GigaVUE-FM Analytics dashboard: Capacity Planning	
 Circuit and Stack GigaStream Statistics Inbound Trend	GigaVUE-FM Analytics dashboard: Circuit & Stack GigaStream Inbound Statistics Trend	
 Circuit and Stack GigaStream Statistics Metric	GigaVUE-FM Analytics dashboard: Circuit & Stack GigaStream Statistics Metric	
 Circuit and Stack GigaStream Statistics Outbound Trend	GigaVUE-FM Analytics dashboard: Circuit & Stack GigaStream Outbound Statistics Trend	
 Daily App Usage	GigaVUE-FM Analytics dashboard: Daily App Usage	
 Daily Bundle Usage	GigaVUE-FM Analytics dashboard: Daily Bundle Usage	
 Dedup (Virtual)	GigaVUE-FM Analytics dashboard: Dedup (Virtual)	
 Endpoint (Virtual)	GigaVUE-FM Analytics dashboard: Endpoint (Virtual)	
 Events	GigaVUE-FM Analytics dashboard: Events	
 Fabric Asset Inventory	GigaVUE-FM Analytics dashboard: Fabric Asset Inventory	
 Fabric Health	GigaVUE-FM Analytics dashboard: Fabric Health	
 Fabric Health Storage	GigaVUE-FM Analytics dashboard: Fabric Health Storage	
 Fabric Map Statistics(Physical)	GigaVUE-FM Analytics dashboard: Fabric Map Statistics	
 Flow Filtering	GigaVUE-FM Analytics dashboard: Flow Filtering	

Rows per page: 20 
< 1 2 3 >

4. In the Editing New Dashboard page, you can:
 - a. Add an existing visualization. Click **Add an Existing** link.
 - b. Create a new object. Click **Create New**. For instructions, refer to [Create Custom Visualizations](#)



5. Click **Save**.
6. In the **Save dashboard** dialog box, enter the **Title** and **Description** for the dashboard and click **Save**.

X

Save dashboard

Title

Description

X

Store time with dashboard

Cancel

Save

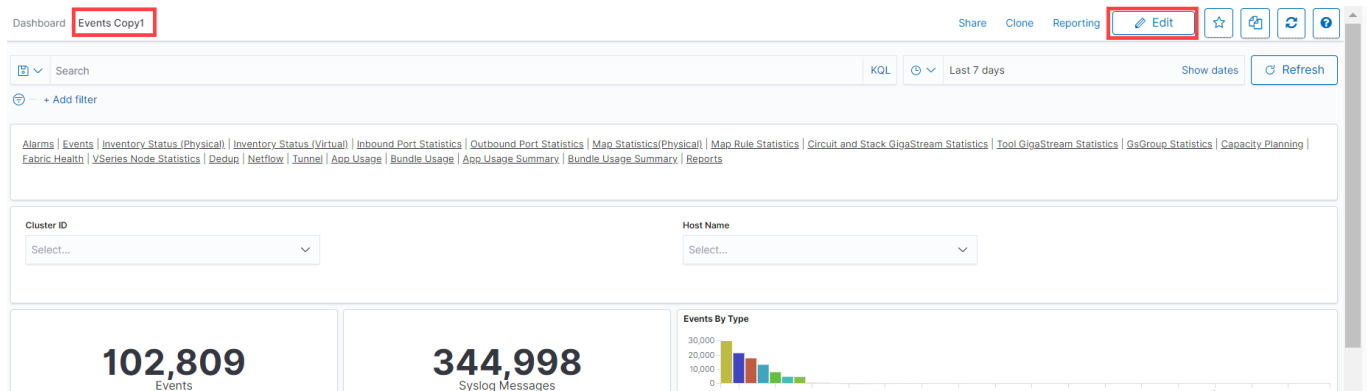
To make further changes to the dashboard, refer to the [Edit Dashboard](#) section.

Edit Dashboard

Edit the new dashboard page to suit your requirements. From the cloned dashboard page, click **Edit** to perform the following operations:

Option	Description
Options	Use to set the following options: • Use margins between panels • Show panel titles

Add	Use to Add Panels to the dashboard
Create New	Use to create a new visualization
	Use to edit the following: • Edit Visualization: Edit the required visualizations. • Clone Panel: Clone the panel. • Edit Panel Title: Edit the panel title. • Maximize Panel: Maximize the panel. • Replace Panel • Delete from Dashboard: Delete visualizations that you no longer need on the new dashboard



Click **Save** to save the changes to the dashboard. In the **Save Dashboard** dialog box, use the toggle option to save the changes to a new dashboard. Click **Cancel** to discard the changes.

Reports

The Reports option allows you to download the data in the dashboards and visualizations in PDF or PNG format.

NOTE: You can download data in .csv format from the Discover page.¹

To download the reports

1. On the left navigation pane, click on .
2. Select **Analytics** and click **Reports**. The list of reports is displayed. It can be either **On Demand** or **Schedule**.
3. Click on a report to view the details and download the report.

¹The CSV file will have empty fields if the field values are zero in the report.

The **Report Definitions** option allows you to schedule automatic generation of reports. To create report definition:

1. Click **Create**.

Create report definition

Report Settings

Name

Report name (e.g Log Traffic Daily Report)

Valid characters are a-z, A-Z, 0-9, (), [], _ (underscore), - (hyphen) and (space).

Description (optional)

Describe this report (e.g Morning daily reports for log traffic)

Report source

☐ Dashboard
 ☐ Visualization
 ☒ Saved search

Select saved search

Select a saved search

Time range

▼

Last 30 minutes

Show dates

Time range is relative to the report creation date on the report trigger.

File format

CSV

Report trigger

Trigger type

☒ On demand
 ☐ Schedule

2. Select or enter the following details under **Report Settings**:

Field	Description
Name	Name of the report.
Description	Description for the report.
Report Source	The source from which the report is generated. It can be Dashboard, Visualization or a Saved Search object. Note: When downloading reports of any dashboard, the parent

	dashboard link of the report will not get highlighted in the report (only the child dashboard link - such as metric/trend will not be highlighted).
Select	Select your Dashboard, Visualization or the Saved Search object, accordingly. Dashboards and Visualizations will be downloaded in PNG or PDF format. Saved search objects will be downloaded in CSV format.
Time Range	Select the time range for your report.
File Format	Select the required file format.
Header and Footer	Add a header or footer for the report. Headers and footers are only available for dashboard or visualization reports.

3. Select or enter the following details under **Report trigger**:

- **Trigger type**

- On Demand
- Schedule

- **Request time**

- **Recurring**: Select **Frequency** and the **Request time**.
- **Cron-based**: Select the Custom cron expression.
- Select the required time zone.

NOTE: GigVUE-FM allows you to create a report with recurring or cron-based options but does not allow you to edit these options after creating the report. In such cases, you must delete the report and create a new report using the required option.

4. Click **Create**.

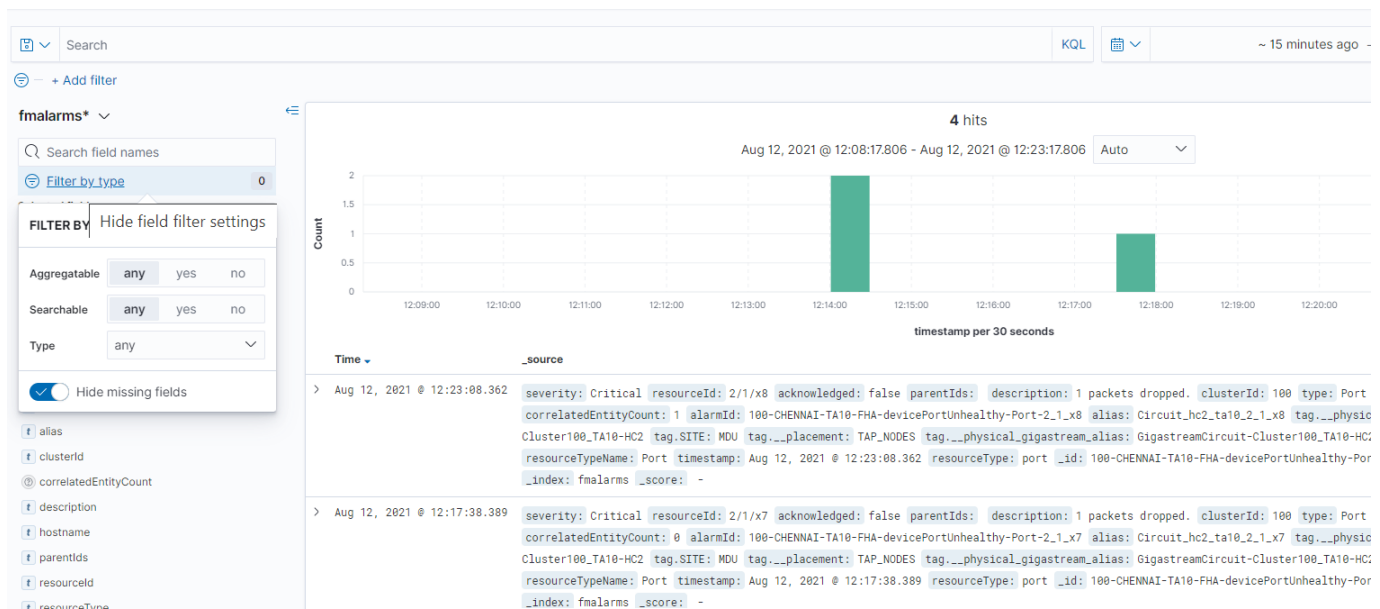
Discover

The Discover page allows you to view and explore your data. This page consists of the following sections:

- **Add filters**: Use to create queries and filters. Click **Add filters** to add a filter. You can also use time filters along with the filter created. Use the saved filters in dashboards and visualizations. Refer to the [Discover](#) section for details.
- **Date Histogram**: Displays how data is ingested over time.
- **Documents**: Displays the documents. Expand the documents to view more details.
- **Field list on the left**: Displays fields available in the data. Click on a field to view the most common values.

The **Filter by Type** option allows you to filter the data based on the following criteria:

Aggregatable	Select Yes to extract summaries from matching documents. For example, count is a type of aggregation.
Searchable	Select Yes to filter the data based on specific conditions. For example, filter the data for the last 24 hours.
Type	Field type. Allowable values are: - String - Number - Source - Date



You can perform the following operations from the Discover page:

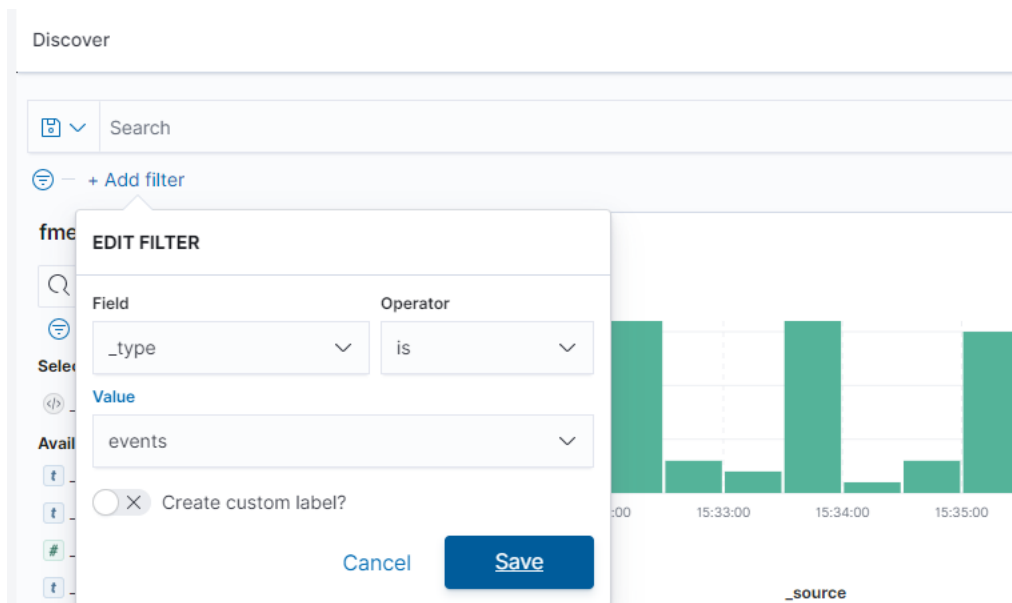
New	Use to create a new saved search object.
Save	Use to save your search and use it later. You can also generate a CSV report or use the saved search object in dashboards and visualizations. Refer to Save Search section for details.
Reporting	Use to generate and download the report in CSV format.
Open	Use to open the list of existing saved search objects.
Share	Use to share the saved search object to other users.
Inspect	Use to view details such as number of hits, index pattern, index pattern id, request and response details.

NOTE: Currently, the Discover page in GigaVUE-FM does not support the search and filtering option on RollUp Index..

Filter

To add a filter:

1. Click **Add filter**. The **Edit Filter** pop-up appears.
2. Select the required field, the operator, and the value.
3. Click **Save** to save the filter.
4. You can create custom label for the filter.



