



GigaVUE Nodes and Clusters 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 Nodes and Clusters Guide	1
Change Notes	3
Contents	4
GV-Nodes-Clusters	10
GigaVUE Nodes and Clusters	10
GigaVUE® HC Series and TA Series Overview	11
Notes on TA Series Nodes	14
About Cluster	14
Overview of Seed Node	15
Manage GigaVUE® Nodes and Clusters	16
Configure Physical Nodes	17
Node Control Options	18
Add New Physical Node or Cluster to GigaVUE-FM	20
Add Nodes Manually	20
Add Nodes From an Excel Spreadsheet	22
Device Level Tagging	23
NAT Behind Nodes	24
Prerequisites	24
Add NAT Behind Nodes	24
Limitations	25
Cluster Discovery Behavior	25
ARP/NDP Timer Settings	25
Change the ARP/NDP Timer Settings	26
Enable Gratuitous ARP on Management Interface	27
SNMPv3 Support	27
Enable SNMPv3 on Nodes	28
Create and Manage Clusters	28
About Cluster	29
Cluster Node Limit	30
Cluster Scaling	31
Cluster Topologies	31

Separate Paths for Cluster Control and Stack Traffic	31
About Cluster Roles	33
Setting a Node's Priority in the Leader Election Process	33
About the "Unknown" Cluster Role	34
Sample Cluster Control Connections	35
Sample Cluster Control Configurations	35
Zeroconf for Cluster Management Ports	35
Keep Cluster Management Ports Connected!	35
Sample Stack-Link Configurations	36
Star Configuration	36
Daisy-Chain Configuration Using GigaStream for Stack-Link	37
Creating Clusters: A Roadmap	37
IPv6 Based Clustering	39
Rules, Notes, and Limitations	39
Create IPv6 based Cluster	40
Switch IPv4 based Cluster to IPv6 based Cluster	40
Rules and Recommendations for Nodes and Clusters	42
Using Command Line Interface for Managing Clusters	45
GigaVUE TA Series and GigaVUE-HC3 Clustering	
Recommendations	47
Cluster Rules	48
Best Practices for OOB Clusters with IGMP Snooping	48
About IGMP Snooping in a Cluster	49
Allow IGMP Traffic	49
Enable an IGMP Querier	50
E-Tag Clustering	50
Stacking Mode	51
Switching Stacking Mode	52
Notes	53
New 6.0	53
Cluster Safe and Limited Modes	54
Safe Mode	54
Limited Mode	55
Support for Cluster Types	55
Create Clusters	55
Regular Cluster Formation Workflow	56
Deployment Checklist	56

Create Regular Cluster Formation	56
Customize Stack Links	58
Edit a Cluster	60
Prerequisites	61
Delete a Node from a Cluster	62
How to Change the Leader Preference of a Device	63
Edit Cluster	63
Prerequisites:	64
Inband Cluster Management	65
Inband Cluster Management Topologies	65
Inband Cluster Management Stack Ports	66
Inband Cluster Management Stack Ports Example	66
Inband Cluster Management Configuration Flow Chart ...	67
Inband Cluster Management Configuration	69
Enable Cluster Management for GigaVUE TA Series	
Nodes	69
Add Nodes to a Cluster	69
Remove Nodes from a Cluster	70
Edit Cluster Parameters	71
Check Cluster Status	72
Cluster Management Events	72
Audit Logs	73
Export Nodes and Clusters	73
Problems with SCP?	74
Events	74
Alarms	75
Audit Logs	75
Search for Specific Nodes Using Keywords	75
Search for Ports on a GigaVUE Node	76
Overview Page	78
Systems Information	78
Failure to Authenticate	79

Ports Information	79
Traffic	80
Workflows	80
Overview of Workflows	80
How to Use Workflows	81
Chassis Table View	83
Live Graphing	83
Safe and Limited Modes	84
Safe Mode	85
Limited Mode	85
Enable SNMP Trap for Safe Mode and Limited Mode	86
Collect Information for Technical Support	87
Manage Not-reachable Nodes in Cluster	87
Rules, Notes, and Limitations	89
Remove Offline Chassis	89
Alarms and Health Status of Not-reachable Nodes	90
Upgrade Cluster with Not-reachable Nodes	91
Backup and Restore of Cluster with Not-reachable Nodes	92
Multi-Path Leaf and Spine	92
Introduction to Multi-Path Leaf and Spine	93
Path Protection	94
Leaf Node Failure	95
Restoration	95
Affected Time	95
Stack Link Failure on Leaf (TAP Connected)	95
Restoration	96
Affected Time	96
Spine Node Failure	96
Restoration	97
Affected Time	97
Stack Link Failure on Leaf (Tool Connected)	97
Configuration Overview	97
Notes and Considerations	99
Leaf-Spine Cluster Deployment	100
Deployment Checklist	100
Pre-deployment checklist	100

Formation Scenario	100
Leaf-Spine Cluster Formation Workflow	101
Create a Leaf-Spine Cluster	101
Cluster Configuration	103
Stack Links configuration	103
Edit a Cluster	105
Prerequisites	106
Delete a Node from a Cluster	108
How to Change the Leader Preference of a Device	109
Spine to Spine and Leaf	111
Introduction to Spine to Spine and Leaf	111
Configuration Overview	113
Configure Stack GigaStream	113
Configure Spine Links	114
Configure Stack Links	115
Notes and Considerations	115
Configuration of Spine to Spine and Leaf Architecture	115
Limitations	115
Leaf-Spine Cluster Deployment	116
Deployment Checklist	116
Documentation	116
Pre-deployment checklist	116
Formation Scenario	116
Fabric Statistics	117
About Fabric Statistics	117
Display Fabric Statistics for All Ports	118
Display Fabric Statistics for a Single Port	121
Port Quick View	121
Export Fabric Statistics	122
Filter Fabric Statistics	122
Clear Fabric Statistics Counters	124

Enable Discovery Protocols	124
Enable Gigamon Discovery on Chassis	125
Enable LLDP and CDP on Chassis	125
Enable LLDP, CDP, and Gigamon Discovery on Ports	126
Limitations of Discovery	127
Topology Visualization	127
Edit Topologies	134
Configure Network Devices	142
Configure Connections	144
Configure Tools	145
Flows	148
About Flows	149
View Flows	152
View the Flow Summary and Statistics	153
View Maps and Ports	156
View Total Ports	157
View Total Unhealthy Ports	157
View Total Maps	158
View Unhealthy Maps	158
Filter Flows	158
How to Change the Flow Layout	159
How to Update Flows	159
View Events	160
Set Notifications	160
Limitations of Flows	161
Device Logs and Event Notifications	161
Stream Device Logs to GigaVUE-FM	162
Cluster Behavior	162
Standardized Logs	162
Device Log Categories	163
Device Log Message Types	163
Device Logging Levels	164
Device Logging Processes	165

View Device Logs	166
Arrange Columns in the Logs View	168
VLAN Resources	169
Device Log Host Servers	170
Add an External Logging Host Server to a Node	170
Host Server Options	171
Edit Host Server Settings	172
Storage Management for Device Logs	173
Access Storage Management	173
Manage Device Log Output	174
Glossary	176

GV-Nodes-Clusters

GigaVUE Nodes and Clusters

This section describes how to configure, manage, and monitor GigaVUE nodes, clusters, and fabrics using GigaVUE-FM. It also includes information about supported deployment topologies, operational visibility, and troubleshooting data. Refer to the following sections:

- [GigaVUE® HC Series and TA Series Overview](#)
- [About Cluster](#)
- [Manage GigaVUE® Nodes and Clusters](#)
- [Multi-Path Leaf and Spine](#)
- [Spine to Spine and Leaf](#)
- [Fabric Statistics](#)
- [Topology Visualization](#)
- [Flows](#)
- [Device Logs and Event Notifications](#)

NOTE: For device backup/restore details refer to the *GigaVUE Administration Guide*.

GigaVUE® HC Series and TA Series Overview

The GigaVUE HC Series delivers performance and intelligence in each of its Deep Observability Pipeline nodes, with port density and speeds that scale to your needs, from 1Gb to 100Gb. With an intuitive Web-based interface (GigaVUE-FM) and a powerful GigaVUE-OS, the Deep Observability Pipeline is able to replicate, filter, and selectively forward network traffic to monitoring, management, and security tools.

The GigaVUE HC Series and GigaVUE TA Series include the following models that run GigaVUE-OS:

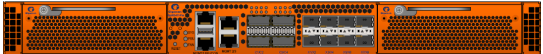
- GigaVUE-HC1
- GigaVUE-HC3
- GigaVUE-HC1-Plus
- GigaVUE-HCT
- GigaVUE-TA25
- GigaVUE-TA25E
- GigaVUE-TA100
- GigaVUE-TA200
- GigaVUE-TA200E
- GigaVUE-TA400
- GigaVUE-TA400E

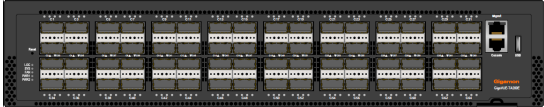
NOTE: This document describes how to configure and operate the GigaVUE-OS for GigaVUE HC Series and GigaVUE TA Series nodes.

GigaVUE-HC1

- 1RU Footprint
- Two Module Slots (Bays)
- Dedicated Cluster Management Port
- Supports all GigaVUE-HC1 Modules
- Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes
- All ports, excluding BPS ports, of same type and speed can be used to create GigaStream.



GigaVUE-HC3	• 3RU Footprint • Four Module Slots (Bays) • Internal Control Card • Extension Board • Dedicated Cluster Management Port • Supports all GigaVUE-HC3 Modules • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes. • All ports, excluding BPS ports, of same type and speed can be used to create GigaStream.	
GigaVUE-HC1-Plus	• 1RU Footprint • Two Module Slots (Bays) and one Fixed Base Module • 4 x 100Gb / 40Gb, 8 x 25Gb, 10Gb, 1Gb connectivity • Supports GigaSMART applications with a fixed rear GigaSMART Module. • Supports Flex Inline in unprotected ports with 10Gb/40Gb/25Gb/100Gb/4 x 10Gb/4x25Gb speed Nodes. • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes • All ports, excluding BPS ports, of same type and speed can be used to create GigaStream.	
GigaVUE-HCT	• 1RU and half rack width system • One Module Slot (Bay) and one Fixed Base Module • 2 x 100Gb/40G bconnectivity • Supports Flex Inline in unprotected ports with 40Gb/100Gb/4x10G/4x25G speed Nodes. • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes • All ports, excluding BPS ports, of the same type and speed can be used to create GigaStream.	

GigaVUE-TA25	• 1 RU Footprint • 1Gb/10Gb/48 x 25Gb/ ports and 8 x 100Gb/40Gb ports, dual hot-pluggable power supplies (AC/DC), four rear hot swappable fan modules, two console ports, and a 10Mb/100Mb/1Gb management port • Optional patch or breakout panel support • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes	
GigaVUE-TA25E	• 1 RU Footprint • 48 x 25Gb/10Gb/1Gb ports and 8 x 100Gb/40Gb port, dual hot-pluggable power supplies (AC/DC), four rear hot swappable fan modules, two console ports, and a 10Mb/100Mb/1Gb management port • Optional patch or breakout panel support • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes.	
GigaVUE-TA100	• 1RU Footprint • 32 x 100Gb/40Gb ports, hot swappable fan modules • Optional patch or breakout panel support • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes.	
GigaVUE-TA200	• 2RU Footprint • 64 x 100Gb/40Gb ports, hot swappable fan modules • Optional patch or breakout panel support • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes.	
GigaVUE-TA200E	• 2RU Footprint • 64 x QSFP28 ports (40G/100G), dual power supply modules (AC/DC) and hot swappable fan modules • UART RS232 Console port (RJ45) and Management port (RJ45).	

GigaVUE-TA400	• 1RU Footprint • 32 x 400Gb /100Gb/ 40Gb QSFP-DD/ QSFP28/QSFP+ ports, dual hot-pluggable power supplies (AC/DC), seven rear hot swappable fan modules, console port and a 10M/100M/1G management port. • Cluster with GigaVUE HC Series and GigaVUE TA Series Nodes.	
GigaVUE-TA400E	▪ 2RU Footprint ▪ 32 40Gb/100Gb/400Gb QSFP-DD/ QSFP28/QSFP+ ports, dual hot-pluggable power supplies (AC/DC), six hot-swappable fan modules, console port and a 10M/100M/1G management port. ▪ Breakout panel support ▪ Console port (RJ45) and Management port (RJ45). ▪ In addition provides 2 x 10Gb/1Gb SFP+/SFP ports ▪ Cluster with GigaVUE HC Series nodes and GigaVUE TA Series Nodes.	

Notes on TA Series Nodes

- On the GigaVUE-TA100, only the first 16 out of 32 100Gb ports are enabled. Two port licenses are available to enable an additional 8 or 16 ports to expand from 16 ports to 24 ports or from 16 ports to 24 ports and then to 32 ports.
- The ports on the GigaVUE-TA100 can be used as network, tool, or hybrid ports.
- For more information about the GigaVUE TA Series nodes, refer to the *GigaVUE TA Series Hardware Installation Guide*.

For adding a physical node to GigaVUE-FM, refer to [Configure Physical Nodes](#).

About Cluster

You can use GigaVUE-FM to create a cluster. Cluster is created from standalone nodes that are currently managed by GigaVUE-FM. The type of cluster that can be created in this software version is out-of-band.

Any GigaVUE® HC Series and GigaVUE® TA Series nodes can be a part of a cluster. However, a GigaVUE® TA Series node cannot be a leader. It can only join a cluster with other GigaVUE HC Series nodes.

In addition to creating a new cluster, you can also manage an existing cluster through GigaVUE-FM. You can add nodes to an existing cluster and remove nodes from an existing cluster.

When a new cluster is created, the nodes joining the cluster must be standalone nodes. If a node is initially part of another cluster, it must be removed from that cluster so that it becomes a standalone node, before it can be added to the new cluster.

Refer to the following notes and considerations for all nodes in a cluster:

- must be currently managed by GigaVUE-FM
- must be running software version 5.1.00, at a minimum
- must be running the same software version and build version
- must be reachable by GigaVUE-FM, that is, it must be online and not have any authentication failures
- GigaVUE TA Series nodes that need an Advanced Features License, must be licensed
- member nodes joining the cluster must have preference less than the leader node
- From GigaVUE-FM 5.7 and above , a node which is prior 5.4.00 will show its installed "Cluster License" as "Advanced Features License".

For information on clustering concepts, refer to [Manage GigaVUE® Nodes and Clusters](#).

Overview of Seed Node

The seed node concept in GigaVUE-FM is different from the cluster leader role.

When a cluster is created, one of the nodes that you have selected for inclusion in the cluster will be deemed as the seed node. The seed node will be used to start the formation of a cluster and will be determined by the cluster leader preference settings of the nodes selected for the cluster.

You can override the seed node selected by GigaVUE-FM. However, the seed node must be a node that has the ability to become the leader.

Initially, the seed node is the source of the configuration information for the other nodes in the cluster. However, the cluster still consists of a leader, a standby node, as well as

normal nodes. With the addition of more nodes to the cluster, a new cluster leader may be desired. If the desired leader is different from the seed node, the leader will then become the source of the configuration information for the other nodes in the cluster.

For creating and managing clusters using GigaVUE-FM, refer to [Create and Manage Clusters](#).

Manage GigaVUE® Nodes and Clusters

This section describes how to add and manage GigaVUE® HC Series and GigaVUE® TA Series nodes on a GigaVUE-FM:

- [Configure Physical Nodes](#) describes the process to add, configure and manage GigaVUE nodes through GigaVUE-FM.
- [Create and Manage Clusters](#) describes the process to create a cluster using the wizard, add nodes to a cluster, remove nodes from a cluster, edit cluster parameters, and add stack links.
- [Upgrade Software on a GigaVUE Node or a Cluster from GigaVUE-FM](#) describes the process to upgrade standalone nodes and clusters through GigaVUE-FM.
- [Search for Specific Nodes Using Keywords](#) provides information about each of the standalone nodes and clusters, including a visual indication of each nodes status.
- [Overview Page](#) provides the information on each node connected to the GigaVUE-FM. This section covers the following: [Systems Information](#), [Ports Information](#), and [Traffic](#).
- [Workflows](#) describes how to use the workflow wizards to create four different types of maps. With the wizards, you can create the following types of maps:
 - Out-of-band maps
 - Inline maps
 - Basic out-of-band GigaSMART maps
 - Advanced out-of-band GigaSMART maps
- [Chassis Table View](#) describes the Chassis Table View when managing a node with GigaVUE-FM.
- [Safe and Limited Modes](#) describes Safe Mode and Limited Mode.
- IPv6 based Clustering Support
- [Rules and Recommendations for Nodes and Clusters](#)

Topics:

Configure Physical Nodes

The Physical Nodes page displays a list of physical nodes and clusters. It provides information about a device's cluster ID, role, model, connection status, device status, and many other details.

To access physical nodes attached to an instance of GigaVUE-FM, log into GigaVUE-FM. On the left navigation pane, go to **Inventory**  and under **Physical**, select **Nodes** to view all the physical nodes and clusters managed by GigaVUE-FM.

The Physical Nodes page displays the following information:

Field	Description
Cluster Id	The name of the cluster.
Host Name	The host name of the box.
Task Status	The status of the upgrade process. When the upgrade process is in progress, the task status displays the number of steps completed successfully out of the total number of steps to be completed. For example, upgrade: step (2/5) Image Fetch Complete. Once the upgrade process is complete, the upgrade status is displayed as Upgrade Success or Upgrade Failure. Note: To clear the task status of the upgrade process, select the required cluster IDs and choose Actions > Clear Task status option.
Node Address	The IP address of the physical node. Note: When assigning an IP address to a device using DHCP, the IP address may change after a reload or device upgrade, resulting in lost connectivity. Previous entries are retained in the node, and stale entries are retained in the GigaVUE-FM database even though the configuration has been deleted from the GigaVUE-FM end. To resolve this issue, Map the IP address to the Mac address of the node in the DHCP server so that GigaVUE-FM won't end up in this state due to the IP address change.
Role	The role of the node in the cluster. The role of the node can be one of Leader, Standalone, Member, or Standby.
Model	The type of the GigaVUE HC Series model.
Box Id	The box Identifier of the node.
Serial Number	Serial number of the device.
SW Version	The version number of GigaVUE-FM.
Licensed	The status of the physical node or Advanced Features license.

Field	Description
Attempted Sync Time	The time and date when the physical node attempted synchronizing with GigaVUE-FM.
Successful Sync Time	The time and date when the physical node was last synchronized with GigaVUE-FM.
Health	The current health status of the GigaVUE node or cluster. To know about how the device health status is computed, refer to Node Health Status. Note: You can monitor the health status of the device by enabling the SNMP notifications. For more information on configuring the email notifications, refer to the “Notifications” section in the <i>GigaVUE Administration Guide</i>.
Alarm	Alarm triggered by the device.
Tag	The tag or site name and value associated to the physical node or cluster. The tag names associated to the physical node or cluster are displayed as separate columns. Under the tag or site name, the respective tag or site value is displayed.
Uboot Version	Uboot version of the device.

NOTE: The columns in the Physical Nodes page can be customized based on the type of content you want to view in the table. For customizing the columns, refer to [Table View Customization](#).

Changes made to the cluster through the CLI are reflected in GigaVUE-FM when it synchronizes with the cluster, which is typically every 5 minutes.

If the latest configuration data is not retrieved from the cluster for more than 30 minutes, a warning is displayed in the cluster Overview page indicating the last time GigaVUE-FM successfully synchronized with the cluster.

To view the last synchronized status, click the cluster and view the status at the top of the Overview page.

Node Control Options

Use the following buttons in the Nodes page to perform specific actions:

Button	Description	Reference
Tags	The Tags drop-down menu button allows	Refer to the Tags section in the <i>GigaVUE</i>

Button	Description	Reference
	you to perform the following actions: • Add: Use to Add tags to standalone nodes and clusters. • Delete: Use to Remove tags from standalone nodes and clusters • Device Level Tagging: Use to associate tags to devices. Refer to the Device Level Tagging section for more details. • Export Tags for Selected: Use to Export tags for the selected nodes. • Export Tag Resources for Selected: Use to Export tag resources for the selected nodes. Note: To create tags you must be a fm_super_admin user.	<i>Administration Guide</i> for details on how to create, edit, delete tags.
Actions	The Actions drop-down menu option allows you to perform the following actions:	
	• Edit: Use to Edit the selected standalone node or cluster.	
	• Image Upgrade: Use to upgrade the image for the selected node or cluster.	Refer to Upgrade Software on a GigaVUE Node or a Cluster from GigaVUE-FM
	• Backup: Use to backup the nodes and cluster. • Restore: Use to restore the nodes and cluster.	Refer to the "Backup and Restore section for more details.
	• Reboot: Use to reboot the nodes and cluster.	Refer to the Reboot the Nodes section for more details.
	• Suppress Alarms: Use to suppress alarms. • Stop Alarm Suppression: Use to stop suppression of alarms.	Refer to Suppressed Alarms section for more details.
	• Clear Task Status: Use to clear the Task status.	Refer to Admin Tasks for more details.
	• Rediscover: Use to rediscover the node.	
	• Disconnect Node: Use to disconnect	

Button	Description	Reference
	the node from GigaVUE-FM.	
Filter	The Filter button allows you to filter the nodes.	
Create Cluster	Use to Create Cluster .	Refer to Create and Manage Clusters section for more details.
Add	Use to Add a physical node to GigaVUE-FM.	Refer to Add New Physical Node or Cluster to GigaVUE-FM .
Delete	Use to Delete a node from GigaVUE-FM.	
Import	Use to Import nodes to GigaVUE-FM.	Refer to Add Nodes From an Excel Spreadsheet section for more details.
Export	Use to Export the nodes from GigaVUE-FM.	Refer to Export Nodes and Clusters section for more details.

Add New Physical Node or Cluster to GigaVUE-FM

You can add physical nodes and clusters to GigaVUE-FM either manually or by importing an Excel spreadsheet. However, before adding a new physical node, ensure that the node credentials are added under the **System > Node Details**.

The node credentials (username/password) used to add a node in GigaVUE-FM must be configured in the node and must have the necessary privileges for read and write operation. If you add a node with read-only privileges, it will impact the device operations performed from GigaVUE-FM.

NOTE: In a cluster configuration, the Normal nodes are seen as Member nodes in GigaVUE-FM.

Add Nodes Manually

To add physical nodes manually, do the following:

1. On the left navigation pane, go to **Inventory**  and select **Physical**.
2. On the Physical Nodes page, click **Add**. The Add Physical Node page displays.
3. Select **Add Manually**.

4. Enter or select the information as shown in the following table:

Field	Description
Node	DNS name or IP address of the node. Click + to add additional nodes or - to remove a node. Note: You must add the nodes by their FQDN or hostname rather than IP, especially in case of NAT nodes. This ensures that GigaVUE-FM and device communication is not interrupted when there is a change in the IP address of the node. When adding clusters, use the VIP of the cluster to add. If VIP is not configured, they you must add the leaders FQDN or IP, which is the primary address of the cluster. Port The HTTPS port number of the device, if it has been changed using CLI. Note: If you do not provide the HTTPS port number, then the default value 443 will be used for device communication.
Secondary IP Address	IP address (nodeAddress) of the node that is used to connect to the cluster, in case the primary IP address is not reachable. This node will be the one which becomes the leader if the leader fails. Note: Secondary IP address is applicable only for clusters configured without VIP. You cannot add a secondary IP address for standalone nodes. You can edit an existing cluster and add the secondary IP address. In case both the primary and the secondary IP address is not reachable the cluster is marked as unreachable.
Custom Login Credentials	Check box to enable custom login credentials. If enabled enter the following details: - User Name - Password
SNMP Version	The SNMP version to be used to register GigaVUE-FM as a SNMP target on the node.
Node behind NAT	Check box to indicate if the node being added is behind NAT. Refer to Add NAT Behind Nodes for details.
Tags	Select the tag key and the tag value to which the node must be associated to. Note: You can only view tags that are permitted for your role. Refer to the "Tags" section in the <i>GigaVUE Administration Guide</i> for more details.

- Click **Submit** to add the node or nodes to the list of physical nodes GigaVUE-FM is managing.

For standalone nodes, both node IP (Device IP) and cluster ID is the node Address (nodeAddress) provided by the user while adding the node.

NOTE: In GigaVUE-FM version 5.5.01, the Node IP was the actual IP and the Cluster ID was either the DNS ID (if the IP address was resolved) or the Node IP (if the IP address was not resolved).

Add Nodes From an Excel Spreadsheet

You can add nodes to GigaVUE-FM by uploading an Excel spreadsheet that contains a list of the physical nodes that you want GigaVUE-FM to manage. You can create the spreadsheet or use a spreadsheet from a previous export of the nodes. From GigaVUE-FM 6.7 release onwards, the format of the spreadsheet must have at least a column with the node addresses and a separate column for the HTTPS port number (if the port number of the node has been changed using CLI) and the header Node Address.



- If you do not provide the HTTPS port number in the Excel spreadsheet, then the default value 443 will be used for device communication.
- For software version greater than 5.11.00, Node_IP should be changed to Node Address to avoid any errors while importing nodes using Excel spreadsheet.

Host Name	Node Address	Model	Box Id	HTTPS Port Number	Serial Number	SW Version	Licensed	Attempted Sync Time	Successful Sync Time	Alarms
gigamon-a0fa62	10.114.34.113	HC1	1	443	HFA62	6.7.00	Yes	2024-06-20 11:23:12	2024-06-20 11:23:12	0
gigamon-a046fc	10.114.34.196	HC3	7	443	J46FC	6.1.00	Yes	2024-06-20 11:23:12	2024-06-20 11:23:12	0
MSWMNAJ9C01339	10.114.84.141	HC3	2	443	JBEE9	6.5.00	Yes	2024-06-20 11:23:11	2024-06-20 11:23:11	2
gigamon-951a34	10.114.178.10	HC3	3	443	J1A34	6.7.00_Beta	Yes	2024-06-20 11:23:10		0
gigamon-a0cd12	dev1.fmttest.lab	HC3	4	8443	JCD12	6.6.00	Yes	2024-06-20 11:23:11	2024-06-20 11:23:11	0
gigamon-a08802	10.114.43.207	HC1	7	443	H8802	6.6.00	Yes	2024-06-20 11:23:14	2024-06-20 11:23:14	0
gigamon-a00e52	10.114.43.79	HC3	4	443	J0E52	6.6.00	Yes	2024-06-20 11:23:14	2024-06-20 11:23:14	0
gigamon-a0e448	10.114.42.213	HC1	3	443	HE449	6.6.00	Yes	2024-06-20 11:23:14	2024-06-20 11:23:14	0

Figure 1 Node List Spreadsheet for Import/Export

NOTE: The format of the spreadsheet is changed in GigaVUE-FM 6.7. To import a spreadsheet created by GigaVUE-FM prior to GigaVUE-FM 6.7, you can modify the previous spreadsheet or do a new export after upgrading to the current version of GigaVUE-FM. An example of a spreadsheet is shown in the figure.

You can also import nodes to GigaVUE-FM by uploading an Excel spreadsheet that contains only the Node Address, username, and password of the nodes that you want to import. An example of such spreadsheet is shown below:

Cluster ID	username	password
10.114.34.113	admin	admin123A!!

To add physical nodes by importing from a spreadsheet, do the following:

1. On the left navigation pane, go to **Inventory**  select **Physical** .
2. On the Physical Nodes page, click **Import**.
The Add Physical Node page displays with the **Import from Excel** option automatically selected. The page displays an area for selecting or dragging and dropping a file.
3. Drop an Excel file onto the page or click **Select File** to upload the file.
The page displays the list of IP address.
4. Select the nodes to add to GigaVUE-FM.
5. Click Submit to add the node or nodes to the list of Physical Nodes GigaVUE-FM is managing.

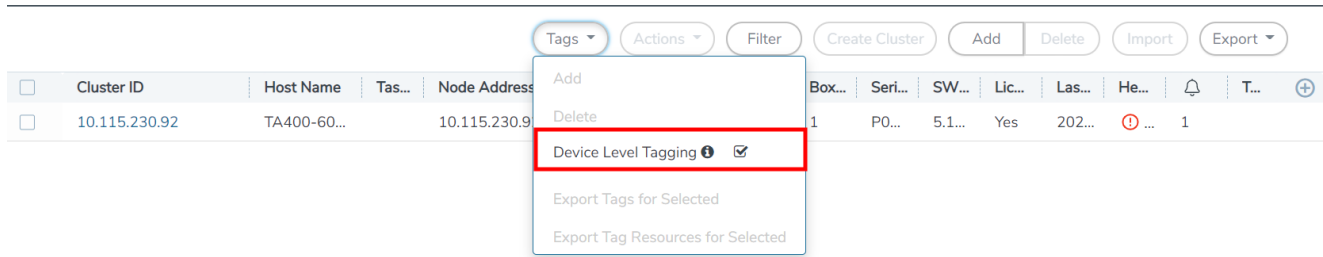
NOTE: If the nodes/clusters that are being imported in to GigaVUE-FM are associated to tags, you must ensure to add the tags to that GigaVUE-FM instance before importing the nodes. Otherwise, the nodes will not be associated to the tags. Refer to the GigaVUE Administration Guide for more details.

Device Level Tagging

Each of the individual nodes in a cluster can be associated with a tag key and a tag value. To assign a tag key to a device:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Click on **Tags** and enable the **Device Level Tagging** option.
3. Select the required node(s). Click **Tags** and select **Add**. The **Add Tags to Resources** page appears.
4. Select the required tag key and the tag value to which the nodes must be tagged.
5. Click **OK**.

NOTE: Only aggregation tags can be configured to the devices.



The nodes in a cluster are now associated to tags which can be used for creating the required topology.

NAT Behind Nodes

GigaVUE-FM can manage nodes and clusters that use Network Address Translation (NAT) for IP address conversion. GigaVUE-FM identifies the nodes behind NAT based on the **Node Behind NAT** option which you must select at the time of adding the nodes. Refer to [Add Nodes Manually](#).

Prerequisites

In order for GigaVUE-FM to manage the devices and clusters that are behind NAT:

- GigaVUE-FM must be running software version 5.7 or higher.
- Devices must be running software version 5.3 or higher.
- Devices must be assigned NAT IP and Fully Qualified Domain Names.
- Domain name server and default search domain must be configured in GigaVUE-FM.

Add NAT Behind Nodes

When managing clusters behind NAT, GigaVUE-FM does not know the NAT IP of the members in the cluster. You cannot also configure the NAT IP of the members. GigaVUE-FM only identifies the private IP of the nodes through the API. Therefore, for device specific operation, GigaVUE-FM uses host names to connect to the nodes. You must therefore configure the domain name server and default search domain in GigaVUE-FM. Refer to the “*NAT Configuration*” section in the *GigaVUE Administration Guide*. If you do not configure the domain name server and search domains, then it may lead to failure in node specific operations.

NOTE: When adding nodes, ensure the following:

- Select the **Node behind NAT** option for a node that is behind NAT.

- Do not select the **Node behind NAT** option for a normal node.

If you fail to perform the above operations, then you may experience inconsistency in managing the nodes.

Refer to the “*NAT Configuration*” section in the *GigaVUE Administration Guide* for details.

Limitations

Though GigaVUE-FM can manage nodes behind NAT from software version 5.3, SNMP traps, Syslog messages and event notifications will not be pushed from the node to GigaVUE-FM. This is because GigaVUE-FM registers its eth0 address as target address on the nodes to receive the notifications but the nodes behind NAT will not be able to reach GigaVUE-FM by its eth0 IP. These limitations are not applicable for node version 5.7 and above.