Save Search

Use the **Save Search** option to save queries, filters, and current view of the Discover page, such as the columns selected in the Document table, the sort order and also the index pattern. To save a search:

1. Create a search criteria that you want to reuse, click **Save** in the toolbar.
2. Enter a name for the search and click **Save**.
3. Use the saved search objects in the dashboards and visualizations by selecting the search objects using the Add from library option.

Find Data

Use the Discover page to find the data you need to analyze. You can also specify the time range in which to view that data:

1. On the left navigation pane, click on .
2. Select **Analytics** and click **Discover**.
3. Select the index patterns for which you want to find the data. For example, *fmalarms*.
4. Adjust the time range to view the data for the required time range.

NOTE: The range selection is based on the default time field in your data. If the data does not have a time field, the range selection is not available.

5. To view the count of data for a given time in the specified range, click and drag the mouse over the histogram.

NOTE: After you upgrade or install GigaVUE-FM, when you query the *fmstats_port* index, additional device statistical data from *fmstats* index is also combined and displayed. This behavior is observed only on day 1 after installation or upgrade of GigaVUE-FM, and will not be noticed from the subsequent day onwards.

Default Dashboards

The following table lists the various default dashboard pages. The default dashboards are categorized as follows:

- System Dashboards
- Physical Dashboards
- Cloud Dashboards
- Hybrid Dashboards
- Inline TLS/SSL Dashboards

NOTE: Few dashboard pages have Control Visualizations that help you narrow down the data displayed in the visualizations based on the selected criteria.

Table 1: System Dashboards.

Dashboard	Details	Visualizations
System Dashboards		
Alarms	Displays data related to Alarms. Alarms is the default dashboard page. Clicking on a legend in the following visualizations in the Alarms dashboard navigates you to the Alarms page. The alarms are listed based on the filters in the Analytics page: - Alarms By Resource Type - Acknowledged vs Unacknowledged Alarms - Alarms by Severity - Unsuppressed vs Suppressed Alarms by Resource Type Use the following fields in control visualizations to filter the Syslog data: Tag Sample - Alarms Cluster ID	Alarms by Resource Type
		Alarms by Severity
		Acknowledged vs. Unacknowledged Alarms
		Alarms Raised vs Cleared by Resource Type
		Suppressed Alarms Count
		Suppressed Alarms by Nodes
		Unsuppressed vs Suppressed Alarms by Resource Type
Events	Displays data related to Events. Clicking on a legend in the following visualizations in the Events dashboard will navigate you to the Events page. The events will be listed based on the filters in the Analytics page: - Events by Severity - Events by Type - Top 10 Event Contributors Use the following fields in control visualizations to filter the Events data: Cluster ID Host Name	Events by Type
		Events by Severity
		Top 10 Event Contributors
Syslog	Displays data related to Syslog. Use the following fields in control visualizations to filter the Syslog data: Syslog Source Host Name Severity	Syslog by Severity
		Top 10 Syslog Contributors

Dashboard	Details	Visualizations
Fabric Health	The Fabric Health tab consists of the following two dashboards: - CPU and Memory - Storage	
	CPU and Memory	
	The CPU and Memory dashboard displays metric and trend visualizations for both threshold and maximum values.	Average CPU Usage Gauge
	Note: After upgrading to software version 5.16.00, the line that depicts the threshold values (blue line) in the following visualizations will not be available for historic time ranges. This is because historical data for threshold is not collected in GigaVUE-FM prior to the upgrade:	Max CPU Usage Gauge
	- Average Memory Usage Trend - Max Memory Usage Trend	Average CPU Usage Trend
	Use the Server Name control visualization to view the memory and storage metric and trend for the particular server.	Max CPU Usage Trend
		Average Memory Usage Gauge
		Max Memory Usage Gauge
		Average Memory Usage Trend
		Max Memory Usage Trend
		Used Vs Total System Memory
	Storage	
	The Storage dashboard displays metric and trend visualizations for both threshold and maximum values.	Average Disk Usage (/var)
	Note: After upgrading to software version 5.16.00, the following visualizations will not be available for historical time ranges. This is because historical data for these visualizations is not collected in GigaVUE-FM prior to the upgrade:	Max Disk Usage (/var)
	- Average Dis Usage (/) - Max Disk Usage (/) - Average Disk Usage (/) Trend - Max Disk Usage (/) Trend	Average Disk Usage (/var) Trend
	Use the Server Control Filter to view the memory and storage metric and trend for the particular server.	Max Disk Usage (/var) Trend
		Average Disk Usage (/config)
		Max Disk Usage (/config)
		Average Disk Usage (/config) Trend
		Max Disk Usage (/config) Trend
		Average Disk Usage (/)
		Max Disk Usage (/)

Dashboard	Details	Visualizations
		Average Disk Usage (/) Trend
		Max Disk Usage (/) Trend
Physical Dashboards		
Inventory Status	Displays status of the physical resources. The following metrics are displayed at the top: - Number of clusters - Number of standalone nodes - Number of Nodes - Number of Ports - Number of Cards Use the Tag Sample - Inventory control visualizations to filter the data.	Nodes by model and software version
		Port by type and health
		Card by type and health
Inbound Port Statistics	Displays statistics of the receiving (Rx) ports in packets per second, bits per second. The dashboards are categorized into: - Metric - Trend The metric tab displays the following visualizations: - Total Port Capacity - Rx Ports Aggregated Average Traffic - Rx Ports Aggregated Average Drop Traffic - Rx Ports Aggregated Average Discard Traffic - Rx Ports Aggregated Average Error Traffic Use the following control visualizations to filter the data: Tag Sample - Statistics Cluster-ID Host Name Port Type Port ID Port Alias With Rollup enabled, you can view statistics for a period of 120 days on hourly granularity.	Top Rx ports by Max Rate (bps)
		Top Rx ports by Average Rate (bps)
		Rx Port Statistics (bps)
		Rx Port Statistics(pps)
		Top Rx ports by Max Traffic Trend (bps)
		Top Rx ports by Max Traffic Trend (pps)
		Top Rx ports by Average Traffic Trend (bps)
		Top Rx ports by Average Traffic Trend (pps)
		Rx Drop Rate(pps)
		Rx Discard Rate(pps)
		Rx Error Rate(pps)
Outbound Port	Displays statistics of the transmitting (Tx) ports in packets per	Top Tx ports by Max

Dashboard	Details	Visualizations
Statistics	second, bits per second. The dashboards are categorized into: • Metric • Trend The metric tab displays the following visualizations: • Total Port Capacity • Tx Ports Aggregated Average Traffic • Tx Ports Aggregated Average Drop Traffic • Tx Ports Aggregated Average Discard Traffic • Tx Ports Aggregated Average Error Traffic • Tx Ports Aggregated Max Traffic Use the following control filters to filter the statistics: • Tag Sample - Statistics • Cluster-ID • Host Name • Port Type • Port ID • Port Alias You can view statistics for a period of 120 days on a hourly granularity.	Rate (bps)
		Top Tx ports by Average Rate (bps)
		Tx Port Statistics (bps)
		Tx Port Statistics(pps)
		Top Tx ports by Max Traffic Trend (bps)
		Top Tx ports by Max Traffic Trend (pps)
		Top Tx ports by Average Traffic Trend (bps)
		Top Tx ports by Average Traffic Trend (pps)
		Tx Drop Rate(pps)
		Tx Discard Rate(pps)
		Tx Error Rate (pps)
Map Statistics	Displays statistics of the Maps. The metric tab displays the following visualizations: • Maps Aggregated Average Traffic (bps) Maps Aggregated Average Traffic (pps) Use the following control visualizations to filter the data: • Tag Sample - Statistics • Cluster-ID • Map Type • Map Alias	Top Maps by Avg Rate (bps)
		Top Maps by Avg Rate (pps)
		Map Statistics (bps)
		Map Statistics(pps)
		Top Map Average Traffic Trend (bps)
		Top Map Average Traffic Trend (pps)
Map Rule Statistics	Displays statistical data related to the map rules and the associated traffic.	Refer to Map Rule Statistics Dashboard for more details.
Map Traffic Statistics	Displays statistics about traffic that has passed/dropped through the fabric to the destination(s). The dashboard is categorized into:	Map Average/ Pass/Drop Traffic (bps)

Dashboard	Details	Visualizations
	• bps • pps Use the following control visualizations to filter the data: • Tag • Cluster-Id (default control filter) • Map Type • Map Alias	Map Average /Pass/Drop Traffic (pps)
Fabric Map Statistics	Displays statistical data related to Fabric Maps. Use the following control visualizations to filter the data: • Tag Sample - Statistics • Fabric Map • Cluster ID to Destination	Fabric Map Destination Tool Traffic (bps)
		Fabric Map Destination Tool Traffic (pps)
		Top Fabric Map Max Tool Traffic Trend (bps)
		Top Fabric Map Max Tool Traffic Trend (pps)
Circuit and Stack GigaStream Statistics	Displays the statistics of the circuit and stack GigaStream. The dashboards are categorized into: • Metric • Inbound Trend • Outbound Trend The metric tab displays the following visualizations: • Circuit and Stack GigaStream Total Capacity (bps) • Circuit and Stack GigaStream Total Capacity by member Ports • Circuit and Stack GigaStream Tx Aggregated Max • Circuit and Stack GigaStream Tx Aggregated Average • Circuit and Stack GigaStream Tx Aggregated Average Drop • Circuit and Stack GigaStream Tx Aggregated Average Discard • Circuit and Stack GigaStream Tx Aggregated Average Error • Circuit and Stack GigaStream Rx Aggregated Max • Circuit and Stack GigaStream Rx Aggregated Average • Circuit and Stack GigaStream Rx Aggregated Average Drop • Circuit and Stack GigaStream Rx Aggregated Average Discard • Circuit and Stack GigaStream Rx Aggregated Average Error Use the following control visualizations to filter the data: • Sample Tag	Circuit and Stack GigaStream Tx Traffic Rate (bps)

Dashboard	Details	Visualizations
	- Cluster ID - Host Name - GigaStream	

Dashboard	Details	Visualizations
		Circuit and Stack GigaStream Tx Traffic Rate(pps)
		Circuit and Stack GigaStream Maximum Tx Rate (bps) by member port Alias
		Circuit and Stack GigaStream Maximum Tx Rate (pps) by member port Alias
		Circuit and Stack GigaStream Average Tx Rate (bps) by member port Alias
		Circuit and Stack GigaStream Average Tx Rate (pps) by member port Alias
		Circuit and Stack GigaStream Tx packets Drop Rate (pps)
		Circuit and Stack GigaStream Tx packets Discard Rate (pps)
		Circuit and Stack GigaStream Tx packets Error Rate (pps)
		Circuit and Stack GigaStream Rx Traffic Rate (bps)
		Circuit and Stack GigaStream Rx Traffic Rate (pps)
		Circuit and Stack GigaStream Maximum Rx Rate (bps) by member port Alias
		Circuit and Stack

Dashboard	Details	Visualizations
		GigaStream Maximum Rx Rate (pps) by member port Alias
		Circuit and Stack GigaStream Average Rx Rate (bps) by member port Alias
		Circuit and Stack GigaStream Average Rx Rate (pps) by member port Alias
		Circuit and Stack GigaStream Rx packets Drop Rate (pps)
		Circuit and Stack GigaStream Rx packets Discard Rate (pps)
Tool GigaStream Statistics	Displays the statistics of the Tool GigaStream. The dashboards are categorized into: - Metric - Trend The metric tab displays the following visualizations: - Tool GigaStream Total Capacity ((bps) - Tool GigaStream Total Capacity by member Ports - Tool GigaStream Tx Aggregated Average (bps) - Tool GigaStream Tx Aggregated Average Drop Traffic Rate (pps) - Tool GigaStream Tx Aggregated Average Discard Traffic Rate (pps) - Tool GigaStream Tx Aggregated Average Error Traffic Rate (pps) - Tool GigaStream Tx Ports Aggregated Max (bps) Use the following control visualizations to filter the data: - Sample Tag - Cluster ID - Host Name - GigaStream	Tool GigaStream Tx Traffic Rate (bps)
		Tool GigaStream Tx Traffic Rate(pps)
		Tool GigaStream Maximum Tx Rate (bps) by member port Alias
		Tool GigaStream Average Tx Rate(pps) by member port Alias
		Tool GigaStream Average Tx Rate (bps) by member port Alias
		Tool GigaStream Maximum Tx Rate (pps) by member port Alias
		Tool GigaStream Tx packets Discard Rate (pps)
		Tool GigaStream Tx packets Drop Rate

Dashboard	Details	Visualizations
		(pps)
GsGroup Statistics	Displays the GigaSMART group statistics: - GsGroup Total Capacity (bps) - GsGroup Total Capacity by member Ports Use the following control visualizations to filter the data: - Sample Tag - Cluster ID - Host Name - GSGroup	GsGroup Max Rx Rate (bps)
		GsGroup Max Rx Rate (pps)
		GsGroup Average Rx Rate (bps)
		GsGroup Average Rx Rate (pps)
		GsGroup Max Rx Rate (bps) by GsEngine Member ports
		GsGroup Max Rx Rate (pps) by GsEngine Member ports
		GsGroup Avg Rx Rate (bps) by GsEngine Member ports
		GsGroup Avg Rx Rate (pps) by GsEngine Member ports
		GsGroup Drop Rate (pps)
		GsGroup Drop Rate by Member Port in Percentage
		GsGroup Packet Buffer Utilization in Percentage
		GsGroup CPU Utilization in Percentage
Fabric Asset Inventory	Displays details about the devices managed by GigaVUE-FM: - Devices - Cards - Fans - Power - Power Modules	Gsgroup Packet buffer and CPU utilization Alert

Dashboard	Details	Visualizations
	- Port SFPs Click the Export: Formatted link option to download the data in each of the visualizations in CSV format. You can also use the Reporting option in the top menu to download the report in PDF or PNG format. Use the following control visualizations to filter the data: - Tag Sample - Inventory - Cluster ID - Host Name	
Capacity Planning	Consists of the following dashboards: - Port - Filter Resources Use the following control visualizations to filter the data: - Tag Sample - Inventory - Cluster ID - Host Name - Port Type - Port ID - Port Alias	
	Port	<i>Port Capacity Distribution</i>
		<i>Port Capacity Distribution - Cluster Id</i>
		<i>Port Summary</i>
	Filter Resources	<i>Filter Resource - Map Rule</i>
		<i>Filter Resource - App Filter</i>
		<i>Filter Resource - Port Filter</i>
Fault Collector	The Fault Collector tab consists of the following two dashboards: - Port Flapping - GigaSMART Core Crash Use the following Control Visualizations to filter the data: - Sample Tag	

Dashboard	Details	Visualizations
	- Cluster ID - Host Name - Port ID - Port Alias	
	Port Flap Displays visualizations related to port flapping.	- Port Flap Events - Port Flapping Histogram - Port Link State Changes - Port Flaps by SFP Part Number - Port Flaps by SFP Vendor Name - Port Flapping Report
	GigaSMART Core Crash Displays visualizations related to GigaSMART application crash.	- GigaSMART App Core Crash Events - GSApp Crashes Histogram - GSApp Crashes by Cluster ID - GSApp Crashes Report
Reports	Provides launch point for various reports. Click the Reports link to view the reports. You can perform the following operations: - Download the data tables in CSV file format. - Export data using Reporting → Generate PDF/PNG. NOTE: The CSV files display only a maximum of 10,000 records. If the number of records exceed 10,000 the additional records do not get displayed in the report.	- Inventory Reports - Performance and Utilization Reports - Fabric Asset Inventory (Physical) Reports
Fault Collector	The Fault Collector tab consists of the following two dashboards: - Port Flapping - GigaSMART Core Crash Use the following Control Visualizations to filter the data: - Sample Tag - Cluster ID	

Dashboard	Details	Visualizations
	- Host Name - Port ID - Port Alias	
Cloud Dashboards	Displays the statistics of virtual resources.	Refer to Virtual Inventory Statistics and Cloud Applications Dashboard
Hybrid Dashboards	Displays statistics of hybrid solutions . This tab has the following dashboard: Secure Tunnels.	
	Secure Tunnels Displays visualizations related to Secure tunnels. Use the following control visualizations to filter data: - Environment - Server / Remote/ Listener Port - Server /Remote / Listener IP	- Average TLS Tunnel Decap Packets - Average TLS Tunnel Encap Packets - Average TLS Tunnel Decap Errors - Average TLS Tunnel Encap Errors - Average TLS Tunnel Encap Packets per IP and port - Average TLS Connection Stats
Inline SSL Dashboards	Displays statistics for Inline TLS/SSL sessions. This tab has the following dashboards: - Session Overall - Session Engine Overview - Traffic Insights - Session Insights - Session Table	

Dashboard	Details	Visualizations
	Engine Diagnostics	
Session Overall	Displays overall count of TLS/SSL sessions intercepted by the node including decrypted, non-decrypted and non-SSL sessions. Use the following control visualizations to filter data: - Host Name - GsGroup Alias - GsEngine ID	- Total Intercepted Sessions - Sessions Trend - Average Decryption Rate - Client TLS Version Trend - Server TLS Version Trend - Policy Based Intercepted Sessions - Intercepted Sessions By Policy Rules
Session Engine Overview	Displays Inline TLS/SSL Session statistics per engine. Use the following control visualizations to filter data: - Host Name - GsGroup Alias - GsEngine ID	- Session Rate Per Engine - Average Decryption Rate Per Engine - Average CPS Per Engine - Engine Metric Table - Average CPU Per Engine
Traffic Insights	Displays the traffic details for each Inline TLS/SSL Session. Use the following control visualizations to filter data: - Host Name - GsGroup Alias - GsEngine ID	- Client Throughput(bps) - Server Throughput(bps) - Overall Volume (Bytes) - Overall Decrypted Volume(Bytes) - Average & Peak value of CPU & CPS - Average CPU Per Engine - Max CPU Per Engine - Max CPS Per

Dashboard	Details	Visualizations
		<i>Engine</i> • <i>CPU Trend Per Engine</i> • <i>CPS Trend Per Engine</i> • <i>CPS Trend & CPU Trend Correlation</i> • <i>Throughput Trend On Network</i> • <i>Throughput Trend On Tool</i>
<i>Session Insights</i>	Displays detailed information about the TLS/SSL session. Use the following control visualizations to filter data: • Host Name • GsEngine ID • Source IP • Destination IP	• <i>Decryption Status</i> • <i>SSL Mode</i> • <i>SSL State</i> • <i>Policy Match By Rules</i> • <i>TLS Version</i> • <i>Top URLs (Max 10)</i> • <i>Top URL Categories (Max 10)</i> • <i>Top Ciphers (Max 10)</i> • <i>Certificates By Type</i>

Dashboard	Details	Visualizations
Session Table	Displays the entire details of a TLS /SSL session in a tabular format. Use the following control visualizations to filter data: • Host Name • GsEngine ID • URL • Source IP • Destination IP • URL Category	• <i>Session Table</i> • <i>Session Table with Policy Debug</i>
Engine Diagnostics	Engine Diagnostics tab provides troubleshooting information of Inline TLS/SSL sessions intercepted by the engine. Use the following control visualizations to filter data: • Host Name • GsGroup Alias • GsEngine ID	• <i>Certificates verified in Cache</i> • <i>SSL Alerts</i>

Dashboard

When you first login to GigaVUE-FM, the Dashboard - Physical & Virtual page is displayed by default. You can navigate to Health Monitor Dashboards from the left navigation pane.

[Table 2: Summary of Dashboard Navigation](#) provides descriptions of the top navigation bar and the left navigation pane in GigaVUE-FM.

Table 2: Summary of Dashboard Navigation

Top Navigation Bar	Left Navigation Pane
Dashboard	Physical & Virtual —Displays the informational widgets for the physical and Virtual nodes.
	Health Monitor—Displays information about GigaVUE-FM such as CPU usage, amount of storage used and available.
Profiles	Allows you to create and view the profiles. A profile allows you to create a customized dashboard to monitor the physical and virtual nodes.

Dashboards for Volume-based Licenses Usage

Licensed GigaSMART applications, when running on a GigaVUE V Series node, generate usage statistics. In the Volume-based Licensing (VBL) scheme, a license entitles specific applications on your V Series nodes to use a specified amount of total data volume over the term of the license. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility into the actual amount of data, each licensed application is using on each node, and track the overuse if any.

In cloud environment:

- when a monitoring session is created and deployed, you can only use applications that are licensed at that point.
- When a license expires, you will be notified, along with a list of monitoring sessions that would be affected in the near future.
- When a license finally expires (and has not been renewed yet), the monitoring sessions using the corresponding license will be undeployed, but not deleted from the database.
- When a license is later renewed or newly imported, such undeployed monitoring sessions will be redeployed.

Using the Volume-based License Application Usage and Bundle Usage dashboards, you can plan for better utilization of the licenses. These dashboards work on the principles of Analytics and are listed together with other dashboards. These VBL dashboards include both summary and daily dashboard pages.

- **Summary usage dashboard:** Displays summary for each period of VBL usage
- **Daily usage dashboard:** Displays more detailed view (down to the granularity of one day) about the app and bundle usages.

NOTE: Clicking on a bar chart on the App or Bundle Usage Summary dashboards does not display any further information. To view the originally displayed visualization if clicked inadvertently as mentioned above, navigate to a different dashboard and return to the original dashboard.

To access the dashboards:

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

Table 3:

Dashboard	Visualizations	Description
Daily App Usage	Licensed App Allowance vs Usage	Displays details about the daily usage of each of the licensed application against the allowance provided and the overage. By default, it is shown for a 90-day time period. However, you can change the interval to the required time period.
	Aggregate Summary	Displays the following aggregation statistics: • Highest Daily Usage • Average Daily Usage • 95th Percentile Daily Usage¹. • Highest Daily Overage • Average Daily Overage • Average Daily Allowance
Daily Bundle Usage	VBL Bundle Usage	Displays details about the usage of bundled license against the allowance and the overage. The bundle can be coreVUE or netVUE.

¹The 95th percentile daily usage for any day is calculated as follows: the daily usage for the trailing 90 days, including and up to the current day, are sorted in ascending order and the usage at the 95th percentile (near the high end) is reported as the 95th percentile usage for the day. In the daily usage widgets, the aggregate statistics uses the maximum of the 95th percentile usage for the days selected as per the Time Filter. The 95th percentile usage statistic allows the user to disregard exceptionally high values of usage (might have occurred due to extraordinary conditions) which do not represent normal high values.

Dashboard	Visualizations	Description
	Aggregate Summary	Displays the following aggregation statistics: • Highest Daily Usage • Average Daily Usage • 95th Percentile Daily Usage • Highest Daily Overage • Average Daily Overage • Average Daily Allowance
App Usage Summary	• Usage (all applications) • Overage (all applications) • Summary per period (Incoming traffic) • Data Usage vs Overage (Incoming traffic)	The Usage Period drop-down option at the top allows you to choose the period for which you want to view the usage details. The duration of each period is 3 months. The following visualizations are displayed for the selected period: • Usage (all applications): Displays breakdown of usage of all your applications • Overage all applications: Displays breakdown of overage of all your applications • Summary per period (Incoming traffic): Displays a tabular view of the license usage/overage summary for the selected period, considering the incoming data traffic (before being processed by the Gigamon applications), • Data Usage vs Overage (Incoming traffic): Displays a bar chart of the license usage vs. overage summary for the selected period. If you do not select the Usage Period, the aggregation of all periods' data is displayed in the top visualizations, and the summary for each of the periods is displayed in the bottom visualizations in the dashboard.
Bundle Usage Summary	• Summary per Period • Bundle Usage vs Overage (Incoming traffic)	The Bundles drop-down allows you to choose the bundle for which you want to see the usage details. • Summary per Period: Displays a tabular view of the bundle usage summary for each period. Days with overage within each period are displayed within this tabular view. The tabular view also includes the total licensed data allowance for the days already elapsed in each period. • Bundle Usage vs Overage (Incoming traffic): Displays a bar chart of the license usage vs. overage summary for the selected bundle.

Dashboard	Visualizations	Description
		If you do not select any bundle, the summary views include the sum of metric values for all bundles that were active during a period.

Refer to the [Analytics](#) section for details on how to clone a dashboard, create a new visualization, and other detailed information.

Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. In case of virtual environment, Analytics support is available for the following cloud platforms:

- AWS
- OpenStack
- VMware ESXi
- Azure

To access the dashboards:

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

The following table lists the various virtual dashboards:

Dashboard	Displays	Visualizations	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: - Number of Monitoring Sessions - Number of V Series Nodes - Number of Connections - Number of GCB Nodes You can filter the visualizations based on the following control filters: - Platform - Health Status	<i>V Series Node Status by Platform</i>	Number of healthy and unhealthy GigaVUE V Series Nodes for each of the supported cloud platforms.
		<i>Monitoring Session Status by Platform</i>	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		<i>Connection Status by Platform</i>	Number of healthy and unhealthy connections for each of the supported cloud platforms
		<i>GCB Node Status by Platform</i>	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: - Platform - Connection - V Series Node	<i>V Series Node Maximum CPU Usage Trend</i>	Line chart that displays maximum CPU usage trend of the GigaVUE V Series Node in 5 minutes interval, for the past one hour. Note: The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor GigaVUE V Series Nodes do not have service cores, therefore the CPU usage is reported as 0.

Dashboard	Displays	Visualizations	Displays
		<i>V Series Node with Most CPU Usage For Past 5 minutes</i>	Line chart that displays Maximum CPU usage of the GigaVUE V Series Node for the past 5 minutes. Note: You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Rx Trend</i>	Receiving trend of theGigaVUE V Series Node in 5 minutes interval, for the past one hour.
		<i>V Series Network Interfaces with Most Rx for Past 5 mins</i>	Total packets received by each of the V Series network interface for the past 5 minutes. Note: You cannot use the time based filter options to filter and visualize the data.
		<i>V Series Node Tunnel Rx Packets/Errors</i>	Displays the reception of packet at the Tunnel RX. This is the input toGigaVUE V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, GigaVUE V Series Node, tunnelName}, before aggregation.
		<i>V Series Node Tunnel Tx Packets/Errors</i>	TX is for output tunnels from VSN. GigaVUE V Series Node Tunnel Tx

Dashboard	Displays	Visualizations	Displays
			Packets/Errors
Dedup	Displays visualizations related to De-duplication application. You can filter the visualizations based on the following control filters: - Platform - Connection - V Series Node	<i>Dedup Packets Detected/Dedup Packets Overload</i>	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		<i>Dedup Packets Detected/Dedup Packets Overload Percentage</i>	Percentage of the de-duplicated packets received against the de-duplication application overload.
		<i>Total Traffic In/Out Dedup</i>	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as the number of packets. You can select the following control filters, based on which the visualizations will get updated: Monitoring session: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that is used by the V Series node are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. V Series node: Management IP of the V Series node. Choose the required V Series node from the drop-down. Tunnel: Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out.	<i>Tunnel Bytes</i>	Displays received tunnel traffic vs transmitted tunnel traffic, in bytes. - For input tunnel, transmitted traffic is displayed as zero. - For output tunnel, received traffic is displayed as zero.