NOTE: Refer to the “*NAT Configuration*” section in the *GigaVUE Administration Guide* for details.

Cluster Discovery Behavior

GigaVUE-FM does not detect individual nodes that were part of a cluster, if the cluster was dismantled using the CLI. GigaVUE-FM always reaches the cluster by its virtual IP address (if configured). When a cluster is dismantled through the CLI, the virtual IP address of the cluster will no longer be available and the cluster is therefore marked as unreachable. There is no change in detecting node additions, removals, or membership changes performed from CLI. Refer to the [Rules and Recommendations for Nodes and Clusters](#) for details on Cluster Configuration through CLI.

Note: When you reboot a device in cluster , the device status appears as **Green** ,whereas the connection status of the device appears as **Connection Failed**, and the role of the device appears as **Standalone**. In the subsequent discovery cycle , the rebooted devices appear in the cluster with their **Role, Device Status** ,and **Connection Status**.

ARP/NDP Timer Settings

The Address Resolution Protocol (ARP) or the Neighbor Discovery Protocol (NDP) timer specifies the aging time on the IP interface. The ARP timer is used for IPv4 addresses and the NDP timer is used for IPv6 addresses. The timer is configurable from 3 to 30 seconds. The default is 30 seconds. When an IP interface is configured, ARP/NDP requests are sent to the IP interface to find the gateway MAC address. When Tunnel encapsulation GSOP

Map is configured with destination tool in local network, ARP/NDP requests are sent to the IP interface to find the tool MAC address. In response, the gateway sends an ARP/NDP reply. The control card tries to match the IP address of the IP interface with the IP address of the ARP/NDP message received. If a match is found, the ARP/NDP status changes to resolved (otherwise the ARP/NDP status is not resolved).

Once the ARP/NDP status is resolved, the ARP/NDP timer of the IP interface controls the interval at which an ARP/NDP request is sent to the gateway to detect if the gateway is reachable or not. Above is applicable to detect tool's reachability part of local network that are configured as part of tunnel encapsulation GSOP Map.

You must enable the IP Gateway Status SNMP trap to send SNMP notifications when the ARP/NDP status changes. To enable SNMP notifications, refer to [Enable or Disable Events for SNMP Notifications](#).

Change the ARP/NDP Timer Settings

The default ARP/NDP timer value is 30 seconds. To change the timer setting at the node-level:

1. On the left navigation pane, go to **Inventory**  select **Nodes**.
2. In the Physical Nodes page, select the node for which you want to change the ARP/NDP timer setting.
3. Go to **Settings > Global Settings > ARP/NDP**.
4. Click **Settings**.
5. In the ARP/NDP Settings page, choose the required **ARP Refresh Time Interval** or the **NDP Refresh Time Interval** in seconds.
6. Click **OK**.

The ARP Entries table and the IPv6 Neighbor Entries table dynamically refresh to display information such as the IP address and Hardware address mapping, aging, state, and interface details.

Click **Clear > Clear ARP Entries** or **Clear > Clear IPv6 Neighbor Entries** to remove the entries from the tables.

Enable Gratuitous ARP on Management Interface

A Gratuitous ARP is an Address Resolution Protocol response that is sent without an ARP request. The Gratuitous ARP response is sent as a broadcast in the network. It is a mechanism by which a device can announce or update its IP address to MAC address mapping. This helps the neighboring devices to discover the device that has sent the Gratuitous ARP response and forward subsequent packets to the device without any delay.

You can enable the Gratuitous ARP on the management interface of a GigaVUE HC Series or GigaVUE TA Series device. Ensure that the management interface is configured with static IP address. A Gratuitous ARP response is sent to the network when:

- the device boots up.
- the IP address of the device changes.
- the link state of the management interface comes up.

NOTE: You cannot enable Gratuitous ARP on the management interface that is configured with DHCP.

To enable Gratuitous ARP on a management interface:

1. On the left navigation pane, go to **Inventory**  and select **Nodes**.
2. Click on a node on which you want to enable Gratuitous ARP. The Overview page of the node appears.
3. In the left navigation pane, select **Settings > Interface > Protocol Configuration**.
4. Select the box ID on which you want to enable Gratuitous ARP, and then click **Edit**.
5. Select the **Gratuitous ARP** check box.
6. Click **Apply**. The Gratuitous ARP is enabled on the management interface of the device.

SNMPv3 Support

Starting with software version 5.4 GigaVUE-FM creates an SNMPv3 user during the upgrade process from version 5.3. The SNMPv3 user is created with same authentication and privacy settings previous held.

NOTE: SNMPv3 support is only available on GigaVUE-FM software version 5.4 user and SNMPv3 users created by GigaVUE-FM cannot be modified by users.

Enable SNMPv3 on Nodes

You can enable SNMPv3 from the node addition page, If node version 5.4 or higher and SNMPv3 is selected, the GigaVUE-FM registers itself as a SNMPv3 trap receiver. If the SNMPv3 is chosen and the node version is 5.3 or below then, FM registers itself as a SNMPv2 trap receiver. When this occurs GigaVUE-FM reports an event that GigaVUE-FM does not support SNMPv3 on the node with 5.3 or lesser version.

Enabling SNMPv3 During Upgrade

1. Go to **Settings** and select **System> Credentials**. The Credentials page displays a listing of the nodes and SNMP versions.
2. Select a node to upgrade, and click **Edit**.
3. Select SNMP version - SMNPv3
4. Click **Save**.

Enabling SNMPv3 on a New Node

1. Select **Physical>Nodes> Add**. The Add Physical Node displays.
2. Enter **Node Name**.
3. Click **Enable**.
4. Enter **Username** and **Password**.
5. SNMP Version: SNMPv3.
6. Click **Submit**.

Create and Manage Clusters

This section describes the GigaVUE-FM clustering. Refer to the following sections for details:

- [About Cluster](#)
- [Create Clusters](#)
- [Support for Cluster Types](#)
- [Regular Cluster Formation Workflow](#)
- [Edit Cluster](#)
- [Add Nodes to a Cluster](#)
- [Remove Nodes from a Cluster](#)
- [Edit Cluster Parameters](#)

- [Check Cluster Status](#)

About Cluster

A cluster consists of multiple GigaVUE-OS nodes operating as a unified fabric such that packets entering the cluster on one node can be sent to a destination port on any other node. You set up packet distribution using the standard box ID/slot ID/port ID format, allowing maps to distribute traffic to any port in the cluster.

The following figure illustrates a sample cluster of GigaVUE-OS nodes.

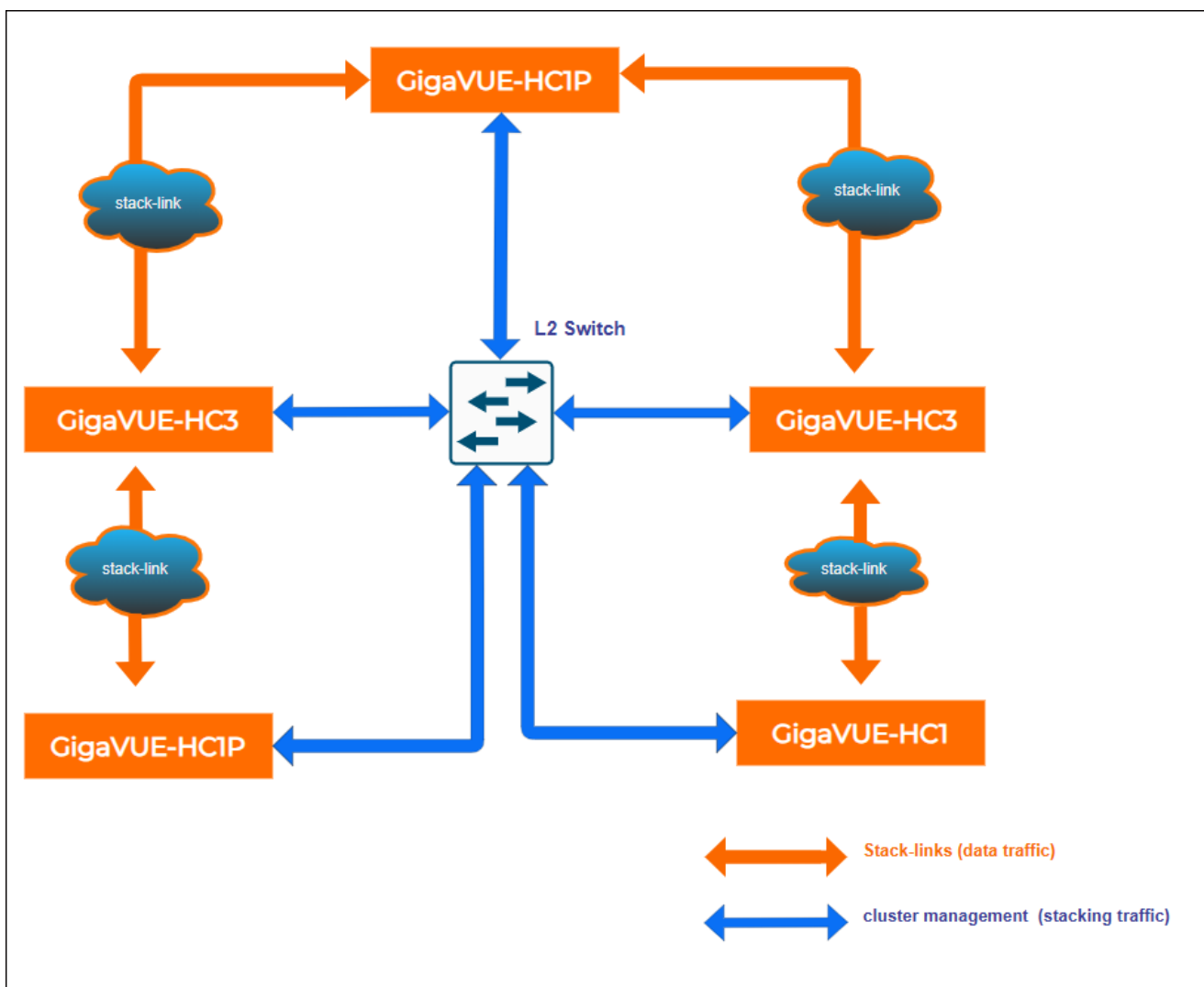


Figure 2 Sample Cluster

Cluster Node Limit

Any GigaVUE-OS nodes can join other nodes in a cluster. The GigaVUE-HC1, GigaVUE-HC3, and GigaVUE TA Series nodes, including Certified Traffic Aggregation White Box (white box), can be included in the same cluster. Starting in software version 4.5, the maximum number of nodes supported in a cluster is 32. For details, refer to [Cluster Scaling](#).

In addition, there is another independent limit, which is for the maximum number of line cards supported in a cluster, across all of the nodes in the cluster. This limit is determined by cost units. Cost units are based on the total number of line cards, line card types, and chassis type. Cost units measure the resources that a node needs in a cluster. The higher the cost unit, the more resources are needed to manage the node.

The following table has examples of line card and chassis types, and their cost units.

Line Card Type or Chassis	Cost Unit
GigaVUE-HC1-Plus	1
GigaVUE-HCT	1
GigaVUE-HC1 Chassis	1
GigaVUE-HC3 Chassis	1
GigaVUE-HC3 Chassis with Control Card version 2 (HC3 CCv2)	1
GigaVUE-TA25	1
GigaVUE-TA25E	1
GigaVUE-TA100	1
GigaVUE-TA200	1
GigaVUE-TA200E	1
GigaVUE-TA400	1
Certified Traffic Aggregation White Box	1

For example, if a GigaVUE-HC3 has one PRT-HC3-C08Q16 line card, one SMT-HC3-C05 GigaSMART line card, and one BPS-HC3-Q35F2G + PRT-HC3-X24 line cards, the cost units are $4 + 1 = 5$.

The cost unit maximum for the various nodes in the cluster is 255.

Therefore, the largest cluster supported is determined either by the maximum number of nodes (32) or by the cost unit maximum, whichever is reached first.

Cluster Scaling

The maximum number of nodes and map rules supported in a cluster is as follows:

Table 1: Maximum Number of Nodes and Map Rules Supported in a Cluster

When a Cluster is Configured with:	Number of Nodes	Maximum Map Rules
Out-of-Band Cluster Management	32	38000
Inband Cluster Management	16	38000

The maximum number of map rules supported in a cluster apply to all nodes in the cluster including GigaVUE® HC Series nodes: GigaVUE-HC3, GigaVUE-HC1, and GigaVUE TA Series nodes: GigaVUE-TA100, and GigaVUE-TA200.

Cluster Topologies

The following cluster topologies are supported:

- Star
- Daisy-chain
- Tree

Separate Paths for Cluster Control and Stack Traffic

There are two types of clustering: out-of-band and inband.

The nodes in a cluster are constantly communicating with one another, exchanging heartbeats to check on one another's status, exchanging configuration information so that changes made on the leader are propagated to other nodes, and making changes to cluster roles based on changes in status.

GigaVUE-OS separates cluster control traffic from the actual flow of packets from ingress ports on one node to egress ports on another for the two types of clustering, as follows:

Feature	Description
Out-of-Band Clustering on Mgmt Ports	With out-of-band clustering, cluster control traffic is carried out-of-band on its own network as follows: • GigaVUE-HC3 nodes use the Mgmt port (eth0) . • GigaVUE-HC1 nodes use the Mgmt port (eth0). • GigaVUE-HC1-Plus nodes use the Mgmt port (eth0). • GigaVUE-HCT nodes use the Mgmt port (eth0). • GigaVUE-TA25 nodes use the Mgmt port (eth0). • GigaVUE-TA25E nodes use the Mgmt port (eth0). • GigaVUE-TA100 nodes use the Mgmt port (eth0). • GigaVUE-TA200 nodes use the Mgmt port (eth0). • GigaVUE-TA200E nodes use the Mgmt port (eth0). • GigaVUE-TA400 nodes use the Mgmt port (eth0). Cluster Management port(s). Using the cluster management port(s) lets you route cluster control traffic over a separate network from the network used to access the Mgmt port. This prevents cluster control traffic from overloading the traffic used to access the Mgmt port. Mgmt Port (eth0). You can also select to use the standard Mgmt port for cluster control traffic. In this implementation, cluster control traffic uses the Mgmt port's Ethernet connection.
Inband Clustering on Stack-Links	Stack-links are used to create a stacking connection between two GigaVUE nodes in a cluster. Stack-links carry traffic from network ports on one node to tool (or GigaSMART) ports on a destination node. With inband clustering, cluster control traffic is carried inband through the stack-link. Stack-links can be constructed out of individual stack ports, for example, a 40Gb port on a PRT-HC0-Q06 or stack GigaStream. You decide which to use with the gigastream and ports arguments in the stack-link command. For example, the following command creates a stack-link between the q1 40Gb port on box 1/slot 1 and the q1 port on box 2/slot 7: (config) #stack-link alias biglink between ports 1/1/q1 and 2/7/q1 comment "40Gb Stack" Stack links are supported at speeds of 10Gb, 40Gb, and 100Gb. Refer to the <i>Hardware Installation Guide</i> for each GigaVUE node for information on stack link support. Keep in mind that because of the 10Gb port density offered by GigaVUE-OS nodes, using only one 10Gb port for a stack-link could cause a serious bottleneck. A stack GigaStream dramatically increases the bandwidth available for stack-links, letting you connect GigaVUE-OS nodes in a cluster and still take advantage of the 10Gb port density. Alternatively, nodes with 40Gb or 100Gb ports can take advantage of their high bandwidth for stack-links. When using stack GigaStream for stack-links, you must create a stack GigaStream on each side of the stack-link and each side must consist of the same number of ports running at the same speed.

About Cluster Roles

Communication with a GigaVUE-OS cluster is accomplished using a leader virtual IP address assigned to the cluster as a whole. Physically, the virtual IP address resolves to only a single leader at any one time. However, the leader role on the GigaVUE-OS node is not statically assigned to a single node. Instead, any node (except GigaVUE TA Series and the nodes residing on a different management subnet) in the cluster can take on the leader role if the situation requires it (for example, if both the leader and the current standby nodes go down).