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

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

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

Rules and Notes

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations. Refer to the [Clone Dashboard](#) section for more details.
- Use the Time Filter option to select the required time interval for which you need to view the visualization.
- Refer to the [Analytics](#) section for details on how to create a new dashboard, clone a dashboard, create a new visualization, and other information about the Discover page and Reports page.

FHA Dashboards for 5G Applications

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly.

5G Applications dashboard provides comprehensive insights into the performance and statistics of GVHTTP2, 5G-Cloud, and 5G-SBI applications. Users can monitor Transaction Metrics, Queue Information, Request Metrics, URI Validation, and VXLAN Network Traffic using the 5G Apps dashboard. Analytics support is available for the following cloud platforms:

- VMware ESXi
- OpenStack
- Third Party Orchestration

To access the dashboards:

1. Go to  -> **Analytics -> Dashboards.**
2. Navigate to **System Dashboards -> 5G Apps Dashboards**. Click on the **Overall 5G Apps** or **Detailed 5G Apps** to view the visualizations.

Refer to the following sections to view the various 5G Apps visualizations:

- [Overall 5G Apps Dashboard](#)
- [Detailed 5G Apps Dashboard](#)
- [NokiaSCP Statistics](#)
- [OracleSCP Statistics](#)
- [EricssonSCP Statistics](#)
- [NokiaHEP3 Statistics](#)
- [Ericsson vTAP Statistics](#)

Overall 5G Apps Dashboard

Displays the overall visualization details of 5G Apps. To access the dashboards:

1. Select the required 5G-Cloud Monitoring Session Name and the GVHTTP2 Monitoring Session Name from the drop-down lists.
2. Select the required GigaVUE V Series Node names from the drop-down list.

Table 1: Overview of 5G Apps Dashboard – Metrics, Visualizations, and Transaction Details

Visualizations	Details
GVHTTP2 Transactions	Displays the cumulative count of Total HTTP2 transactions that occurred in the selected GVHTTP2 Servers, along with a breakdown of successful and failed transactions.
5G-Cloud Transactions	Displays the Total, Partial, and Failed Transactions that occurred in 5G-Cloud. For Nokia SCP, Total and Partial Transactions are not supported.
GVHTTP2 Queue	Displays the cumulative number of packets placed in or removed from the RX queue and the number of packets attempting to enter the RX Queue when it is full, and RX packets dropped due to queue limitations or excessive message size.
GVHTTP2 Stream Failures	Displays the cumulative count of total number of packet where headers or data frames were received but could not be processed because stream size exceeds maximum supported stream size, also total occurrences where a new HTTP2 streams which are timed out on the GVHTTP2 servers.
GVHTTP2 SSL Connection / Socket / ngtcp2 library failures	Displays the cumulative count of total SSL connection failures and socket failures in either mTLS or clear text mode, and the total ngtcp2 library errors in the GVHTTP2 servers.
GVHTTP2 Tx Socket Errors	Displays the cumulative count of the total number of packets that failed to transmit to the TX Tunnel.
GVHTTP2 Request Types	Displays the cumulative count of total HTTP2 requests received by the GVHTTP2 servers, categorized into GET, POST, PUT, and other types of requests.
GVHTTP2 URI's	Displays the cumulative count of the number of HTTP2 requests with Valid and Invalid paths for the current GVHTTP2 mode.
GVHTTP2 Tx Packets	Displays the count of the total number of packets successfully transmitted to the TX Tunnel. This visualization is not intended for comparative analysis.
5G-Cloud Rx Packets	Displays the cumulative count of the total received packets from the GVHTTP2 application. This visualization is not intended for comparative analysis.
5G-Cloud Rx Drops	Displays the total number of messages/packets drops due to queue full and VNI ID mismatch.
5G-Cloud Transaction Flow	Displays the total number of transaction flows allocated and active,

Visualizations	Details
	the number of times a new Transaction Flow was retrieved, and the number of times Transaction Flows were inserted.
5G-Cloud Transaction Flow Error	Displays the total number of errors encountered while attempting to retrieve new Transaction Flows, insert Transaction Flows into the active table, and age out Transaction Flows.
5G-Cloud TCP Flow	Displays the total number of TCP flows allocated and active, the total number of times a new TCP Flow was retrieved, and the total number of times TCP Flows were inserted into the Active TCP Flow table during the interval.
5G-Cloud TCP Flow Error	Displays the total number of failures when attempting to retrieve new TCP flows, errors when inserting TCP flows into the active table, and instances of TCP flows that have aged out.
5G-Cloud Tool Synthesized Requests & Responses	Displays the cumulative count of Mirrored Transaction HTTP/2 requests and responses synthesized towards the tool port output, including retransmissions.
5G-Cloud Tool Synthesized Packets	Displays the total cumulative count of Mirrored Transaction packets synthesized toward the tool port. This visualization is not intended for comparative analysis.
5G-Cloud Tx Packets	Displays the cumulative count of total transmitted packets sent to the tool. This visualization is not intended for comparative analysis.

Detailed 5G Apps Dashboard

Displays the detailed visualizations details of 5G Apps. To access the dashboards:

1. Select the required 5G-Cloud Monitoring Session Name and the GVHTTP2 Monitoring Session Name from the drop-down lists.
2. Select the required GigaVUE V Series Node names from the drop-down list.

Table 2: Detailed 5G Apps Dashboard – Visualization and Metrics Overview

Visualizations	Details
Total Transactions occurred per GVHTTP2	Displays the total number of HTTP2 transactions that occurred per GVHTTP2 Server.
Total Transactions Successful per GVHTTP2	Displays the total number of Successful HTTP2 transactions that occurred per GVHTTP2 Server.
Total Transactions Failed per GVHTTP2	Displays the total number of Failed HTTP2 transactions that occurred per GVHTTP2 Server.
5G-Cloud Transactions	Displays the Total, Partial, and Failed Transactions that occurred in 5G-Cloud. For Nokia SCP, Successful and Partial transactions are not applicable.
Packets Queued In per GVHTTP2	Displays the number of packets in RX queue.
Packets Queued Out per GVHTTP2	Displays the number of packets dequeued from the RX queue.

Visualizations	Details
Packets Queued Full per GVHTTP2	Displays the number of packets dropped due to RX queue being full.
Rx Packet Drops per GVHTTP2	Displays the number of RX packets dropped due to queue limitations.
Rx packets Oversized per GVHTTP2	Displays the number of RX packets that were dropped due to the greater message size.
Stream Header Overflows per GVHTTP2	Displays the total number of packets where headers were received but could not be processed because stream size exceeds maximum supported stream size on the GVHTTP2 server.
Stream Buffer Overflows per GVHTTP2s	Displays the total number of packets where data frames were received but could not be processed because stream size exceeds maximum supported stream size on the GVHTTP2 server.
Stream Timeouts per GVHTTP2	Displays the total occurrences where HTTP2 streams are timed out on the GVHTTP2 server.
Total SSL Connection Failures per GVHTTP2	Displays the total SSL connection failures in the GVHTTP2 server.
Total Socket Failures per GVHTTP2	Displays the total socket failures in mTLS or clear text mode in the GVHTTP2 server.
Total nghttp2 library errors per GVHTTP2	Displays the total nghttp2 library errors in the GVHTTP2 server.
TX Socket Send Errors per GVHTTP2	Displays the total number of packets that failed to transmit to the TX Tunnel.
TX Socket Size Errors per GVHTTP2	Displays the total number of packets that failed to transmit to the TX Tunnel due to the larger packet size.
Total Requests per GVHTTP2	Displays the total number of HTTP2 requests received by the GVHTTP2 Server.
GET Requests per GVHTTP2	Displays the total number of HTTP2 GET requests received by the GVHTTP2 Server.
POST Requests per GVHTTP2	Displays the total number of HTTP2 POST requests received by the GVHTTP2 Server.
PUT Requests per GVHTTP2	Displays the total number of HTTP2 PUT requests received by the GVHTTP2 Server.
Other Requests per GVHTTP2	Displays the total number of HTTP2 Other requests received by the GVHTTP2 Server.
Total URI's per GVHTTP2	Displays the number of URI's.
Requests with Valid URI's per GVHTTP2	Displays the number of HTTP2 requests with Valid paths.
Requests with Invalid URI's per GVHTTP2	Displays the number of HTTP2 requests with Invalid paths.
TX Packets per GVHTTP2	Displays the total number of packets successfully transmitted to the VXLAN TX Tunnel per GVHTTP2. This visualization is not intended for comparative analysis.
5G-Cloud Rx Packets	Displays the cumulative count of the total packets received from the GVHTTP2 application. This visualization is not intended for comparative analysis.

Visualizations	Details
5G-Cloud Rx Drops	Displays the total number of messages/packets drops due to queue full and VNI ID mismatch.
5G-Cloud Transaction Flow	Displays the total number of transaction flows allocated and active, the number of times a new Transaction Flow was retrieved, and the number of times Transaction Flows were inserted.
5G- Cloud Transaction Flow Error	Displays the total number of errors encountered while attempting to retrieve new Transaction Flows, insert Transaction Flows into the active table, and age out Transaction Flows.
5G-Cloud TCP Flow	Displays the total number of TCP flows allocated and active, the total number of times a new TCP Flow was retrieved, and the total number of times TCP Flows were inserted into the Active TCP Flow table during the interval.
5G-Cloud TCP Flow Error	Displays the total number of failures when attempting to retrieve new TCP flows, errors when inserting TCP flows into the active table, and instances of TCP flows aging out from the Active TCP Flow table during the interval.
5G-Cloud Tool Synthesized Requests & Responses	Displays the cumulative count of Mirrored Transaction HTTP/2 requests and responses synthesized towards the tool port output, including retransmissions.
5G-Cloud Tool Synthesized Packets	Displays the total cumulative count of Mirrored Transaction packets synthesized toward the tool port. This visualization is not intended for comparative analysis.
5G-Cloud Tx Packets	Displays the cumulative count of total transmitted packets sent to the tool. This visualization is not intended for comparative analysis.

NokiaSCP Statistics

Displays the visualization details of Nokia SCP statistics. To access the dashboards:

- Select the required 5G-Cloud Monitoring Session Name and the GigaVUE V Series Node names from the drop-down lists.

Table 3: NokiaSCP Statistics – Overview of Message Parsing and Processing Metrics

Visualizations	Details
Message Parsing	Displays the total number of messages received from the SCP and indicates whether they were parsed successfully.
Parsing Errors	Displays the errors encountered while parsing the message/frame in Nokia SCP.
Message Processing	Displays the total number of messages received from the SCP that failed to process.
Processing Errors	Displays the errors encountered while processing the message/frame in Nokia SCP.

OracleSCP Statistics

Displays the visualization details of Oracle SCP statistics. To access the dashboards:

- Select the required 5G-Cloud Monitoring Session Name and the GigaVUE V Series Node names from the drop-down lists.

Table 4: Overview of OracleSCP message parsing and processing metrics, including error statistics.

Visualizations	Details
Message Parsing	Displays the total number of messages received from the SCP and indicates whether they were parsed successfully.
Parsing Errors	Displays the errors encountered while parsing the message/frame in Oracle SCP.
Message Processing	Displays the total number of messages received from the SCP that failed to process.
Processing Errors	Displays the errors encountered while processing the message/frame in Oracle SCP.

EricssonSCP Statistics

Displays the visualization details of Ericsson SCP statistics. To access the dashboards:

1. Select the required 5G-Cloud Monitoring Session Name and the DPDK MonitoringSession Name from the drop-down lists.
2. Select the required GigaVUE V Series Node names from the drop-down list.

Table 5: Ericsson SCP packet and stream statistics overview.

Visualizations	Details
Rx packets from Ericsson SCP	Displays the packet statistics received at Ericsson SCP, showing only the packets forwarded to the 5G-Cloud App
Tx packets to 5g Cloud	Displays the packet statistics transmitted to the 5G-Cloud application.
5g Cloud App Packets	Displays the packet statistics for the 5G-Cloud application, including packets received from Ericsson SCP and packets transmitted to Tools.
HTTP2 Monitored Streams	Displays the statistics of concurrent HTTP2 monitored stream flows.
HTTP2 Monitored Stream Errors	Displays statistics of concurrent HTTP2 Monitored Streams during error and age-out conditions.
TCP Monitored Flows	Displays statistics of concurrent TCP monitored flows.
TCP Monitored Flow Errors	Displays statistics of concurrent TCP Monitored Flows during error, age-out, and TCP reassembly timeout conditions.