When a new node becomes the leader, it takes ownership of the virtual IP address used for leader access to the cluster. Because all of the nodes in the cluster share the same database, this transition takes place seamlessly, ensuring that the cluster survives the failure of one or more nodes.

The virtual IP address is assigned to the primary control card in the configuration jump-start wizard:

Step xx: Cluster mgmt virtual IP address and masklen? [0.0.0.0/0]

Each node in the cluster is performing one of the following roles at any given time:

- **Leader** – This node has possession of the cluster's virtual IP (VIP) address and takes responsibility for dispatching commands to the entire cluster.
- **Standby** – This node takes over the leader role in the event of a failure on the node currently holding the role.
- **Normal** – These nodes perform normal GigaVUE operations with minimal cluster responsibilities. However, they, too, have a complete copy of the cluster's database. When a leader fails and standby is promoted to be the new leader, an election process takes place automatically between all normal nodes, ensuring that a new standby is found.

Setting a Node's Priority in the Leader Election Process

Clusters of GigaVUE-OS nodes perform a leader election in the following situations:

- Cluster reload
- Leader or standby node failure

In either of these cases, a new node is selected to perform the necessary role(s). You can set the **cluster leader preference** for each individual node in the cluster to specify how likely the node is to claim a leader/standby role. Higher values are more likely to claim the leader/standby role; lower values are less likely.

Use preference settings from 10 to 100 for leader, standby, and normal roles. Use preference settings from 1 to 9 for normal nodes that are excluded from taking the leader or standby role.

In software version 4.5, the preference cannot be set to zero. A node with a preference of 0 in an earlier software version will be changed to 1 after upgrading to 4.5 or higher.

GigaVUE-OS sets defaults for the **preference** argument based on the type of control card in use. If you choose to change a node's **preference** setting, it is generally preferable to set higher priorities for nodes with more processing power. GigaVUE-HC3 node provides the most processing power, followed by GigaVUE-HC1 nodes, followed by GigaVUE TA Series nodes.

NOTE: All GigaVUE TA Series nodes including the white box, will automatically be added to a cluster with preference set to 1 because any Traffic Aggregator can never take the role of, or be eligible to be, the leader.

Note: The Clustering Daemon (Clusterd) restarts, if the no card slot 1/4 down force command is executed after performing a cluster reload.

In addition, in an event of a cluster reboot, any GigaVUE TA Series node in a cluster may show as standby for a couple of minutes while the cluster is coming up from the reboot cycle. However, once the cluster is up and running, none of the GigaVUE TA Series nodes can be a standby.

About the “Unknown” Cluster Role

In addition to the standard roles in [About Cluster Roles](#), the system may occasionally report a node operating with an **unknown** cluster role. A node with an unknown cluster role is no longer being actively managed by the leader.

When a node that was formerly part of a cluster transitions to an **unknown** cluster role, its database will typically be out of synchronization with the leader's. You can restore the node to the cluster by using the **reset factory keep-all-config** command, followed by a reboot, and running **configuration jump-start** to rejoin the cluster with a clean local database.

NOTE: If a leader gets unknown cluster role, do not perform any configuration on the leader node as database sync may not happen.

Sample Cluster Control Connections

The GigaVUE-OS provides a flexible approach to cluster control traffic, allowing you to route it over cluster management or Mgmt ports. The ports available and their ethx designations vary by control card version and node type, as summarized in the following table:

Control Card/Node Type	Possible Cluster Control Ports	Deployment Models
HCCv2 Control Card	Mgmt (eth0)	Mgmt (eth0) and L2 switch
GigaVUE-HC3 Node	Mgmt (eth0)	Mgmt (eth0) and L2 switch
GigaVUE-HC1 Node	Mgmt (eth0)	Mgmt (eth0) and L2 switch
GigaVUE TA Series Nodes	Mgmt (eth0)	Mgmt (eth0) and L2 switch

Sample Cluster Control Configurations

Nodes in the same cluster must use the same cluster interface. For example, if there is a GigaVUE-TA100 in the cluster, all nodes in the cluster must use eth0.

Zeroconf for Cluster Management Ports

By default, cluster management ports use zero configuration networking (zeroconf) to establish networking settings. This eases configuration when establishing clusters using the cluster management port(s).

Keep Cluster Management Ports Connected!

IMPORTANT: Clusters implemented using the cluster management ports for cluster control traffic must ensure that the cluster management ports of all nodes in the cluster are connected at all times. This prevents a situation where multiple leaders claim the management VIP address, resulting in the inability to connect to it at all.

Sample Stack-Link Configurations

This section illustrates some sample configurations for the data-carrying stack-links in a cluster, including a star configuration and a daisy-chain using a GigaStream. You can see a combination of star and daisy-chain in [About Cluster](#).

IMPORTANT: Ensure that you do not cable the stack-links in a loop. Use a star or daisy-chain configuration, as follows:

Star Configuration

Use a GigaVUE-OS node as the hub in a star configuration. This makes it easy to create a star configuration that maximizes traffic distribution efficiency. With a star configuration, no destination is further than two hops away. Note that the following image only shows the stack-link connections and not the cluster control connections from the control cards.

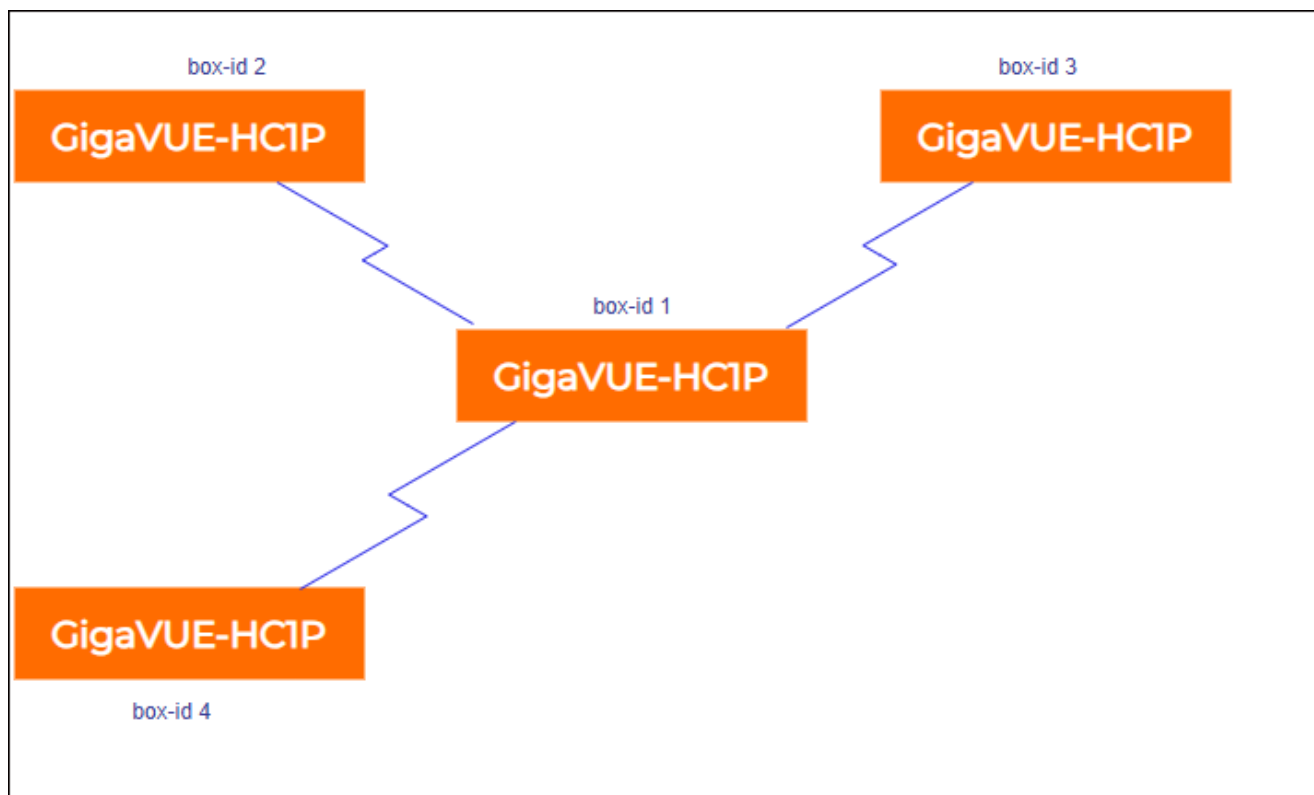


Figure 3 Star Configuration

Daisy-Chain Configuration Using GigaStream for Stack-Link

You can connect two GigaVUE-OS nodes together in a daisy-chain, for example, using any 10Gb line card port. Since there can be up to 96 10Gb ports on a single GigaVUE-HC3 node, the stack-link needs enough bandwidth to handle expected cross-node traffic volume. Create a stack GigaStream out of up to 24x10Gb (PRT-HC3-X24) or 8x100Gb (PRT-HC3-C08Q16) or 16x40Gb (PRT-HC3-C08Q16) ports to handle expected cross-node traffic loads.



Figure 4 *Daisy-Chain Configuration using GigaStream for Stack-link*

Creating Clusters: A Roadmap

Setting up a cluster consists of the major steps shown in the following figure:

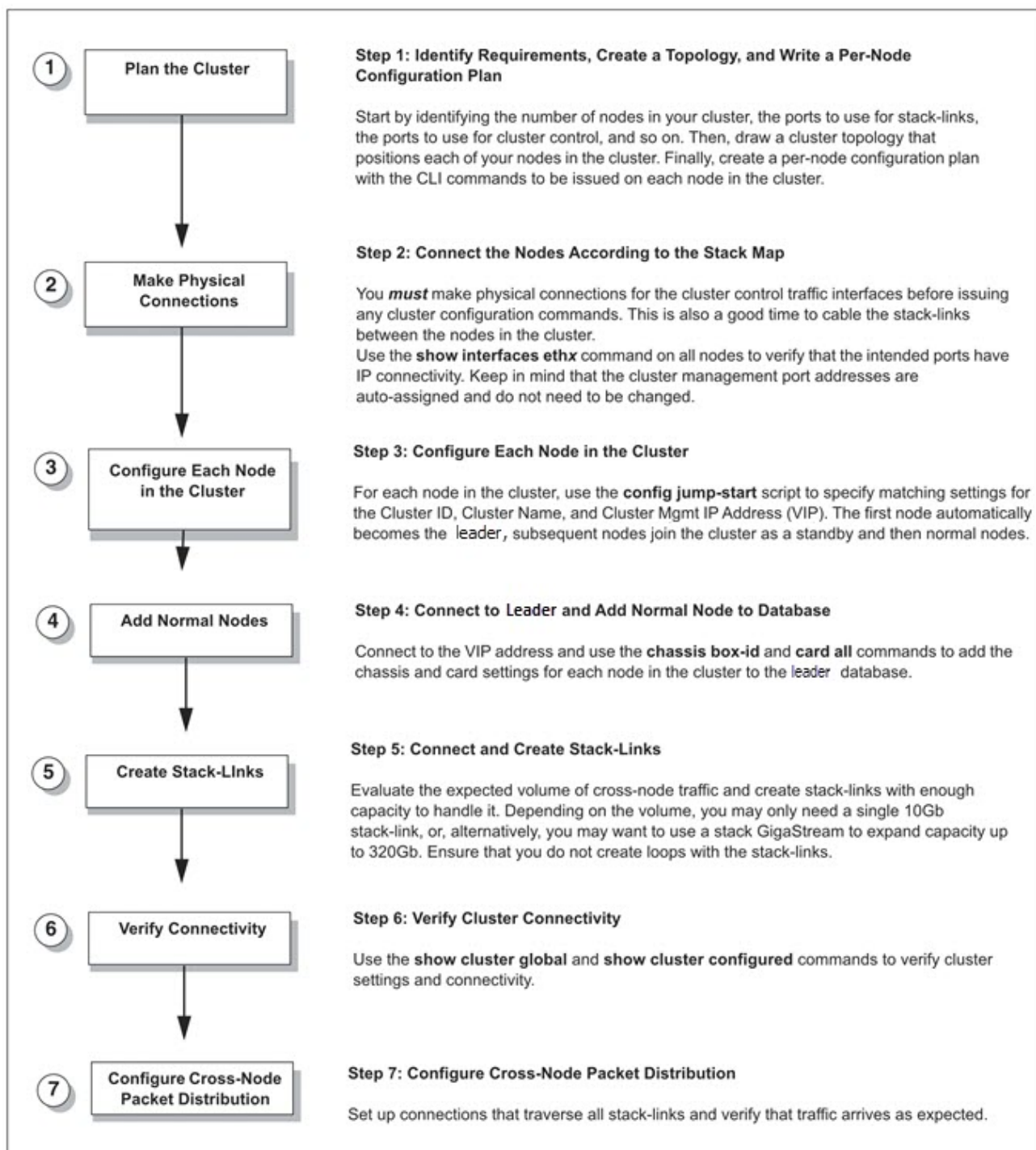


Figure 5 *Creating Clusters: Major Steps*

IPv6 Based Clustering

Until software version 6.1.00, you can create new clusters or manage an existing cluster only using the IPv4 protocol. Starting from software version 6.2.00, support for IPv6 based clustering is available based on which you can create new clusters and manage existing clusters using IPv6 protocol. You can configure the cluster topologies and perform cluster-related operations using IPv6 stacking. IPv6-based clustering is applicable for both GigaVUE HC series devices and GigaVUE TA Series devices.

Rules, Notes, and Limitations

Refer to the following rules, notes, and limitations:

- IPv6 based clustering is available only for the following types of clusters:
 - Physical device out-of-band clustering: Auto-discovery of IPv6 cluster is supported.
 - Layer 3 out-of-band clustering: Manual discovery of the IPv6 cluster using the primary IP address, secondary IP address and cluster VIP.
- IPv6 support for Inband clustering is not supported.
- You can create new IPv6 based clusters from both GigaVUE-FM and the CLI. However, switching an existing IPv4 based cluster to IPv6 based cluster can be performed only from the CLI. Refer to [Switch IPv4 based Cluster to IPv6 based Cluster](#) for details.
- Both auto-discovery and manual discovery of the cluster devices are supported in IPv6 based clustering. You can configure the following addresses as IPv6 addresses for manual discovery:
 - Primary Address
 - Secondary Address
- Regular OOB clusters and Layer 3 OOB clusters can be created and managed using either all IPv4 addresses or all IPv6 addresses. You cannot have both IPv4 and IPv6 address within the same cluster. However, for Layer 3 OOB clusters, Virtual IP address can be configured as either IPv4 or IPv6 address, irrespective of the cluster control protocol.
- When adding nodes to existing cluster, you cannot add an IPv6 node to an existing IPv4 cluster and vice-versa. Also, when creating clusters, select the cluster protocol based on the IP address of the node that is managed in GigaVUE-FM. For example, if a node is managed with IPv4 address, then when creating a cluster, cluster protocol must be IPv4.
- The leader node should be configured with a higher preference than the standby nodes to ensure failover management.
- When creating a IPv6 cluster from GigaVUE-FM, it is recommended to use 0.0.0.0 as the VIP address.