NokiaHEP3 Statistics

Nokia HEP3 Statistics dashboard displays the following visualizations. To access the dashboards:

- Select the required 5G-Cloud Monitoring Session Name and the GigaVUE V Series Node names from the drop-down lists.

Message Statistics

Table 6: Displays the visualization details of Nokia HEP3 message statistics

Visualizations	Details
HEP3 Message Overall Statistics	Displays the overall statistics of HEP3 messages received at the 5G-Cloud application.
HEP3 Rx Traffic Statistics	Displays the count of HEP3 bits received each second at the 5G-Cloud application.
HEP3 Message Statistics	Displays the count of HEP3 messages received at the 5G-Cloud application.
Missing Mandatory HEP3 Chunks Statistics	Displays the statistics of missing mandatory HEP3 chunks, detailing the total number of messages that lacked these required chunks, along with individual counts for each specific missing chunk.
Available Mandatory HEP3 Chunks Statistics	Presents the statistics for the mandatory HEP3 chunks that are available. This includes the overall number of messages containing all the required chunks, along with counters for each specific mandatory chunk. In each message, only one of the IPv4 or IPv6 chunks will be included, never both.
Tx Traffic Rate in Bits from 5G-Cloud to Tool	Displays the total number of bits transmitted per second from the 5G-Cloud application to the tools or probes.
Tx Traffic Rate in Packets from 5G-Cloud to Tool	Displays the total number of packets transmitted per second from the 5G-Cloud application to the tools or probes.
HEP3 FQDN Queries Statistics	Displays the statistics for FQDN queries conducted within the 5G-Cloud application during the synthesis of HEP3 messages.
HEP3 FQDN Interface Name Statistics	Displays the statistics related to FQDN queries for interface names within the 5G-Cloud application during the synthesis of HEP3 messages.
Service Map Queries Statistics	Displays Service Map lookup query statistics generated in the 5G-Cloud Application during HEP3 message synthesis.
Service Map Action Statistics	Displays statistics for actions performed on Service Map queries in the 5G-Cloud Application during HEP3 message synthesis.

Protocol Statistics

Table 7: Displays the visualization details of Nokia HEP3 protocol statistics

Visualizations	Details
Transport Protocol Statistics	Displays the identified transport protocol statistics in the HEP3 payload.
Application Protocol Statistics	Displays the identified application protocol statistics in the HEP3 payload.
Outbound TCP Flow Statistics	Displays the Outbound TCP flow statistics data from the 5G-Cloud application to the tool/probes.
Outbound TCP Flow Error Statistics	Displays the Outbound TCP flow error statistics data from the 5G-Cloud application to the tool/probes.

Ericsson vTAP Statistics

To access the dashboards:

- Select the required EVTAP Monitoring Session Name and GigaVUE V Series Node Name from the drop-down lists to view the visualizations and metric details. Ericsson vTAP Statistics dashboard displays the following visualizations:

Packet Statistics

Table 8: Displays the visualization details of Ericsson vTAP packet statistics

Visualizations	Details
Rx Packets from EVTAP	The view displays aggregated packet statistics collected from the Ericsson VTAP interface.
5g SBI App Packets	The view displays the Rx and Tx packet statistics for the 5G-SBI application.
Tx Packets	The view displays the transmitted packet statistics.
5g SBI App Bits	The view displays the Rx and Tx bit statistics for the 5G-SBI application.
Layer 7 HTTP Ingress TEP Statistics	The view displays the packet statistics received at ingress TEPs that handle Layer 7 HTTP traffic.
Layer 7 HTTP Egress TEP Statistics	The view displays the packet statistics transmitted from egress TEPs that handle Layer 7 HTTP traffic.
Native HTTP Ingress TEP Statistics	The view displays the packet statistics received at ingress TEPs that handle native HTTP traffic.
Native HTTP Egress TEP Statistics	The view displays the packet statistics transmitted from egress TEPs that handle native HTTP traffic.
Non SBI Ingress TEP Statistics	The view displays the packet statistics received at ingress TEPs that handle non-SBI traffic.
Non SBI Egress TEP Statistics	The view displays the packet statistics transmitted from egress TEPs that handle non-SBI traffic.

TCP Statistics

Table 9: Displays the visualization details of Ericsson vTAP TCP statistics

Visualizations	Details
TCP Flows	The view displays the TCP flow statistics for the 5G-SBI application.
TCP Flow States	The view displays the statistics related to TCP flow states for the 5G-SBI application.
HTTP2 Transaction Flows	The view displays the HTTP/2 transaction flow statistics for the 5G-SBI application.
HTTP2 Transaction Flow States	The view displays the statistics related to HTTP/2 transaction flows for the 5G-SBI application.
Synthesized Statistics	The view displays the statistics related to message synthesis in the 5G-SBI application.
Error Statistics	The view displays the message synthesis error statistics for the 5G-SBI application.
Messages Statistics	The view displays the message statistics for the 5G-SBI application.
Messages Error Statistics	The view displays the message error statistics for the 5G-SBI application.
NF ID Look up	The view displays the NF Instance ID lookup statistics for the 5G-SBI application.
FQDN Look up	The view displays the FQDN lookup statistics for the 5G-SBI application.

GigaSMART Mobility Session and Flow Filtering Dashboards

GigaSMART mobility session and flow filtering dashboards display flow filtering summary reports and statistics pertaining to the mobility solutions on an hourly, daily, weekly, or monthly interval. You can export the data from the dashboards page, and create your own flow ops visualizations for your required use cases.

How to Access the Dashboards

To access the Mobility Session and Flow Filtering dashboards:

- **From the Dashboard menu:** Go to  -> **Analytics** -> **Dashboards** -> **5G LTE Sessions**
- **From the Traffic menu:** Go to  -> **Physical** -> **Orchestrated Flows** -> **Mobility** -> **Dashboard**

- **From the Inventory menu:** Go to  -> **Physical -> Nodes ->GigaSMART Groups -> Report -> Flow Filtering**

The following dashboards are displayed:

5G LTE Sessions

The following table displays visualizations for 5G and LTE Session statistics

Table 4: Default Mobility Dashboards.

Visualizations	Details
Mobility 5G Session Statistics	Displays maximum aggregation of 5G numSessions, numSessions available and session capacity for all the GigaSMART groups pertaining to the mobility solutions against the time stamp.
Mobility LTE Session Statistics	Displays maximum aggregation of LTE numSessions, numSessions available and session capacity for all the GigaSMART groups pertaining to the mobility solutions against the time stamp.
5G Sessions by GSGroup Alias	Displays the maximum aggregation of all 5G statistics parameters for each GigaSMART group pertaining to the mobility solutions. The data columns are sortable and the user can find top N values by sorting across each field.
LTE Session by GSGroup Alias	Displays the Max aggregation of all LTE statistics parameters for each GigaSMART group pertaining to the mobility solutions. The data columns are sortable and the user can find top N values by sorting across each field.
Mobility Session No SFFP Match	Displays Max aggregation of LTE and 5G num of SFFP No Match for all the GigaSMART groups pertaining to the mobility solutions against time stamp.

Flow Filtering

The following table displays visualizations related to flow filtering statistics

Table 5: Default Mobility Dashboards.

Visualizations	Details
Flow Filtering Statistics	Displays Max aggregation of controlTunnels, controlUserTunnels, controlOnlyTunnels and pendingSession for all the GigaSMART groups pertaining to the mobility solutions against timestamp.
Flow Filtering Statistics per GsGroup	Displays Max aggregation of of controlTunnels, controlUserTunnels , controlOnlyTunnels and pendingSession for each GigaSMART group pertaining to the mobility solutions. The data columns are sortable and the user can find top N values by sorting across each field.

Flow Filtering Interface Statistics

The following table displays visualizations related to flow filtering interface statistics

Table 6: Default Mobility Dashboards.

Visualizations	Details
Flow Filtering Interface Statistics - Packets	Displays Max aggregation of rxPkts, txPkts and droppedPkts for all the interface types in all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Interface Statistics - Bytes	Displays Max aggregation of rxBytes, txBytes and droppedBytes for all the interface types in all GigaSMART groups pertaining to the mobility solutions against timestamp.
Flow Filtering Interface Statistics - GTPC Packets	Displays Max aggregation of GTPC packets for all the interface types in all GigaSMART groups pertaining to the mobility solutions against timestamp.
Flow Filtering Interface Statistics - Packets Percentage	Displays Percentage for sum of tx and sum of dropped packets to sum of rx packets for all the interface types in all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Interface Statistics per Interface type	Displays Max aggregation of all Flow Filtering Interface stats for each interface type in each GigaSMART group pertaining to the mobility solutions. The data columns are sortable and the user can find top N values by sorting across each field.

The Flow Filtering Correlation Statistics

The following table displays visualizations related to flow filtering correlation statistics.

Table 7: Default Mobility Dashboards.

Visualizations	Details
Flow Filtering Correlation Statistics - Control	Displays Max aggregation of control correlations statistics for all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Correlation Statistics - User	Displays Max aggregation of user correlations statistics for all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Control Correlation Statistics per Control Message	Displays the Max aggregation of all Flow Filtering Correlation User stats for each GigaSMART group pertaining to the mobility solutions.

Flow Filtering Correlation Statistics

The following table displays visualizations related to flow filtering correlation statistics

Table 8: Default Mobility Dashboards.

Visualizations	Details
Flow Filtering Correlation Statistics - Control	Displays Max aggregation of control correlations statistics for all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Correlation Statistics - User	Displays Max aggregation of user correlations statistics for all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Control Correlation Statistics per Control Message	Displays the Max aggregation of all Flow Filtering Correlation User stats for each GigaSMART group pertaining to the mobility solutions.

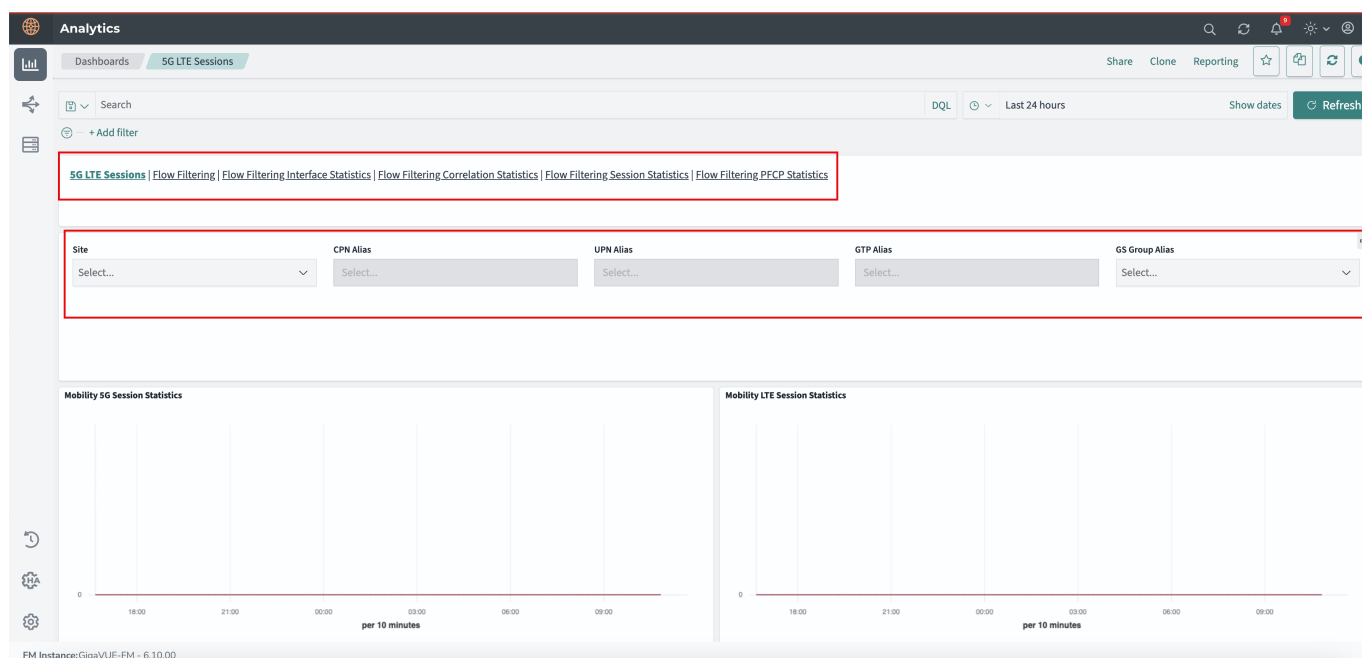
Flow Filtering Session Statistics

The following table displays visualizations related to flow filtering session statistics

Table 9: Default Mobility Dashboards.