Create IPv6 based Cluster

You can configure regular clusters and leaf-spine clusters by selecting the required protocol as either IPv4 or IPv6. Refer to the following topics for details:

- [Regular Cluster Formation Workflow](#)
- [Leaf-Spine Cluster Formation Workflow](#)

Switch IPv4 based Cluster to IPv6 based Cluster

GigaVUE-FM does not allow you to directly switch an IPv4 based cluster to IPv6 based cluster and vice-versa. You must use the GigaVUE-OS CLI to perform the switching operation. Refer to the following table:

S.No	From	Steps
1	GigaVUE-FM GUI	Disconnect the device from GigaVUE-FM. 1. Go to Inventory > Physical > Nodes. 2. Select the required cluster. 3. From the Actions drop-down, select Disconnect Node. The device gets disconnected from GigaVUE-FM. Config-sync updates will not take place and API updates will be blocked. Note: Do not perform any configurations in the device after disconnecting the device from GigaVUE-FM.
2	CLI	Execute the following command from the CLI prompt of the leader node: Seattle [1010: leader] config # cluster ip-ver-switch diagnostics The diagnostics command establishes a server-client relationship between the leader and the member nodes of the cluster and checks if all the devices in the cluster are reachable and if there are any firewall or routing issues. Fix the issues and re-execute the command.
3		Execute the following command in the CLI prompt of the leader node to change the communication protocol version from IPv4 to IPv6 and vice-versa. Seattle [1010: leader] config # cluster ip-ver-switch Note: Before executing this command ensure that configurations are synced and all unsaved changes are saved.

S.No	From	Steps
		This command checks the following: • if all the devices have the proper IPv4 or IPv6 addresses to switch over. • If the devices are stable. If any of the devices in the cluster is in Safe mode, this command will be aborted. This command reloads the cluster. NOTE: In case of Layer3 OOB nodes, reconfigure the primary and secondary IP address of the leader node in all the member nodes of the cluster.
4	GigaVUE-FM GUI	1. Go to Inventory > Physical > Nodes. 2. Select the required cluster. 3. From the Actions drop-down, select Edit Cluster. 4. Click Change Protocol / VIP option. 5. Enter the following details: • From the Protocol drop down, Select IPV6 • VIP (mandatory) • Primary IP (mandatory for L3 OOB Clusters) • Secondary IP 6. Click OK. Note: Before connecting the Node in FM, if the VIP address is modified in device , you must add the new VIP address and credentials in Node Details page(Refer to Node Details section for adding VIP address and its credentials).
5	GigaVUE-FM GUI	Reconnect the device back to GigaVUE-FM. 1. Go to Inventory > Physical > Nodes. 2. Select the required cluster. 3. From the Actions drop-down, select Connect Node.

Refer to the following sections the GigaVUE-OS CLI Reference guide for configurations related to IPv6 based clustering:

S.No	Details in the GigaVUE-OS CLI Reference Guide	Reference
1	The cluster CLI command is updated for the following: - To configure protocol as ipv4 or ipv6 protocol - To verify if the devices in the cluster are reachable by the cluster leader - To switch from IPv4 to IPv6 or vice-versa	cluster
2	Example to remove a device from IPv4 cluster and add the same device to another IPv6 cluster.	How to Remove a Node from an IPv4 Cluster and Add it to an IPv6 Cluster and Vice-versa
3	For the Layer 3 Out of Band clustering, the primary IP address and secondary IP address of the cluster is cleared. After the protocol is switched, you must reconfigure the primary IP address and secondary IP address based on the switched IP.	Clustering a Node Using Layer 3 Out-of-Band Manual Discovery

Rules and Recommendations for Nodes and Clusters

Keep in mind the following rules and recommendations when managing nodes and clusters:

- If you add a node as a standalone node or as a cluster manually in GigaVUE-FM, the node will remain in that state unless you delete the standalone node/cluster. Refer to [Using Command Line Interface for Managing Clusters](#) for rules on adding and deleting the nodes using CLI.
- You can add a cluster to GigaVUE-FM using the cluster VIP or the IP address of the leader.
- The state of the cluster is decided based on the cluster API response from the device.
- Before joining an existing GigaVUE node to a cluster, it is recommended to use the **reset factory only-traffic** command to clean up existing traffic-related configuration. For example, in a cluster there is one leader and the other nodes are GigaVUE-TA nodes. When the leader is removed from the cluster, the GigaVUE-TA nodes moves to the unknown state. If another leader joins the cluster with a different database, the GigaVUE-TA nodes that are existing in the cluster will remain in the unknown state.

- Remove all physical loops before enabling the cluster. An accurate cluster topology will help with this. The GigaVUE-OS node automatically detects and prevents configurations that would cause loops, but it is best to avoid them in the first place.
- Star configurations offer the most efficient use of bandwidth. In general, use one GigaVUE-OS node at the hub of your star and then connect spokes off of that.
- GigaVUE-FM does not discover devices when both the IP interface address and GigaVUE-FM IP are on the same network.
- Create stack-links with enough capacity to match expected cross-node traffic. For example, you can use a 24x10Gb (PRT-HC0-X24) or 6x40Gb (PRT-HC0-Q06) for the GigaVUE-HC3 node.
- Configure only the stack type ports that you will use in the stack-link configuration. Loops can be created if stack type ports are configured but then not used in a stack-link.
- The first node added to the cluster becomes the leader. This is important when creating a new cluster using an existing, already-configured node and a new node. If you want to keep the configuration on your existing node, use it as the first node in the cluster. This way, the existing node becomes the leader and the new node inherits its configuration, preserving your existing settings. GigaVUE TA Series nodes are an exception since they cannot be the leader.
- When joining a new node to an existing cluster, give the new node a lower precedence than the leader. Once the database has synchronized to the existing leader, you can increase the precedence to make the newly joined node the leader, if that is required.
- You cannot have more than one leader in a cluster.
- For Inband Clustering, you must make physical connections for the cluster control traffic interfaces before issuing any cluster configuration commands. Because the first node added to a cluster becomes the leader, configuring cluster settings before physically connecting the cluster control network results in a situation with multiple leaders attempting to connect to the same cluster.

NOTE: Merging clusters is not supported.

- For Layer 3 Out of Band clustering, the leader and the standby nodes must reside within the same subnet.
- GigaVUE TA Series and Certified Traffic Aggregation White Box nodes in a cluster can have tool, network, hybrid, and stack ports.
- A GigaVUE TA Series node cannot be a leader. It can only join a cluster with other node types, such as GigaVUE-HC1, GigaVUE-HC3, GigaVUE-HC1-Plus, or GigaVUE-HCT.
- A GigaVUE TA Series node cannot be a standby node either. If the cluster has one leader and all other nodes are GigaVUE TA Series nodes, the cluster will not have a standby.
- Since a GigaVUE TA Series node can never be a leader or a standby in a cluster, a database restore is not possible. The best option is a text restore that has the information of the other nodes in the cluster removed from the text backup of the GigaVUE TA Series.

- If GigaVUE-HC1 and GigaVUE-HC3 devices are member nodes of a scaled cluster of approximately 10K map rules, then the following sequence of steps should be avoided:
 - a. Removal of nodes from the cluster.
 - b. Reload the removed node with 10K map rules.

If the above steps are done, the nodes may get locked out and you will not be able to log in to the devices. To remove a GigaVUE-HC1 or GigaVUE-HC3 node from a cluster and use it as a standalone node:

- Remove the node out of cluster.
- Erase the configuration using the "no traffic all" command on the standalone node.
- Reload the node.

RBAC and Tag Control on Nodes and Clusters:

- A user belonging to the Infrastructure Management resource category can create clusters in GigaVUE-FM using the nodes that he has access to, depending on the tag keys and the tag values assigned to him. The tag keys and the tag values of the user will be applied on the nodes and the cluster. Similarly, when the user removes a node from the cluster, the removed node gets the tags of the user.
- If a user has tag key and tag value set to ALL (as in the case of a super admin or admin user), then the tag key and the tag value applied to the nodes in the cluster depends on the tag value of the leader of the cluster. Similarly, if a node is removed from the cluster, then the tag value of the leader is applied to the removed node.

Example:

Consider the following:

- **tag key:** Location
- **tag values:** California, Texas, Washington and New York
- User configured with tag key Location and has access to all tag values (ALL). Also, the user has access to the following devices.
- dev1 - 10.115.46.11 - Tag-> Location: Texas
- dev2 - 10.115.46.12 - Tag -> Location: California

If the user creates a cluster C1 with dev1 and dev2, and dev1 as a seed node, as the user has access to all tag values of the tag Location, the tag value is derived from the seed device. In this example, the seed device is dev1 which has tag value Texas.

The created cluster C1 will have the tag key: Location with value Texas.

- For nodes with single-valued tags, if you change the tag value of the node, a confirmation message pops-up. Based on the response, the tag value of the node is changed. Refer to the [Create User-defined Tag](#) section in the GigaVUE Administration Guide.

Using Command Line Interface for Managing Clusters

The following table provides information on the behavioral changes observed in GigaVUE-FM when the nodes are managed from CLI.

Process	Until Software Version 5.10.00	From Software Version 5.11.00
Add Nodes to Cluster	If the node is already managed by GigaVUE-FM: The node will be added to the cluster and stack mode will be updated. If the node is not already managed by GigaVUE-FM: The node will be added to GigaVUE-FM.	If the node is already managed by GigaVUE-FM: Config sync will fail and is notified with appropriate messages. You must first delete the node from GigaVUE-FM and then add the node to the cluster. For example, consider the following nodes and clusters managed by GigaVUE-FM: - Stand alone node A - Cluster C with nodes B and C. To add the standalone node A to cluster C, you must first delete the node A from GigaVUE-FM and then add the node to cluster C. If the node is not already managed by GigaVUE-FM: The node will be added to GigaVUE-FM.
Remove nodes from cluster	The node removed will be managed as a standalone node in GigaVUE-FM.	The node removed from the cluster will also be removed from GigaVUE-FM. If you want GigaVUE-FM to manage the node as a standalone device, you must add the node again. Refer to Add New Physical Node or Cluster to GigaVUE-FM section.
Edit Cluster ID	The new cluster id will get updated	The next config sync will fail because of

Process	Until Software Version 5.10.00	From Software Version 5.11.00
	during the next config sync cycle.	the change in cluster ID. You must remove the cluster and add it again, so that the cluster is rediscovered with the new cluster ID.
Moving nodes between clusters	The node is removed from the existing cluster and added to the new cluster.	The node will be moved to the new cluster only if it is removed from the existing cluster. If the node is not removed from the existing cluster, config sync will fail until the node is removed from existing cluster. This could happen when the config sync for the cluster from which the device is moved out is triggered first. For example, consider the following nodes and clusters managed by GigaVUE-FM: Cluster C1: Nodes A, B, C Cluster C2: Nodes E, F, G If node E is moved from C2 to C1 through CLI, then following will be the behavior in the next config sync: If cluster C1 first completes the config sync: • Config sync will fail. This is because a device which is already in C2 is now being claimed in C1. • As soon as cluster C2 completes the config sync, node E will be removed from C2. • The next config sync will succeed for cluster C1. If cluster C2 first completes the

Process	Until Software Version 5.10.00	From Software Version 5.11.00
		config sync: - Node E will be removed from C2. - When config sync for C1 is completed, node E will be added to C1. If you keep moving the nodes from C2 to C1, then all but the last node will get moved. To move the last node you must first delete the cluster C2. In the subsequent config sync, node G will get added to cluster C1.

NOTE: If a node in a cluster does not report during config sync, GigaVUE-FM will remove the node, and an alarm with severity status 'Critical' is triggered (*Alarm description: Device is not reported*). If the node reports back to the same cluster, then the alarm will be cleared. However, if you acknowledge or delete the alarm and the node does not report back (if the node has been removed or added to another cluster) within an hour after the alarm has been acknowledged, then GigaVUE-FM will clear the alarm.

GigaVUE TA Series and GigaVUE-HC3 Clustering Recommendations

The following recommendations are for GigaVUE-TA Series and GigaVUE-HC3 nodes in a cluster:

- When a GigaVUE-TA Series or GigaVUE-HC3 is connected to a node of a different type, ports may not become operationally up until the stack-links are created between the stack ports. To ensure the ports become operationally up:
 - Configure the specified ports as stack ports.
 - Configure the stack-link between the stack ports.

Cluster Rules

Clusters must adhere to the following rules:

Rule

All GigaVUE-OS nodes in a cluster must run the same version of the GigaVUE-OS software, including the major and minor version numbers.

Each GigaVUE-OS node in a given cluster must share the same **Cluster ID**, **Cluster Name**, and **Cluster Mgmt IP Address**. You can configure these settings in the **config jump-start** script, or, alternatively, use separate **cluster** commands to set them. When adding a node present on the same IP subnet to an existing cluster, so long as you specify the cluster ID correctly, the cluster Mgmt IP address (VIP) will be synchronized from the leader automatically.

Cluster management ports must be on the same IP subnet.

Each GigaVUE-OS node in a cluster must have its own unique box ID. The box ID is assigned to a chassis from the leader with the **chassis box-id <box ID> serial-num <serial number>** command (). Keep in mind that if you are using GigaSMART trailers to identify ingress ports, only box IDs from 1-64, inclusive, are supported.

You can only connect optical-to-optical stack-links. Stack-links must be at least 10Gb. In addition, they must use the same transceiver types, such as LR-to-LR, or SR-to-SR.

Use a stack-link between different types of GigaVUE-OS nodes so long as the medium, speed, and number of ports involved is the same on both sides.

Best Practices for OOB Clusters with IGMP Snooping

The following are best practices for out-of-band (OOB) clusters if Internet Group Management Protocol (IGMP) snooping is enabled in the cluster.

Clustering relies on the IGMP protocol to discover peer nodes and to communicate with them. Switches often have IGMP snooping enabled by default, which will filter IGMP packets from ports that do not have periodic IGMP membership reports. This can cause IGMP packet drops in out-of-band clusters.

Refer to [About IGMP Snooping in a Cluster](#) for more information. Also refer to the following best practices:

- allow Internet Group Management Protocol (IGMP) traffic by using an IP filter chain. Refer to [Allow IGMP Traffic](#).
- enable an IGMP querier. Refer to [Enable an IGMP Querier](#).

These best practices result in the following:

- hostnames being properly displayed in CLI commands that display cluster information such as **show cluster global brief**
- nodes joining clusters faster, especially nodes that are not capable of becoming a leader, such as GigaVUE TA Series nodes
- no multiple leaders being created in an out-of-band cluster. This can occur when a node that is capable of becoming a leader is not able to see the current leader and hence elects itself as a leader.

About IGMP Snooping in a Cluster

IGMP snooping is a networking feature that monitors IGMP membership reports received from different ports on a networking switch and learns the ports to which multicast groups belong. When a port stops sending membership reports about a multicast group, the switch will stop forwarding the group's traffic to the port.

An IGMP querier is a router (or switch) feature that periodically queries the network for multicast group interests. If a node on the network belongs to a certain multicast group, it responds to the queries, the router then records or refreshes its record of the node's interest in the traffic for the group, and the router forwards traffic to the network towards the node. The switches on the network with IGMP snooping enabled also learn from the responses and maintain their records about the nodes' interests in groups and forward traffic accordingly.

Hostnames are detected using Multicast Domain Name System (mDNS) packets, which are in multicast group 224.0.0.251.

An IP filter is a chain of rules for the treatment of packets. Refer to the *"Using IP Filter Chains for Security"* section in the *GigaVUE-OS CLI Reference Guide*.

Allow IGMP Traffic

If IP filtering is enabled (and IGMP snooping is enabled):

- Verify that IGMP traffic is allowed.
- For example, issue the following CLI commands:
(config) # ip filter chain INPUT rule append tail target ACCEPT dup-delete protocol igmp
(config) # ipv6 filter chain INPUT rule append tail target ACCEPT dup-delete protocol igmpv6
- Verify that mDNS traffic is allowed.