Visualizations	Details
Flow Filtering Session Statistics - Sessions	Max aggregation of sessions for all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Session Statistics - Tunnels	Max aggregation of tunnels for all GigaSMART group pertaining to the mobility solutions against timestamp.
Flow Filtering Session Statistics per Interface type	Displays Max aggregation of all Flow Filtering session and tunnel stats for each interface type in each GigaSMART group pertaining to the mobility solutions. The data columns are sortable and the user can find top N values by sorting across each field.
GTP Threshold limit utilization Alerts	Provides an alert when the threshold has crossed the configured limit for Session usage, Tunnel usage, CPU Utilization and I Packet Buffer Utilization.
Gsgroup CPU usage in percentage	Displays percentage of CPU utilization in all GigaSMART groups pertaining to the mobility solution

Refer to the following screen shot.



Rules and Notes

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations.
- You cannot visualize CLI configurations on these default dashboards.
- Flow Filtering Dashboards are not supported for 5G flow-ops report.
- You can use the following control visualizations to filter and visualize the data based on the following criteria:
 - Site
 - CPN Alias
 - UPN Alias
 - GTP Alias
 - GS Group Alias

GigaSMART Inline TLS/SSL Dashboards

GigaSMART Inline TLS/SSL Dashboards offer insights into session performance, network capacity, traffic decryption, compliance analysis, and historical data. Monitoring decryption statuses and anomalies helps organizations enhance security.

These dashboards provide real-time alerts and detailed reports for network security administrators to maintain data integrity and security compliance. It allows you to visualize the information with GigaVUE-FM. These dashboards are supported only for Gen 3 GigaSMART card platforms.

A few of the use case scenarios where the Inline TLS/SSL Dashboard could detect and manage anomalies:

- Alert administrators when a TLS handshake involves certificates signed with insecure hash algorithms.
- Alerts can be triggered when CBC mode is used, especially in older versions of TLS (for example, TLS 1.0 and TLS 1.1), advising an upgrade to more secure cipher modes like GCM (Galois/Counter Mode).
- Identify and report the use of certificates with weak signatures in the network traffic, facilitating a swift response to enhance security.
- Automatic detection and reporting of expired certificates help maintain continuous security compliance and trust.
- Monitoring and analyzing trends in decryption success and failure rates can pinpoint disruptions or anomalies in encrypted traffic handling.

- Ensure only approved cryptographic standards are used and generate compliance reports for auditing purposes.

To access the dashboard:

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

Inline TLS/SSL Dashboard can be categorized into two types:

- Basic Dashboards
- Advanced Dashboards

Basic Dashboards

The Basic dashboards are available by default and provides an overall information on the session. You can use the below control filters and specify the time period to visualize and filter the dashboard information:

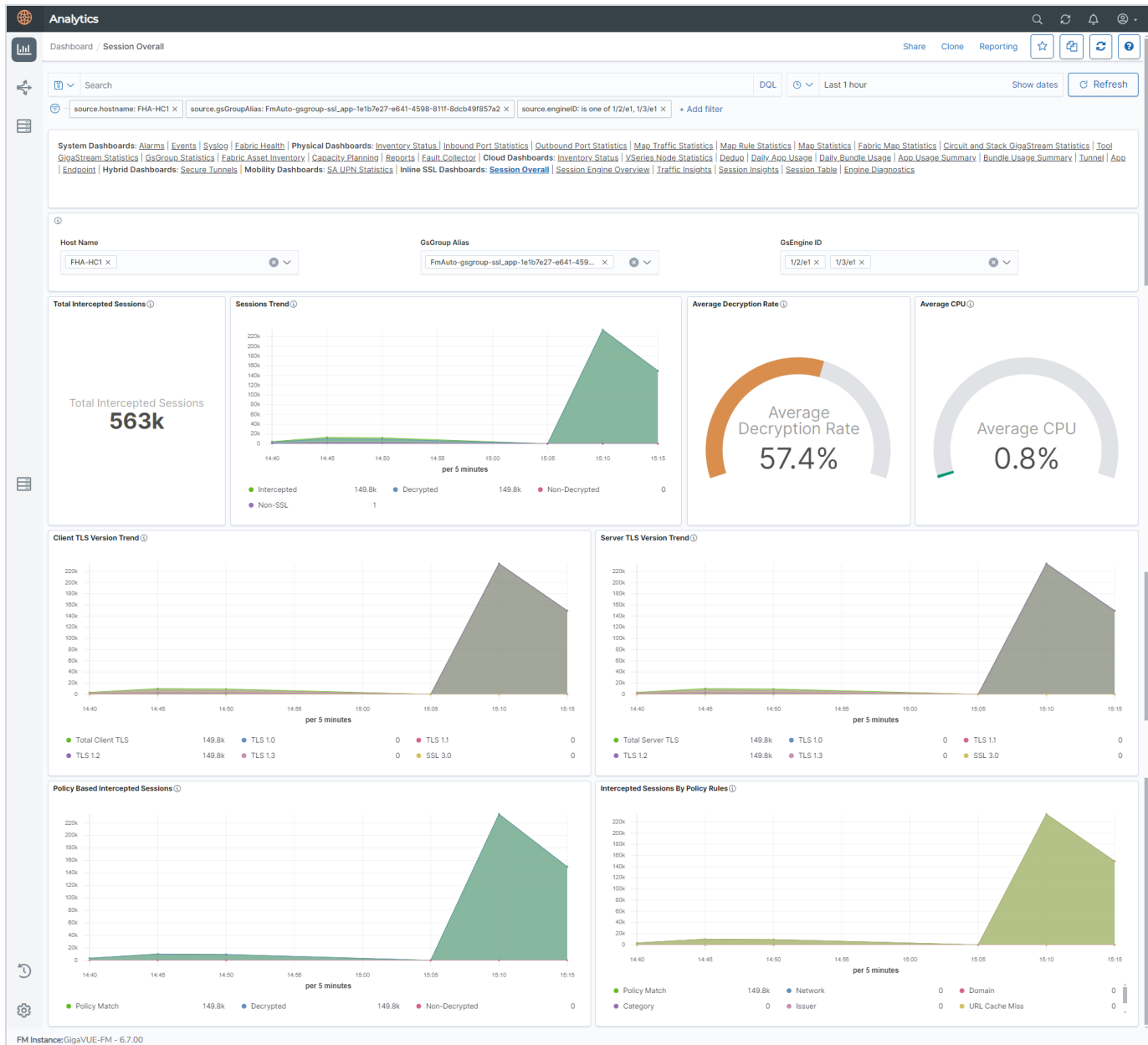
- Host Name
- GigaSMART Groups Alias (GSGroup Alias)
- GigaSMART Engine ID (GSEngine ID)

The following table displays visualizations on the overall details of encrypted traffic.

Table 10: Session Overall Dashboard

Visualizations	Details
Total Intercepted Sessions	Displays overall count of intercepted sessions by the node over time period. This page does not display per engine unless specified by a filter.
Sessions Trend	Displays the trend of all Inline TLS/SSL session that has been received over a specified time period and per specified GigaSMART engines. The trend included the visualization of the Intercepted/Decrypted/Non-SSL Sessions.
Average Decryption Rate	Displays the average rate of Inline TLS/SSL sessions that have been decrypted over the specified time period..
Average CPU	Displays an average CPU utilization of all engines in Session Overall Page.
Client TLS Version Trend	Displays an overview of the incoming traffic's TLS version of the incoming data.

Visualizations	Details
<i>Server TLS Version Trend</i>	Provides an insight into the TLS version distribution at the server side.
<i>Policy based Intercepted Session</i>	Displays the trend of decryption status of Inline TLS/SSL session based policy.
<i>Intercepted Sessions By Policy Rules</i>	Displays the trend of Inline TLS/SSL session based on Policy rules such as; Domain ,Category, Issuer, URL Cache Miss, Network and Default. Note: The no. of sessions that gets matched to a Network Policy Rule will not be displayed in the Total Intercepted Session widget.

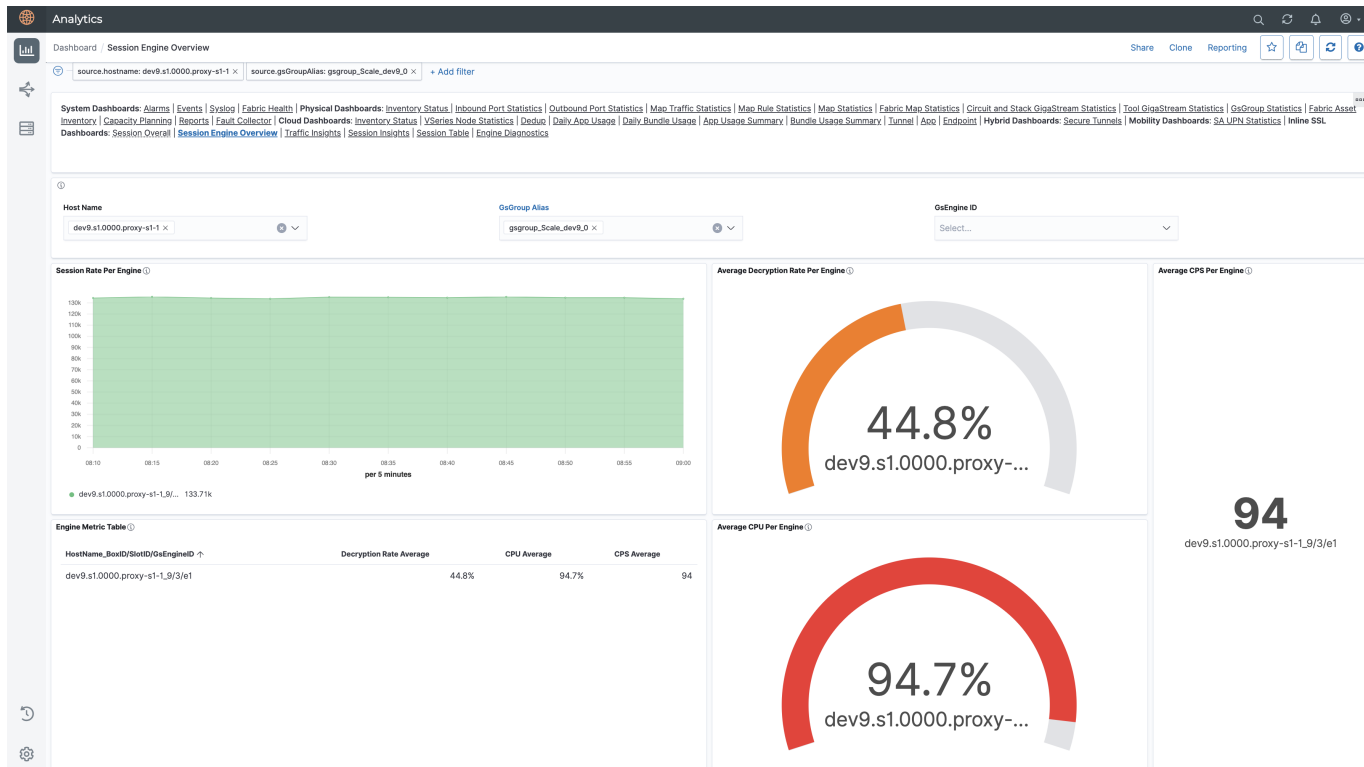


The following table displays visualizations related to Inline TLS/SSL Sessions per Engine

Table 11: Session Engine Overview Dashboard

Visualizations	Details
Sessions Rate per Engine	Displays the rate at which Inline TLS/SSL sessions are intercepted per engine.
Average Decryption Rate per Engine	Displays the average rate of sessions that got decrypted per engine.

Visualizations	Details
Average CPS per Engine	Displays the average Connections per Second (CPS) performance metric per engine.
Average CPU per Engine	Displays the average CPU utilization per engine.
Engine Metric Table	Displays the Decryption rate per engine, average CPS and average CPU rate in a tabular format. The details are displayed as Host Name/Engine ID. For example; FHA-HC1 (Host Name)_1/3/e11(GSEngine ID)

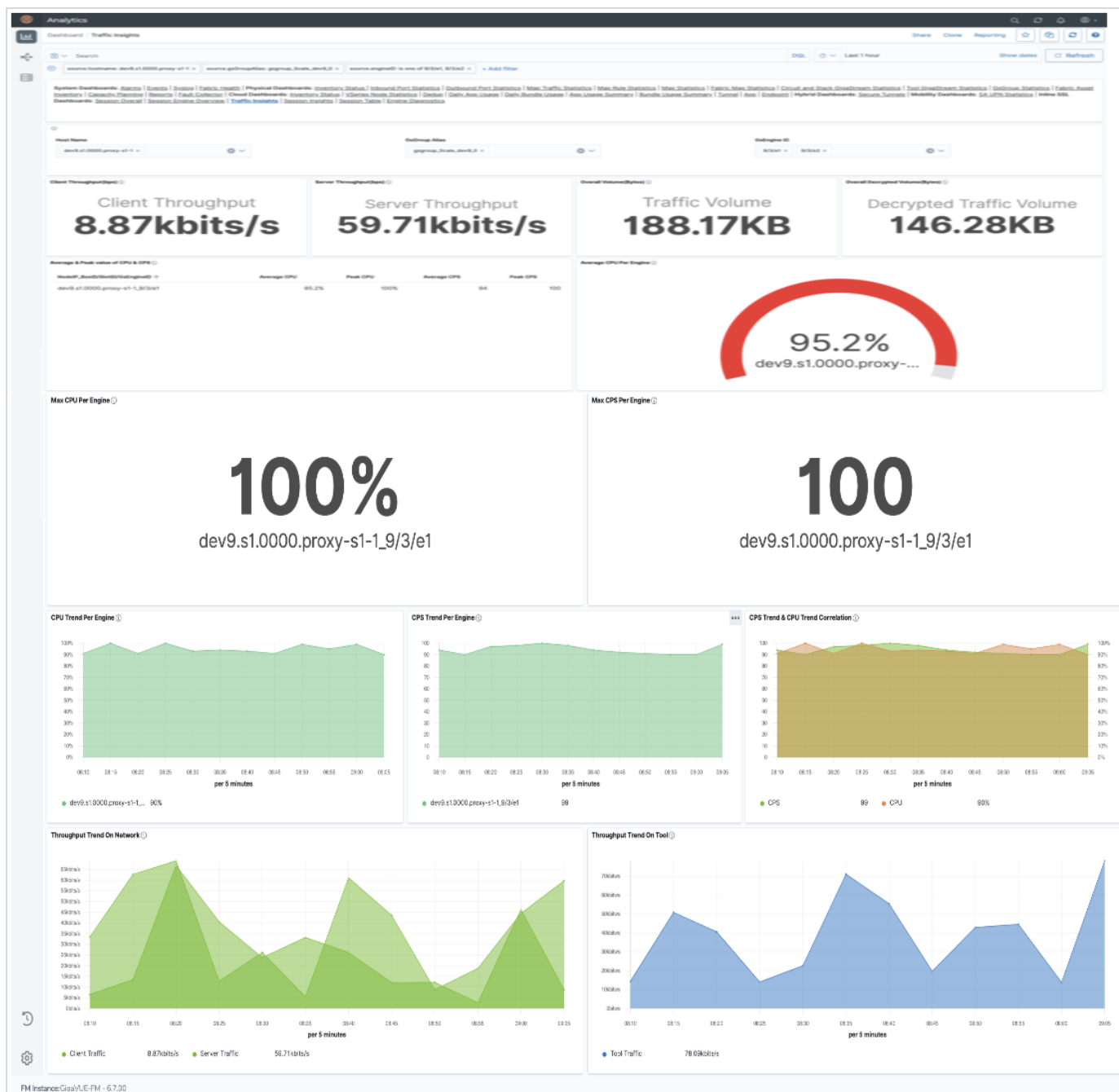


The following table displays visualizations related to the traffic that is handled with a Inline TLS/SSL sessions

Table 12: Traffic Insights Dashboard

Visualizations	Details
Client and Server Throughput (bps)	Displays the traffic throughput that is received from the client and the throughput that is handled at the server side. This throughput is displayed in bits per second (bps) value.
Overall Volume(Bytes)	Displays the volume of traffic that is being handled in

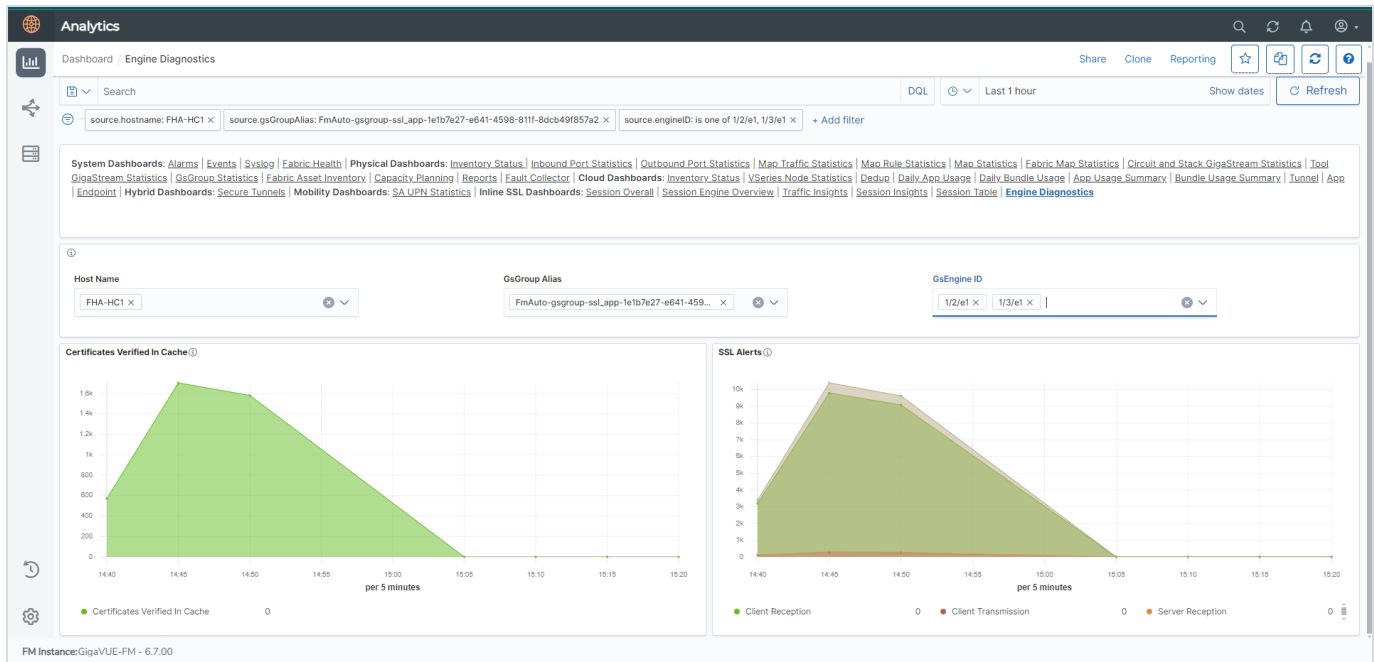
Visualizations	Details
	Bytes. This takes into account both TCP and SSL sessions.
Overall Decrypted Volume (Bytes)	Displays the overall decrypted volume of all engines unless filtered by engine ID control filter in Bytes unit
Average CPU Per Engine	Displays the average CPU performance per engine
Max CPU Per Engine	Displays the maximum CPU utilization that was observed per engine. This is static rate and is not displayed based on a time frame.
Max CPS Per Engine	Displays the maximum Connection Per Second (CPS) rate that was observed per engine. This is static rate and is not displayed based on a time frame.
Average & Peak value of CPU & CPS	Displays the average and peak values of CPU and CPS observed per engine in a tabular format.
CPU Trend per Engine	Displays a trend of CPU utilization that was achieved over a time period per engine.
CPS Trend per Engine	Displays a trend of the Connections per Second that was achieved over a time period per engine.
CPS Trend & CPU Trend Correlation	Displays a correlation between the CPU and CPS trend of the engine within a time period.
Throughput Trend on Network	Display the throughput trend of traffic that was received from both client and server side.
Throughput Trend on Tool	Displays the throughput trend of traffic that was received on the Tool.



The following displays the certificates and SSL alerts related to a GigaSMART engine

Table 13: Engine Diagnostics Dashboard

Visualizations	Details
Certificates verified in Cache	Displays the number of certificates that were verified in cache over a time period
SSL Alerts	Displays the number of SSL alerts that were received both from client and server.



Advanced Dashboards

Advanced Dashboards are available only if you enable it while configuring your Inline TLS/SSL Decryption session.

System Requirements

The system requirements for utilizing Inline TLS/SSL Advanced Dashboards are as shown below.

Requirements	Support up to 100 Devices (GigaVUE-FM Standalone)	Support up to 100 Devices (GigaVUE-FM HA Mode)
Memory	128GB	128GB
Virtual CPU	Minimum 12 CPU NOTE: It is recommended to have 16 CPU for continuous traffic with maximum supported limit of 18k sessions/second for three Advanced Statistics enabled GigaSMART engines.	Minimum 12 CPU NOTE: It is recommended to have 16 CPU for continuous traffic with maximum supported limit of 36k sessions/second for six Advanced Statistics enabled GigaSMART engines.
Disk Space	Refer to "Large Configuration" category under "Virtual Computing Resource Requirement in Scaled Environments" section in GigaVUE-FM Installation and Upgrade Guide for disk space details.	Refer to "Large Configuration" category under "Virtual Computing Resource Requirement in Scaled Environments" section in GigaVUE-FM Installation and Upgrade Guide for disk space details.
Virtual Network Interface	1	1
Number of GigaVUE-FM nodes	1	3

Configure Advanced dashboard

To configure advanced dashboards:

- Go to, **Traffic**  **>Configuration Canvas > Select the device> Inline SSL APP.**
- Enable the toggle option **Advanced Session Statistics.**

Rules and Notes

Keep in mind the following rules and notes when using the Advanced Dashboard:

- Advanced Dashboard data will be retained for 24 hours.
- For a standalone GigaVUE-FM node, the Advanced Dashboard is available for a maximum of three GigaSMART engines.
- In a GigaVUE-FM High Availability group with three GigaVUE-FM nodes, a maximum of six GigaSMART engines will be supported.
- Configure NTP time sync or ensure that your device and GigaVUE-FM are synchronized with the date and time zone.

You can use the below control filters and specify the time period to visualize and filter the dashboard information:

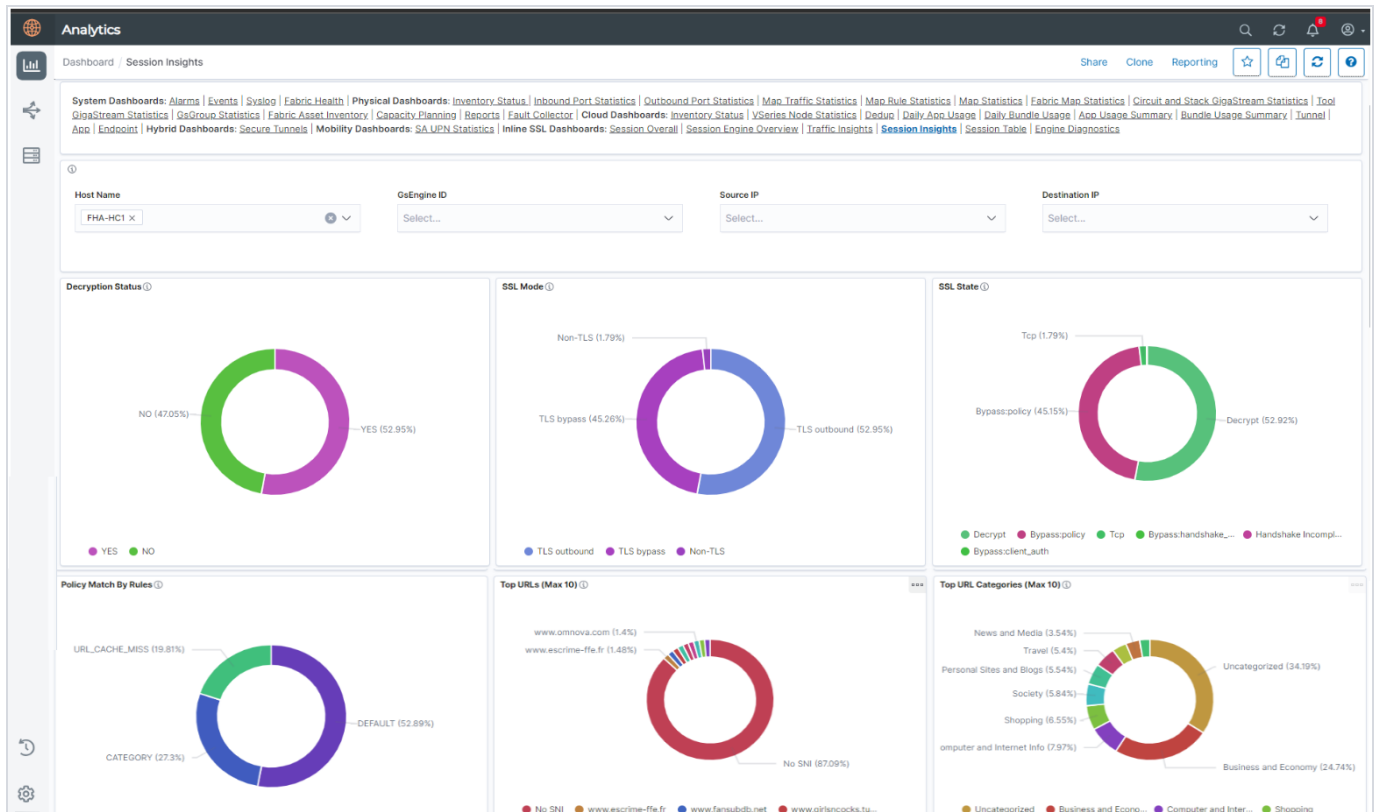
- Host Name
- GigaSMART Engine ID (GSEngine ID)

- URL (Only for Session Table Dashboard)
- Source IP
- Destination IP
- URL Category (Only For Session Table Dashboard)

The following table displays visualizations on the details of an Inline TLS/SSL session.