If IGMP snooping is disabled, you do not need to allow IGMP traffic. However, you must allow UDP multicast traffic that targets 224.0.0.251. For example, issue the following CLI command:

```
(config) # ip filter chain INPUT rule append tail target ACCEPT dup-delete dest-addr 224.0.0.251 /32
```

where:

dest-addr specifies the multicast group

Enable an IGMP Querier

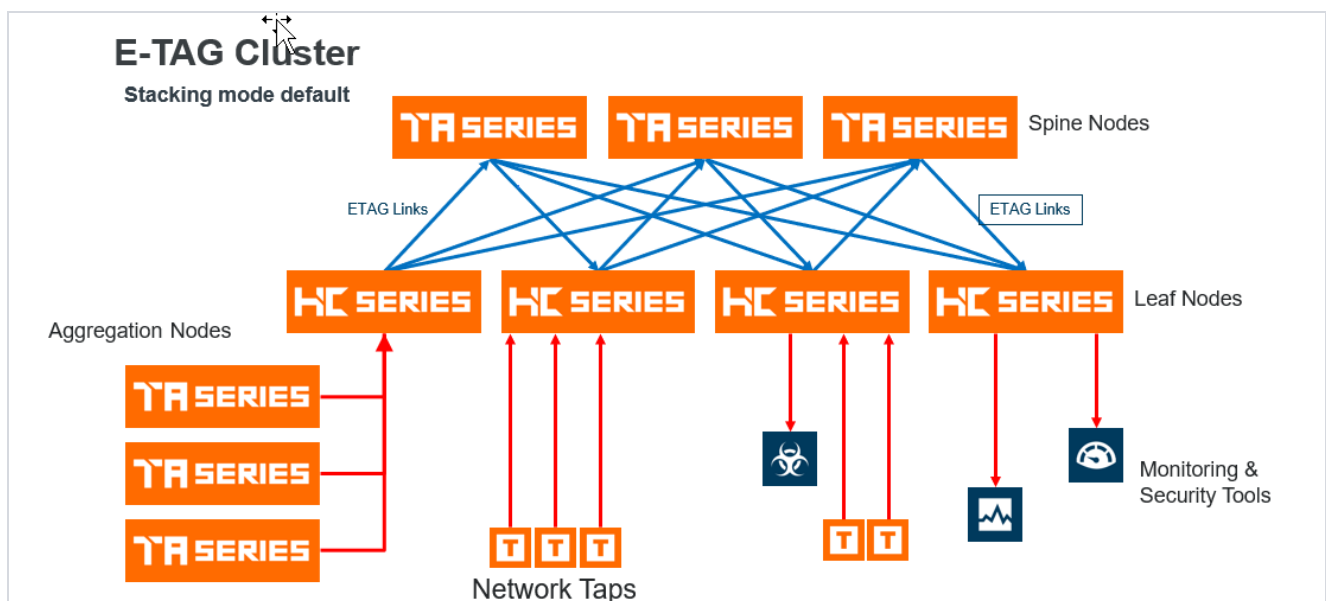
If IGMP snooping is enabled:

- Check if there is an IGMP querier on the cluster network. The querier periodically sends queries that trigger the nodes in the cluster to send IGMP membership reports. For example, use a sniffer tool to verify if there is an IGMP querier on the network, such as Wireshark.
- IGMP snooping and IGMP snooping querier settings vary by networking switch. Refer to the respective documentation for how to configure them on your device.

When IGMP traffic is allowed and an IGMP querier is enabled in the network, the switches in the network will be refreshed through the IGMP membership reports.

E-Tag Clustering

The 5.16 release introduces a new E-Tag based stacking mode to cluster with GigaVUE-TA400 or GigaVUE-HCT. All legacy cluster topologies (leaf-spine, tree, etc.) with OOB cluster management are supported with E-tag stacking mode. Refer to the example below.



The new E-TAG stacking mode is supported on all the platforms listed below.

- GigaVUE-HC3 CCv1 & CCv2
- GigaVUE-HC1
- GigaVUE-HC1-Plus
- GigaVUE-HCT
- GigaVUE-TA25
- GigaVUE-TA25E
- GigaVUE-TA100
- GigaVUE-TA200
- GigaVUE-TA200E
- GigaVUE-TA400
- GigaVUE-TA400E
- DELL S4112F-ON

The BiDi optics on stack ports are also supported in E-Tag stacking mode.

NOTE: The GigaVUE-TA400 and GigaVUE-HCT platforms support only Default (E-Tag) stacking mode and do not support Legacy stacking mode. All other platforms support both Legacy and Default (E-Tag) stacking modes.

Stacking Mode

The E-Tag Clustering introduces a user selectable stacking mode. The stacking modes are as follows:

- **Legacy:** This option selects Legacy stacking mode.
- **Default:** This option selects E-Tag stacking mode.

To configure the default stacking mode or the legacy stacking mode through GigaVUE-OS -CLI use the following commands :

(config) # system stacking-mode legacy: Selects the Legacy Stacking mode

(config) # no system stacking-mode legacy: Selects the Default Stacking mode.

Legacy Stacking Mode	E-Tag (Default) Stacking Mode
(config) # system stacking-mode legacy (config) # show system stacking-mode Stacking Mode configuration: Mode : legacy-mode	(config) # no system stacking-mode legacy (config) # show system stacking-mode Stacking Mode configuration: Mode : default-mode

NOTE: After user confirmation the system stacking-mode legacy command immediately resets the traffic configuration and initiates a cluster reload of all nodes. After the cluster is up, the configuration saved in the backup file must be applied manually to restore the traffic configuration.

For example :

```
[cluster: leader] (config) # no system stacking-mode legacy
! WARNING: Changing stacking mode will automatically
! - Take backup of config in file stacking_mode_config_backup.txt
! - Reset factory only traffic config
! - RELOAD the cluster
! - User must manually apply stacking_mode_config_backup.txt after bootup
Confirm stacking mode change? [no] yes
Configuration saved to database 'initial'
System shutdown initiated -- logging off.
```

After the cluster is up and user is logged back in, apply the saved configuration in the backup file:

```
[cluster: leader] (config) # configuration text file stacking_mode_config_backup.txt apply
fail-continue
```

Refer to the [system](#) section in GigaVUE-OS CLI Reference Guide to know more.

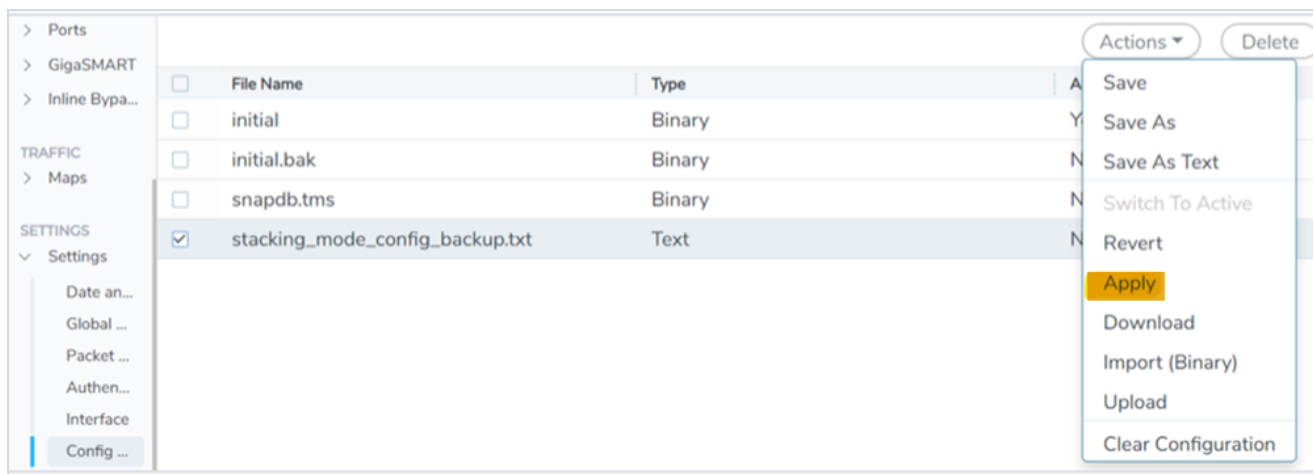
To configure from GigaVUE-FM use the stacking mode drop-down options. Refer to the [Regular Cluster Formation Workflow](#), [Edit Cluster Parameters](#), [Leaf-Spine Cluster Formation Workflow](#).

Switching Stacking Mode

The Stacking mode can be switched from Legacy to Default and vice versa. Switching the stacking mode will reload the cluster and maintain a backup file of the last applied configuration. A Confirmation window appears advising that a backup file is generated with the updated traffic configuration. The configuration saved in the backup file must be applied manually to restore the traffic configuration after the cluster is up. The command used to apply the backup configuration is as follows:

```
[cluster: leader] (config) # configuration text file stacking_mode_config_backup.txt apply
fail-continue
```

Refer below, to apply the backup configuration file from GigaVUE-FM.



Switching the stacking mode will not be allowed if the cluster includes an unsupported node.

Refer to [Regular Cluster Formation Workflow](#), [Edit Cluster Parameters](#), [Leaf-Spine Cluster Formation Workflow](#) to know more.

Notes

1. The L3 and L4 fields hashing of double tag Q-in-Q traffic is not supported over stack links in E-Tag mode on non GigaVUE-TA400 platforms. This limitation is not applicable for GigaVUE-TA400.
2. Common hash settings for all stack and non-stack GigaStream in E-Tag mode. Fabric advanced-hash command is not applicable to stack GigaStream in default stacking mode but applicable to GigaSMART groups on GigaVUE® HC Series.
3. In an E-tag cluster having MPLS Header Stripping enabled on GigaVUE-TA25, GigaVUE-TA25E and GigaVUE-HC1-Plus source/network ports, the customer outer vlan tag gets stripped along with MPLS labels specifically for tagged MPLS customer traffic.

New 6.0

1. Circuit ports as destination in GigaSMART first level maps (L2 circuit encapsulation tunnels with first level map) are not supported in E-Tag mode in 5.16 release. This is supported from release version 6.0.
2. The L2GRE and VXLAN tunnel encapsulation and decapsulation are not supported in E-Tag mode in 5.16 release. This is supported from release version 6.0.
3. The MPLS Header Stripping is not supported on GigaVUE-TA25 in the E-Tag mode in 5.16 release. It is supported on GigaVUE-TA25 from release version 6.0. On GigaVUE-TA25, the outer customer VLAN tag will also be stripped along with MPLS header for the VLAN tagged MPLS packets.

4. MPLS Header Stripping in E-Tag mode in 5.16 release on GigaVUE-HC3, GigaVUE-TA200, GigaVUE-TA100 has one limitation of 4 byte VLAN tag added when header strip enabled ports are mapped to tool ports within the same box/node specifically. This limitation is not applicable from 6.0 release version.
5. VXLAN Header Stripping in E-Tag mode in 5.16 release on platforms other than GigaVUE-TA400, GigaVUE-TA25 has limitation of 4 byte VLAN tag added when header strip enabled ports are mapped to tool ports within the same box/node specifically. This limitation is not applicable from 6.0 release version.

Cluster Safe and Limited Modes

Safe and limited modes in cluster safeguard critical provisioning errors for both standalone nodes and nodes in a cluster.

During provisioning operations such as configuring a map, in rare scenarios there can be unrecoverable system errors that can potentially put the cluster, clustered nodes, or standalone nodes into unsafe or unstable states. Once in such a state, additional operations or configuration changes can cause the node to crash, the cluster to deform, or data traffic to be impacted. For example, due to a node attempting to rejoin a cluster, a chassis can end up in a reboot loop. In previous software versions, there was no way to prevent entering the loop.

These modes provide notification, stop further operations from being performed, and give you time to troubleshoot and plan the recovery of the cluster, the clustered node, or the standalone node.

Two modes are supported. The first is called safe mode and is triggered when the node detects unrecoverable errors, but the existing flow maps are not impacted. The second is called limited mode and is triggered when the node detects continuous system reboots. In this mode, the node will become standalone and only basic configuration will be allowed.

Safe Mode

A node enters safe mode when there are unrecoverable errors. Any node in a cluster can enter this mode. The purpose of this mode is to detect system configuration failures early and avoid future failures, such as system crashes.

Examples of unrecoverable errors are when there are inconsistencies between the system and the running configuration or when the cluster configuration did not merge properly with the existing configuration.

As part of merge error recovery, nodes joining a cluster are automatically restarted so the merge error can be fixed. If the restart cannot correct the merge error, the node will enter safe mode.

Another example is that a GigaVUE TA Series node could enter safe mode when unlicensed cluster ports are used in an offline configured map. (It is recommended to use only licensed ports in map configurations.)

A node will automatically enter safe mode.

To recover from safe mode, reload the node. If safe mode persists, contact Gigamon Technical Support.

Limited Mode

A node automatically enters limited mode when it detects repeated system crashes.

Limited mode is triggered when there are three (3) failures/system crashes within 15 minutes. In limited mode, the cluster configuration is ignored. No cluster configuration or GigaVUE-OS configuration is accepted when the node is in limited mode.

When limited mode has been detected, collect information and report it to Gigamon Technical Support.

Support for Cluster Types

The GigaVUE-FM workflow supports only out-of-band clusters; not inband clusters. To create and manage an inband cluster, refer to the *GigaVUE-OS CLI Reference Guide*.

Create Clusters

GigaVUE-FM supports workflow-based configurations for forming clusters. Starting from software version 6.2.00, you can create only IPv6 clusters from GigaVUE-FM.

- Refer to [Regular Cluster Formation Workflow](#) for instructions on how to use the regular cluster formation workflow.
- Refer to [Leaf-Spine Cluster Formation Workflow](#) for how to use the leaf-spine cluster workflow

Regular Cluster Formation Workflow

Gigamon's Cluster formation can be done for maximum of 64 devices.

GigaVUE-FM supports workflow-based configurations for forming a cluster. This workflow walks through the required steps to form a complete cluster for a regular cluster.

NOTE: Refer to [Leaf-Spine Cluster Formation Workflow](#) for how to use the Leaf-Spine Cluster workflow

Deployment Checklist

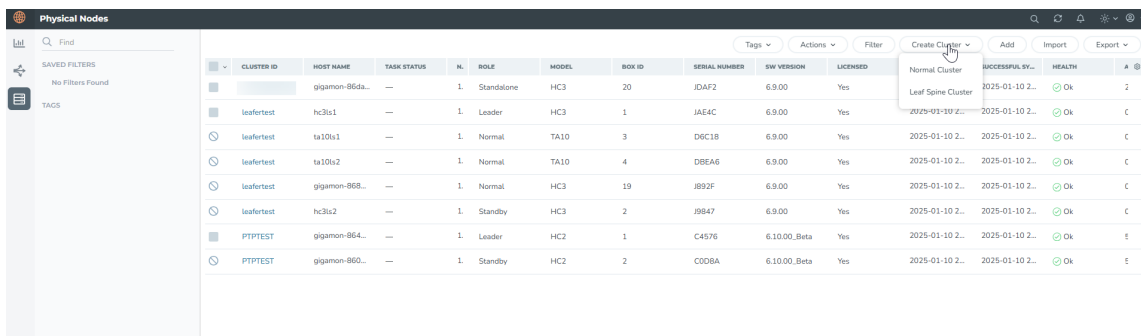
Before forming a Cluster, it is strongly recommended that you familiarize yourself with the relevant documentation and review the following deployment checklist:

- Gigamon Fabric Management must be upgraded to GigaVUE-FM 5.3.00 or later.
- Gigamon device must be upgraded to GigaVUE-OS 5.2.00 or later
- Advanced Features License must be installed on GigaVUE-TA devices.
- Physical connection must be established to create stack links.
- Devices must be physically connected to create links among devices from GigaVUE-FM.

Create Regular Cluster Formation

To create a cluster:

1. From the left navigation pane, go to **Inventory > Physical > Nodes..**
2. Click **Create Cluster** and select Normal Cluster.



The screenshot shows the 'Physical Nodes' page in GigaVUE-FM. On the left is a navigation pane with 'Physical Nodes' selected. The main area displays a table of nodes. A dropdown menu is open from the 'Create Cluster' button in the top right, showing 'Normal Cluster' and 'Leaf Spine Cluster' options.

CLUSTER ID	HOST NAME	TASK STATUS	N.	ROLE	MODEL	BOX ID	SERIAL NUMBER	SW VERSION	LICENSED	CREATE DATE	SUCCESSFUL BY...	HEALTH	
	gigamon-86da...	---	1.	Standalone	HC3	20	JDAF2	6.9.00	Yes				
	leafertest hc3s1	---	1.	Leader	HC3	1	JAE4C	6.9.00	Yes				
	leafertest ta10s1	---	1.	Normal	TA10	3	D6C1B	6.9.00	Yes	2025-01-10 2...	2025-01-10 2...	Ok	C
	leafertest ta10s2	---	1.	Normal	TA10	4	D6EA6	6.9.00	Yes	2025-01-10 2...	2025-01-10 2...	Ok	C
	leafertest gigamon-868...	---	1.	Normal	HC3	19	J892F	6.9.00	Yes	2025-01-10 2...	2025-01-10 2...	Ok	C
	leafertest hc3s2	---	1.	Standby	HC3	2	J8847	6.9.00	Yes	2025-01-10 2...	2025-01-10 2...	Ok	C
	PTPTTEST gigamon-864...	---	1.	Leader	HC2	1	C4576	6.10.00.Beta	Yes	2025-01-10 2...	2025-01-10 2...	Ok	F
	PTPTTEST gigamon-860...	---	1.	Standby	HC2	2	C00BA	6.10.00.Beta	Yes	2025-01-10 2...	2025-01-10 2...	Ok	F

Figure 6 Create Cluster

- Filter the nodes based on the Software Version, Model, Stacking Mode, Hostname or IP address, and the Protocol through which the nodes communicate with each other.

Notes:

- GigaVUE-TA and GigaVUE-HCT devices are not supported in Legacy stacking mode.

Select Nodes

1
2

Select Nodes
Configure Cluster

i Select nodes and configure cluster to begin the cluster creation process.

Software Version: Select

Model: Select

Stacking Mode: Legacy

Protocol: IPv4

Q Hostname/IP

	HOSTNAME	MODEL	SOFTWARE VERSION	IP	
☐	gigamon-86daf2	HC3	6.9.00		

|<
<
Go to page: 1 of 1
>
>|

1 node(s) total

Cancel
Next

- Select the nodes to include in this cluster and click **Next**. (Click a device to select it; click it again to deselect it).
- In the Cluster Configuration window, enter a valid **Cluster ID** and Virtual IP (**VIP**) and select the leader in the **Seed Node** list.

NOTE: The leader cluster preferences in GigaVUE-FM determine which of the nodes will be the default seed node. GigaVUE-TA devices cannot be a leader.

Cluster Configuration

✓

2

Select Nodes

Configure Cluster

i

All form elements are mandatory unless indicated as optional.

Cluster ID

Cluster ID

VIP

0.0.0.0/0

Seed Node

gigamon-867d97

i

This node is used to bootstrap a cluster. All additional cluster members will inherit system-level configurations from this node.

Stacking Mode

Legacy

Node Software Version

6.9.00

Next Step

Back

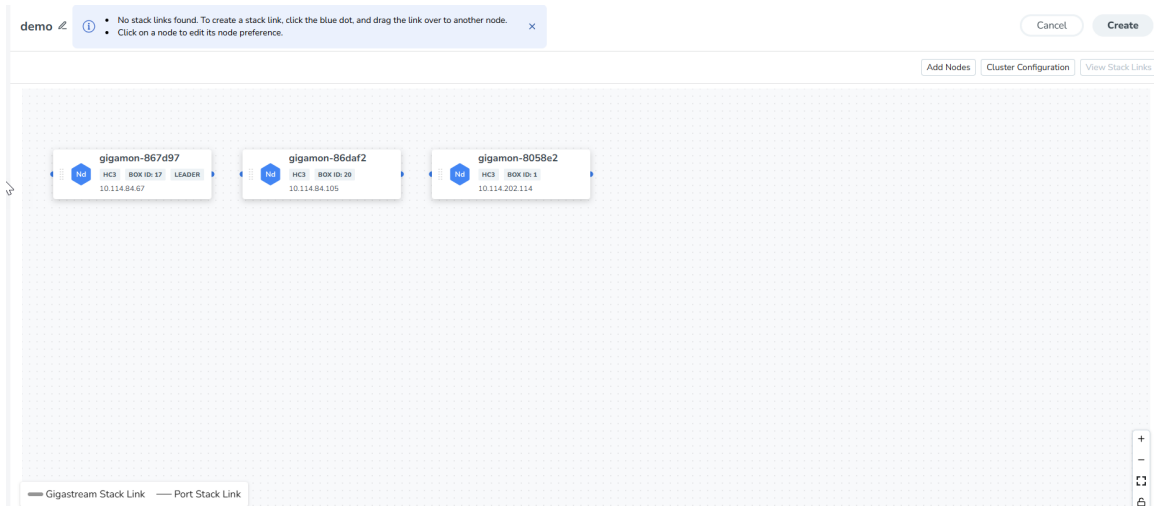
Go to Canvas

- After completing the Cluster Configuration details, click **Go to Canvas**.

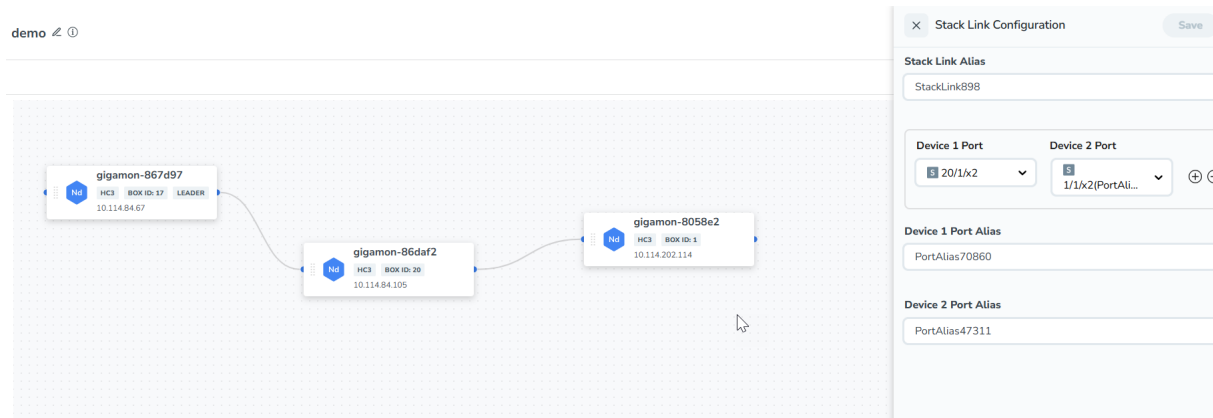
NOTE: Use the **Back** button to return to the Select Devices page and revise the device selection for this cluster.

Customize Stack Links

Finally, customize the stack links to define how the nodes should be connected.



7. Connect any two devices to create a stack link between those two devices. Click the tip of the node and drag your cursor to the second node tip to create a link. After you create the link, a dotted line illustrates the connection.



8. Configure the formed links in the **Stack Links** Configuration panel:
 - a. Select ports in each device that are compatible, for example: x-x ports, x-q ports, q-c ports, and x-c ports.
 - b. Select one or more ports from each device to create a GigaStream stack link.
 - c. Click **Save**.

GigaVUE-FM generates the aliases for each Port stack link and GigaStream stack link. You can edit these aliases.

NOTE: While creating cluster, click **View Stack Links** on the right corner of the canvas to view the details of the stack links of the cluster.

9. Click **Create** to start the cluster creation process.

The Create Cluster progress window in the lower right corner of the page shows the status of every node as it joins the cluster. It takes a few minutes for the cluster to form. The cluster creation process involves the following steps:

- Cluster[clusterName] Creation Successful followed by Seed device
- Verifying Nodes[Will display HostName of all devices]
- Adding Node[HostName] to cluster [clusterName]
- Node[HostName] successfully joined to the cluster.
- Configuring cards for cluster[clusterName]
- Rediscovering cluster[clusterName]
- Configuring ports for the cluster[clusterName].
- Configuring ports will display the status of each stack link and GigaStream whether the creation is successful or not.

When the cluster formation process is complete, you can view the completion message in the progress window.

NOTE: Refer to [Check Cluster Status](#) for Events.

The screenshot displays the GigaVUE Nodes and Clusters interface. On the left, there is a sidebar with a search bar and a list of tags, including 'Ghdfdttyfuf'. The main area shows a table of nodes with columns: CLUSTER ID, HOST NAME, SW VERSION, MODEL, TASK STATUS, NODE ADDRESS, ROLE, BOX ID, SERIAL NUMBER, and LICE. The table lists 16 nodes, including 'leafertest' and 'ClusterId'. A 'Create Cluster' progress window is visible in the bottom right corner, showing a progress bar at 24%.

CLUSTER ID	HOST NAME	SW VERSION	MODEL	TASK STATUS	NODE ADDRESS	ROLE	BOX ID	SERIAL NUMBER	LICE
leafertest	hc3ls2	6.9.00	HC3	—		Standby	2	J9847	Yes
leafertest	ta10ls2	6.9.00	TA10	—		Normal	4	DBEA6	Yes
leafertest	ta10ls1	6.9.00	TA10	—		Normal	3	D6C18	Yes
leafertest	hc3ls1	6.9.00	HC3	—		Leader	1	JAE4C	Yes
ClusterId	gigamon-86722e	6.6.00	HC2	—		Standby	60	C722E	Yes
ClusterId	gigamon-86b9fc	6.6.00	HC1	—		Leader	13	HB9FC	Yes
	gigamon-8058e2	6.9.00	HC3	—		Standalone	1	J58E2	Yes
	gigamon-86daf2	6.9.00	HC3	—		Standalone	20	JDAF2	Yes
	gigamon-86892f	6.9.00	HC3	—		Standalone	19	J892F	Yes
	gigamon-867d97	6.9.00	HC3	—		Standalone	17	J7D97	Yes
	gigamon-869879	6.9.00	HC3	—		Standalone	60	J9879	Yes
	PUSPA-DELL4112	6.9.00_Beta	DELL-S4112F...	—					

10. Click **Go to Cluster** in the progress window to view the cluster overview.

Edit a Cluster

The Edit cluster option supports only the following operations to the existing cluster:

- Multiple devices can be added to the existing cluster in a single update operation.
- Stack links can be created only from the new device which is added into the cluster wizard.
- Leader preferences can be changed for each device through edit cluster option.
- Stack link alias and GigaStream alias can be edited for newly created links.
- Stacking mode can be changed from Legacy to Default and vice versa.

**Notes:**

- You cannot change the stacking mode and also add or remove a device simultaneously. Only one task can be performed at a time.

NOTE:

- No option to remove the existing stack links through cluster canvas.
- No option to create links in existing devices.
- Addition and deletion of devices in a single update operation should not be appreciated.
- No option to edit the existing stack link alias and GigaStream alias.

Prerequisites

Standalone devices that have maps cannot be added to cluster if ports used in maps overwrites with the selected ports in stack link table.

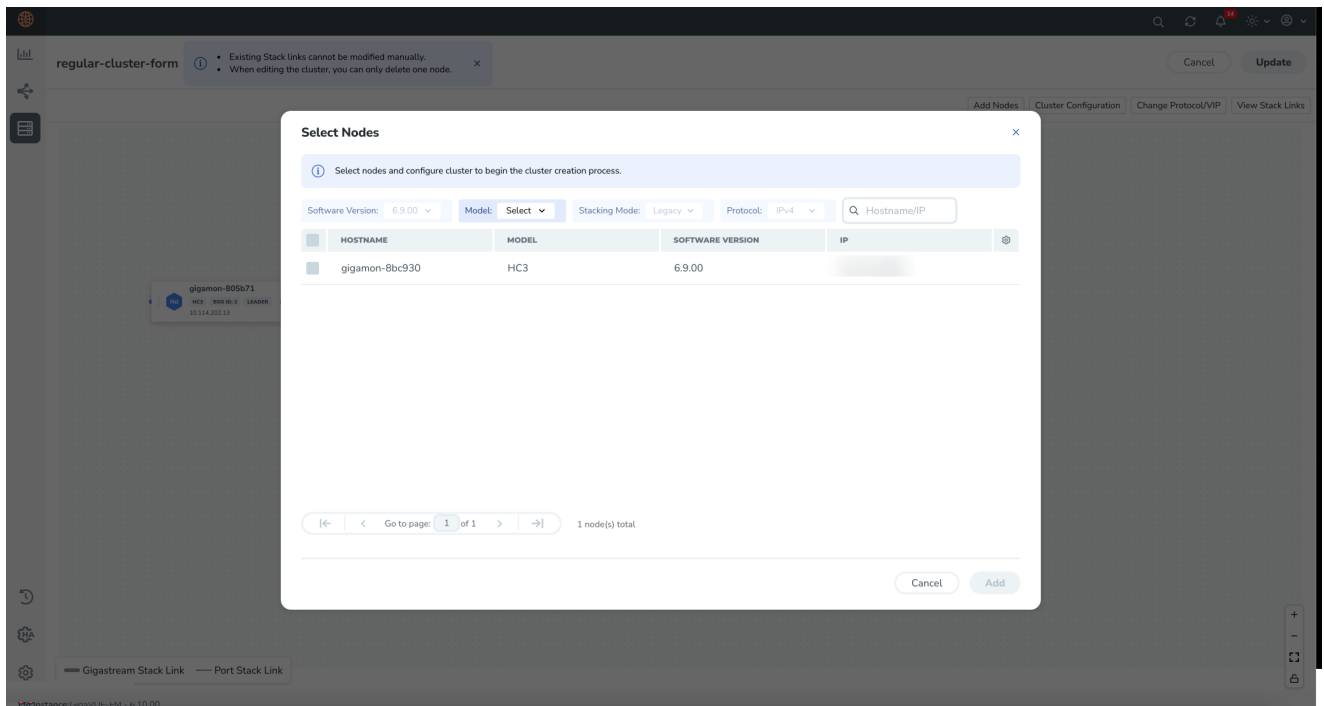
This workflow describes how to add a node to an existing cluster.

- Select a cluster and choose **Actions > Edit cluster**.

The screenshot shows the 'Physical Nodes' table in the GigaVUE interface. The table has columns: CLUSTER ID, HOST NAME, TASK STATUS, NO., ROLE, MODEL, SERIAL NUMBER, SW VERSION, LICENSED, and ATTEMPTED SYN. The 'regular-cluster-form' node is selected. The 'Actions' dropdown menu is open, showing options like Backup, Restore, Reboot, Suppress Alarms, Stop Alarm Suppression, Clear Task Status, Rediscover, Connect Node, Disconnect Node, and Delete. The 'Edit Cluster' option is highlighted.

CLUSTER ID	HOST NAME	TASK STATUS	NO.	ROLE	MODEL	SERIAL NUMBER	SW VERSION	LICENSED	ATTEMPTED SYN.
leaf-spine-test	hc3ls2	—	fca...	Leader	HC3	347	6.9.00	Yes	2025-01-22 1..
leaf-spine-test	ta10ls1	—	fca...	Normal	TA10	1C18	6.9.00	Yes	2025-01-22 1..
leaf-spine-test	ta10ls2	—	fca...	Normal	TA10	1EA6	6.9.00	Yes	2025-01-22 1..
leaf-spine-test	hc3ls1	—	fca...	Standby	HC3	1E4C	6.9.00	Yes	2025-01-22 1..
regular-cluster-form	gigamon-805...	—	10...	Leader	HC3	1B71	6.9.00	Yes	2025-01-22 1..
regular-cluster-form	gigamon-805...	—	10...	Standby	HC3	1BE2	6.9.00	Yes	2025-01-22 1..

- The Edit Canvas displays the existing stack link configuration details in the cluster canvas. Click **Add Nodes** to view the standalone devices.
- Select the required devices from the table in the **Select Nodes** window and click **Add**.



4. In the canvas, draw the links between the newly added device. (**NOTE:** no new link is created for the existing device.)
5. Configure the stack link details in the stack link quick view.
6. Click **Save**.
7. Change the stacking mode as required.
8. Click **Update** to initiate the update process. A confirmation window appears advising that a backup file is generated with the updated traffic configurations. The configurations saved in the backup file must be applied manually to restore the traffic configurations.
9. Click **OK** to run the cluster update.

When the cluster update operation starts, a notification window appears at the right corner of the GigaVUE-FM window to show the status progression of each node, card, GigaStream and stack link.