Table 14: Session Insight Dashboard

Visualizations	Details
Decryption Status	Displays the number of Inline TLS/SSL sessions that were decrypted and not decrypted.
SSL Mode	Displays the distribution of TLS/SSL Session modes. The modes are as follows: • TLS/SSL Outbound- : Sessions decrypted due to ISSL inbound deployment. • TLS/SSL Inbound-Sessions decrypted due to ISSL outbound deployment. • TLS/SSL Bypass- The session mode that is neither inbound or outbound. • Non-SSL - TCP sessions that are not an TLS/SSL session.
SSL State	Displays the distribution of TLS/SSL Session statuses.
Policy Match By Rules	Provides an insight into the TLS/SSL session that matches the Policy Rules. Note: The Policy Rule CATEGORY indicates the URL category.
TLS Version	Displays the TLS version of the sessions. Note: The counter "Bypass/Error" denotes sessions that were not able to determine the TLS version.
Top URLs (Max 10)	Displays the top 10 URLs that were accessed during the Inline TLS/SSL Session.
Top URL Category (10 Max)	Displays the Category of top 10 URLs accessed in Inline TLS sessions Note: 'Uncategorized' signifies SNIs that could not be categorized or Non TLS sessions. Note: 'Unknown' signifies TLS Bypass and IP address based URLs.
Top Ciphers (Max 10)	Displays the top 10 Ciphers that performed the Inline TLLS/SSL Decryption.
Certificates by Type	Displays the certificates received are valid or non-valid.



The following table displays visualizations related to Inline TLS/SSL Sessions per Engine in a tabular format.

Table 15: Session Table Dashboard.

Visualizations	Dashboard
Session Debug Table	Displays the entire Sessions Debug details throughout the system that has enabled Advanced Session Statistics. Each field can be added or removed as a customized filter option by using + - button.
Session Policy Debug Table	Displays the entire Sessions Policy Debug details throughout the system that has enabled Advanced Session Statistics. It points out to the policy rules that got matched or the policy verdict of Decryption or non decryption. Each field can be added or removed as a customized filter option by using + - button.

The screenshot displays the GigaVUE-FM Analytics interface. At the top, there's a navigation bar with 'Analytics' and a search bar. Below the navigation bar, there's a filter section with 'source.hostname: FHA-HC1' and 'source.engineID: 1/2/e1'. The main content area shows two tables: 'Session Debug Table' and 'Session Policy Debug Table'. The 'Session Debug Table' has columns for Time, certSubjectName, sslSni, srcIP, dstIP, urlCategory, sslCipher, certIssuer, protocol, certValidationStatus, and decryption. The 'Session Policy Debug Table' has columns for Time, srcIP, dstIP, srcPort, dstPort, toolStatus, sslState, policyMatch, and policyVerdict. Both tables show data for May 28, 2024, at 15:51:37:000.

Session Debug Table

Time	certSubjectName	sslSni	srcIP	dstIP	urlCategory	sslCipher	certIssuer	protocol	certValidationStatus	decryption
May 28, 2024 @ 15:51:37:000	www.malditaflojera.com	www.malditaflojera.com	10.168.3.88	192.168.3.135	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.betgps.com	www.betgps.com	10.168.32.161	192.168.4.84	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.conape.go.cr	www.conape.go.cr	10.168.17.255	192.168.4.121	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.optiononesolution.com	www.optiononesolution.com	10.168.32.160	192.168.4.196	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.pih-emr.org	www.pih-emr.org	10.168.18.1	192.168.1.46	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.vbks.at	www.vbks.at	10.168.3.88	192.168.3.110	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.ecfmultimedia.com	www.ecfmultimedia.com	10.168.3.89	192.168.2.231	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.buzzoye.pk	www.buzzoye.pk	10.168.18.0	192.168.3.69	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES
May 28, 2024 @ 15:51:37:000	www.seriesedesenhos.com	www.seriesedesenhos.com	10.168.3.90	192.168.1.126	Uncategorized	AES128-GCM-SHA256	ca1.com	TLS outbound	UNKNOWN_CA	YES

Session Policy Debug Table

Time	srcIP	dstIP	srcPort	dstPort	toolStatus	sslState	policyMatch	policyVerdict
May 28, 2024 @ 15:51:37:000	10.168.3.88	192.168.3.135	52024	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.32.161	192.168.4.84	60230	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.17.255	192.168.4.121	57387	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.32.160	192.168.4.196	53023	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.18.1	192.168.1.46	3126	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.3.88	192.168.3.110	51999	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.3.89	192.168.2.231	50647	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.18.0	192.168.3.69	35148	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT
May 28, 2024 @ 15:51:37:000	10.168.3.90	192.168.1.126	21734	443	TOOL_NOT_BYPASS	Decrypt	DEFAULT	DECRYPT

FM Instance: GigaVUE-FM - 6.7.00

OpenSearch Indices and Fields Used in Analytics

GigaVUE-FM uses the following OpenSearch indices to store data¹. These OpenSearch indices store different sets of data based on usability. The document mappings of the indices are also different.

- **fmstats***: For storing statistics information of entities such as maps, gsgrops, gsops, etc (except port)
- **fmstats_ports***: For storing statistics information of the port

¹These indices were introduced during different time frames for various purposes. The data models of these indices were designed as per the need during the time of development.

- **fminventory**: For storing the inventory and assets.
- **fmevents**: For storing events
- **fmalarms**: For storing alarms.

The following table lists the new keys introduced in software version 6.0:

Table 16:

New Field	Applicable Indices	Type	Description
resource.id.entityid	• fmalarms • fmevents • fmstats: Applicable for the following document types: ◦ vport stats ◦ gsop stats ◦ gtap port stats	text	Represents the entity ID. Holds value exactly similar to resourceid in the existing alarms/events document. If the resourceid does not exist in the document, the resource.id.entityid also will not exist. Example: For alarms related to port, port ID will be the resourceid, and resource.id.entityid.
resource.id.deviceid	• fmalarms • fmevents • fmstats_ports • fmstats: Applicable for the following document types: • gsgroup stats • gsgroup port rate core rate stats • vport stats • Map and MapRule stats • gsop stats	text	Represents the deviceid. That is, hostname. If the hostname does not exist in the document, the resource.id.deviceid also will not exist in the document
resource.id.clusterid	• fmalarms	text	Represents the clusterid. If the clusterid does not exist in the document, then resource.id.clusterid also will not exist in the document

New Field	Applicable Indices	Type	Description
	• fmstats: Applicable for the following document types: • vport stats • gsop stats		
resoure.type	• fmalarms • fmevents • fmstats: Applicable for the following document types: • vport stats • gsop stats	text	Represents the resource type (port, map, device, gsgroup)
resource.id.alias	• fmalarms • fmevents • fminventory • fmstats_ports • fmstats: Applicable for the following document types: • vport stats • gsop stats • Map and Map Rule stats	text	Represents the alias name of the associated entity of the alarm. If the alias does not exist in the document, then resource.id.alias will not exist in the document.
resource.name	• fminventory • fmstats • fmstats: Applicable for the following document types: • vport stats • gsop stats		Represents the key used to uniquely identify a particular entity across the system. For example, for ports, ClusterID, and PortId can be combined and used to uniquely identify the entity. In case of map, ClusterID, and map alias name are used. The value will be in the form of ClusterId__EntityId
port.alias	fmstats_ports		Represents the alias name of the port's alias.
port.dir	fmstats_ports		Represents the direction of the port.

New Field	Applicable Indices	Type	Description
gsGroup.alias	• fmstats: Applicable for the following document types: • gsgroup stats • gsgroup port rate, and core rate stats documents • vport stats • gsop stats		Represents the alias name of the gsgroup alias
map.alias	• fmstats: Applicable for the following document types: • Map and MapRule stats • gsop stats		Represent the alias name of the map alias
gsVport.alias	• fmstats: Applicable for the following document types: • vport stats • gsop stats		Represents the alias name of the vport alias

New Field	Applicable Indices	Type	Description
cluster.mode	fminventory		Represents the mode of the device with respect to the cluster. Applicable values are as follows: • leader • standby • standalone • normal
linkSpeedInBits	• fmstats_ports		Represents the link speed in bits per second. Note: It is recommended to use the linkSpeedInBits field in custom visualizations (instead of linkSpeed)

Deprecated Fields in Analytics

The following table lists the fields that will be deprecated in the future software versions. It is recommended to use the replaced fields instead.

Table 17:

Deprecated Field	Replaced Field
Ports	
portIdToClusterId	<i>resource.name</i>
portId	<i>resource.id.entityId</i>
clusterId	<i>resource.id.clusterId</i>
objectType	<i>resource.type</i>
alias	<i>resource.id.alias</i>
Maps	
clusterId	<i>resource.id.clusterId</i>
objectType	<i>resource.type</i>
alias	<i>resource.id.alias</i>

Deprecated Field	Replaced Field
Map Rule	
clusterId	<i>resource.id.clusterId</i>
objectType	<i>resoure.type</i>
alias	<i>resource.id.alias</i>

Analytics Appendix

The below section describes the Analytics components and the specific fields .

Ports

The below section lists the dimensions and metrics collected for Ports .

Dimensions

Fields	Description
hostname	The hostname of the device.
portType	The type of Port.
resource.name	This is a combination of cluster id and port Id (entity ID).
resource.type	This shows the type of statistics that is being analyzed.
resource.id.entityId	The Port Id.
resource.id.clusterId	The Cluster Id.

Metrics

The metrics is further categorized to Gauge Metrics and Counter Metrics

Gauge Metrics

For Rolled Up data the Gauge metrics stores average , maximum, minimum and sum value.

Fields	Description
port.tx.utilztn	The transmission packets total utilization.
port.tx.packetRps	The transmission packets by rate per second
port.tx.bitsRps	The transmission packet bits by rate per second.
port.rx.utilztn	The received packets total utilization.

Fields	Description
port.rx.sfpPowerMin	The minimum SFP power.
port.rx.sfpPowerMax	The maximum SFP power.
port.rx.bitsRps	The Received packet bits rate per second.

Counter Metrics

For Rolled Up data the counter metrics stores only maximum value.

Fields	Description
port.tx.packetDiscard	The transmission packets that were discarded.
port.tx.octets	The transmission octets that passed via port.
port.tx.packetErr	The transmission packets that encountered error at the port.
port.tx.packetDrop	The transmission packets that were dropped.
port.tx.packets	The transmission packets that were passed
port.rx.packetDiscard	The received packets that were discarded
port.rx.octets	The received octets that were passed
port.rx.packetErr	The received packets that encountered error at the port.
port.rx.packetDrop	The received packets that were dropped.
port.rx.packets	The total received packets.
linkSpeedInBits	The link speed of port in bits.

Maps

The below section lists the dimensions and metrics collected for Maps.

Dimensions

Fields	Description
cluster Id	The cluster Id of the device.
host	The host of the device
objectType	The type of statistics.
alias	The alias assigned to the map.
mapType	The type of map.
mapSubtype	The sub type of the map.
ruleOrder	The order in which the rule is configured.
resource.name	This is a combination of host, alias and rule order.
resource.type	The type of statistics.

Fields	Description
resource.id.deviceId	The device id.
resource.id.alias	The alias assigned to the map.
resource.id.entityId	The entity Id of the map.
resource.id.clusterId	The cluster Id of the map.
map.alias	The alias assigned to the map.

Metrics

The metrics is further categorized to Gauge Metrics and Counter Metrics . Here we have described the counter metrics.

Counter Metrics

For Rolled Up data the counter metrics stores only maximum value.

Fields	Fields
map.octets	The total octets processed
map.octets_rule_pass	The number of octets passing the rule.
map.octets_rule_drop	The number of octets dropped due to the rule.
map.packets	The total packets.
map.packets_rule_pass	The packets that passed the matching rule.
map.packets_rule_drop	The packets That were dropped due to not matching the rule.

Map Rule

The below section lists the dimensions and metrics collected for Map Rules.

Dimensions

Fields	Fields
clusterId	The cluster Id of the device.
host	The host name of the device.
objectType	The type of statistics.
alias	The alias assigned to the map rule.
ruleType	The type of map rule.
ruleUniqueld	The unique ID assigned to the map rule.
ruleOrder	The order of map rule.
resource.name	This is a combination cluster id, alias and rule order.

Fields	Fields
resource.type	The type of statistics.
resource.id.deviceId	The device Id.
resource.id.alias	The alias assigned to the map rule.
resource.id.entityId	The entity Id of the map rule.
resource.id.clusterId	The cluster Id of the device.
map.alias	The alias assigned to the map rule.
mapRule.ruleUniqueId	The unique ID assigned to the map rule.

Metrics

The metrics is further categorized to Gauge Metrics and Counter Metrics . Here we have described the counter metrics.

Counter Metrics

For Rolled Up data the counter metrics stores only maximum value.

Fields	Fields
mapRule.octets	The total octets processed through map rule.
mapRule.packets	The total packets processed through map rule.
mapRule.octets_rule_drop	The total octets dropped due to the map rule.
map.accepted	The total octets accepted.
mapRule.acceptedBytes	The total bytes accepted.
mapRule.acceptedPkts	The total packets accepted.
mapRule.matched	The total octets matched with map rule.
mapRule.matchedBytes	The total bytes matched with map rule.
mapRule.matchedPkts	The total packets matched with map rule.
mapRule.rejected	The total octets that were rejected due to not matching with map rule.
mapRule.rejectedPkts	Total packets rejected not matching rule.
mapRule.rejectedBytes	Total bytes rejected not matching rule.

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)