When the cluster update operation is complete, a notification window confirms the completion of the cluster updates.

10. Click **Go to Cluster** to go to view the cluster overview.

The created GigaStreams appears in the device Port Groups page, and the created stack links appear in the device Stack Links page.

Delete a Node from a Cluster

This workflow describes how to remove a device node from a cluster.

NOTE: Only one device can be removed from the cluster per update operation.

The device should not contain any map configurations in a cluster. Those devices cannot be removed until the maps are present.

1. Select a cluster and choose **Actions > Edit cluster**. Only one device can be deleted from the canvas.
2. To remove a device, click the device to be removed from the canvas and click **Remove Node**.

The removed device will be deleted from canvas.

3. Click **Update** to initiate the cluster-update operation.

The Manage Cluster notification window shows the progress of nodes being removed from the cluster. When the device is successfully removed from the cluster, a notification window confirms the successful deletion of the cluster.

4. Click **Go To Cluster** to go into device overview page and see the cluster details.

How to Change the Leader Preference of a Device

This workflow describes how to change the device's leader preference.

1. Select a cluster and choose **Edit cluster** under Actions.
2. To set the leader preference for a device, click the device and update the **Leader Preference** details in the **Node Configuration** quick view that appears in the side pane.

3. Update the leader preference text box and click **Update** to proceed.

The Update Cluster notification appears to show the progress of the cluster update. When the process is complete, **Cluster updation completed**, message appears in the notification window.

4. Click **Go To Cluster** to go to the device overview page and see the cluster details.

Edit Cluster

The **Edit Cluster** action supports the following types of changes:

- Leader preferences can be changed for each device.
- Multiple devices can be added to the existing cluster in a single update operation.
- Stack links can be created only from a new device that is being added.
- Stack link alias and GigaStream alias can be edited for newly created links.

- Nodes can be removed from an existing cluster, one at a time.
- To enable the Cluster VIP change, the credentials for the new VIP must be added on the [Node Details](#) page in GigaVUE-FM, for a seamless connection of GigaVUE-FM with the cluster.
- You can edit the tag id and tag values associated to nodes and clusters:
 - To edit a configured tag ID and tag value of a node/cluster, you must be an admin user with read and write access.
 - If you replace a single-valued tag value associated to a node, a confirmation message pops-up before replacing the tag value.
- Stacking mode can be changed from Legacy to Default and vice versa.



Notes:

- You cannot change the stacking mode and also add or remove a device simultaneously. Only one task can be performed at a time.

The following options are not supported by the Edit Cluster action:

- There is no option to remove existing stack links through the cluster wizard.
- There is no option to create links in existing devices.
- Addition and deletion of devices in a single update operation is not supported and is not recommended. If you attempt to add and delete devices in a single update operation, you may get unexpected results.
- There is no option to edit the existing stack link alias and GigaStream alias.
- There is no option to rename a cluster directly from GigaVUE-FM. If you rename a cluster using the GigaVUE-OS CLI, the rename does not reflect in the GigaVUE-FM. To rename a cluster that is managed from GigaVUE-FM:

1. Remove the cluster from GigaVUE-FM.
2. Take a backup/log session. Run the `show run` and `show diag detail` commands from the leader node.
3. Disable cluster on all nodes using the command `no cluster enable`. Start with the member nodes and disable the leader node at the end.
4. From leader node, in configure mode, run the command `cluster id <new-cluster-id>` to change the cluster name.
5. Enable the cluster on all nodes. Start with the leader by running the command `cluster enable`. Leader node will push the new cluster name to all the nodes.
6. Once the cluster is up and running, add the cluster back to GigaVUE-FM.

Prerequisites:

You must clear all configurations on a node before adding it to a cluster.

Edit options:

- [Add Nodes to a Cluster](#)
- [Remove Nodes from a Cluster](#)
- [Edit Cluster Parameters](#)

Inband Cluster Management

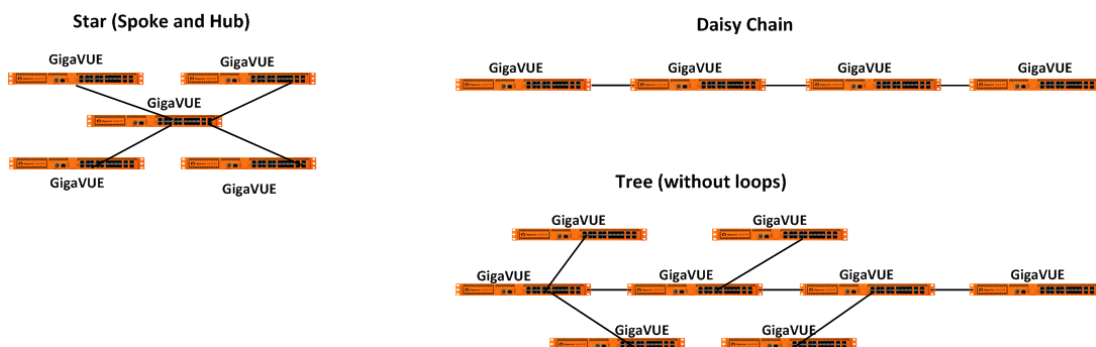
Inband Cluster Management simplifies traditional network management and maintenance by creating a virtual device to manage multiple physical nodes. This simplified approach makes it possible to oversee large networks by defining policies that span across multiple devices. The Inband Cluster Management feature is designed to reduce operational cost and extend coverage by eliminating a dedicated management network.

Inband Cluster Management is supported on all GigaVUE-OS nodes except GigaVUE-TA400, GigaVUE-TA400E, and GigaVUE-HCT.

Inband Cluster Management Topologies

The benefits of Inband Cluster Management are to eliminate the Layer-2 Ethernet network and create a virtual management network through the data path where the data traffic is flowing.

Inband Cluster Management supports multiple topologies that include:



NOTE: Subsets or aggregations of these topologies may be created; however, it is important not to create a loop within these specified topologies.

Loops are typically created in the following scenarios:

- **Two Node Loops** occur between two nodes in a cluster forming two or more stack links and the stack links are not contained in one GigaStream.
- **Multi-Node Loops** occur when multiple nodes form a cluster whereby a link connects between node A and node B, another link connects between node B and node C, and yet another link connects between node C and node A.

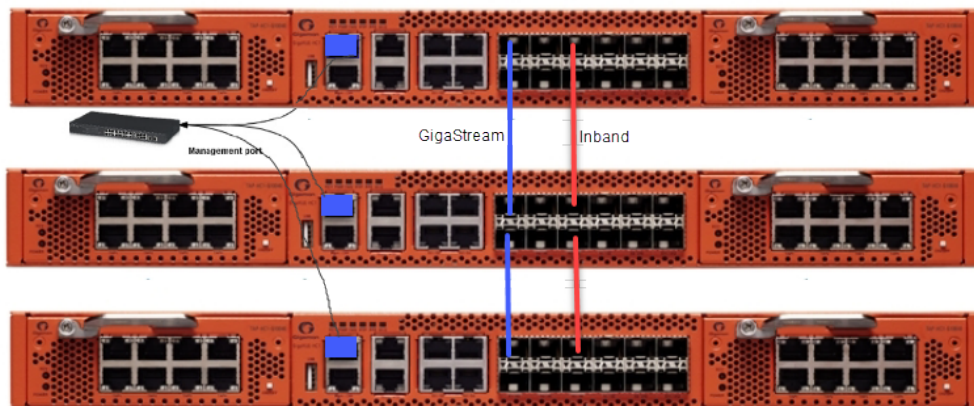
Inband Cluster Management Stack Ports

A common Inband Cluster Management topology is configured between the Layer 2 device's Ethernet management port to a GigaVUE-OS node using a stack port configuration.

Two or more GigaVUE-OS nodes may be directly connected in a one-to-many relationship between physical connections. GigaVUE-OS nodes may also be indirectly connected if there is a path of stack ports between the nodes.

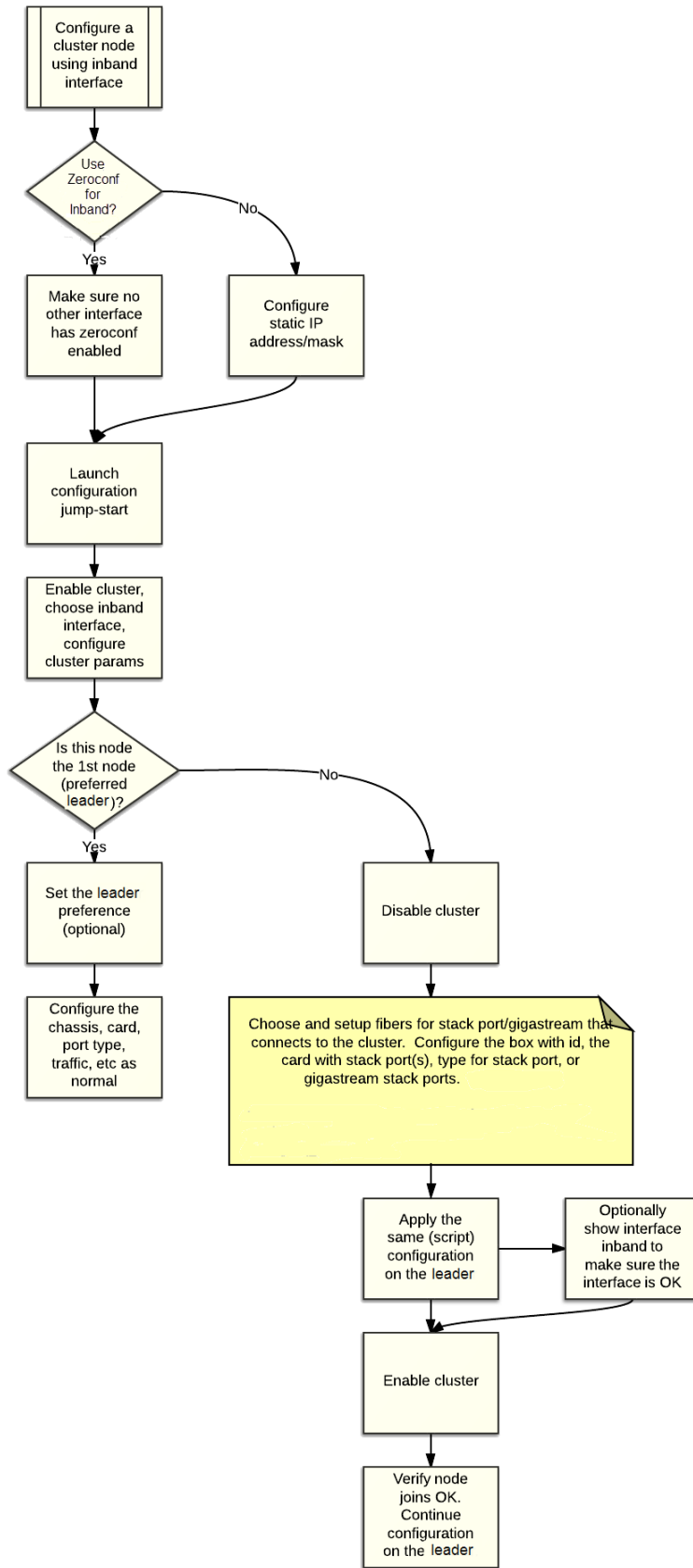
Inband Cluster Management Stack Ports Example

Inband Cluster Management Stack Ports The following figure visually depicts how Inband Cluster Management uses the grouping of stack ports to connect between GigaVUE-HC1 nodes.



NOTE: Ensure that there is a physical connection between the stack ports of the two nodes that are being added to the Inband cluster.

Inband Cluster Management Configuration Flow Chart



Inband Cluster Management Configuration

An interface called "Inband" has been created upon boot-up to ensure backward compatibility with an existing clustered infrastructure. This interface has similar properties and characteristics of a typical Ethernet interface such as eth0.

NOTE: Ensure that there is a physical connection between the stack ports of the two nodes that are being added to the Inband cluster.

Enable Cluster Management for GigaVUE TA Series Nodes

To enable clustering, GigaVUE TA Series nodes require an Advanced Features License. This license can be obtained by contacting Gigamon Sales team. In order to obtain the license for a Gigamon node, have the node serial number available. All licenses are tied to the serial number and cannot be moved.

For licensing the GigaVUE-OS on a white box, users can access the GigaVUE-OS licensing portal and obtain the license key online. In order to generate the license, the following are required: the serial number of the white box, digital footprint, and Gigamon Installation Key (GIK).

Add Nodes to a Cluster

You can manage an existing cluster through GigaVUE-FM by adding nodes to it. The nodes must be standalone nodes that are currently managed by GigaVUE-FM.

When a node joins an existing cluster, all of its existing traffic configuration, including maps, will be replaced by the configuration of the leader.



- If you add a node to a cluster using CLI commands, then the node will be added to GigaVUE-FM only if it is not already managed by GigaVUE-FM. If the node is already managed by GigaVUE-FM, then config sync operation will fail. Refer to the [Rules and Recommendations for Nodes and Clusters](#) section for more details.



- When a new node is added to an existing cluster, if the leader is in secure cryptography mode, then the node joining the cluster will also be changed to secure cryptography mode.

The following is an example of adding nodes to an existing cluster using GigaVUE-FM.

1. From the left navigation pane, go to **Inventory > Physical > Nodes**.
2. Select a cluster and choose **Actions > Edit Cluster**. The Edit Cluster - Canvas appears showing the existing stack link configuration details in the cluster wizard. Standalone devices appear in the Devices pane.
3. Drag the required devices from the Devices pane into the Edit Cluster canvas under the leaf or spine container.
4. Connect the newly added devices to other devices to create stack links.
Click the tip of the node and drag your cursor to the second node tip to create a link. After you create the link, a dotted line will illustrate the connection
NOTE: No new link is created for existing devices; they need to be added manually.
5. Configure the stack link details in the stack link table and click **Save**.
6. Click **Update** to update the configuration.
A Confirmation window appears advising that all traffic configurations will be erased on newly added or removed nodes.
7. Click **OK** to continue.
8. The Manage Cluster update notification window appears showing the status of each update activity on the nodes, cards, GigaStreams and stack links.
9. After the cluster update operation completes, a “Manage Cluster Completed” message appears.
10. Click **Go to Cluster** to view the updated cluster overview

Remove Nodes from a Cluster

You can manage an existing cluster through GigaVUE-FM by removing nodes from it. After a node is deleted from a cluster, it will become a standalone node. FM will continue to manage it.

For nodes leaving a cluster, the username and password of the admin account on the cluster will be used for managing the node after it has been removed from the cluster.

NOTE: If you remove a node from a cluster using CLI commands, then the node is removed from GigaVUE-FM. If you want the node to be managed by the same GigaVUE-FM instance, you must add the node as a new device by providing the credentials.

To remove nodes of an existing cluster using GigaVUE-FM:

1. From the left navigation pane, go to **Inventory > Physical > Nodes..**
2. Select a cluster and choose **Actions > Edit Cluster.**

The Edit Cluster - Canvas appears showing the existing stack link configuration details in the cluster wizard. Standalone devices appear in the Devices pane.

NOTE: Only one device can be deleted from canvas per operation. It can be any device from the cluster.

3. Right-click the device to be removed from the canvas and click **Remove.**
Right click to remove
4. The removed device is deleted from the canvas.
5. Click **Update** to update the configuration.
A Confirmation window appears advising that all traffic configurations will be erased on newly added or removed nodes.
6. Click **Ok** to continue.
7. The Manage Cluster update notification window appears showing the status of each update activity on the nodes, cards, GigaStreams and stack links.
8. After the cluster update operation completes, a “Manage Cluster Completed” message appears.
9. Click **Go to Cluster** to view the updated cluster overview.

Edit Cluster Parameters

When editing a cluster node, you can only edit the cluster leader preference. You can only change the cluster leader preference on one node at a time.

For the leader preference, higher values are more likely to claim the Leader and Standby roles; lower values are less likely.

To edit leader preferences:

1. To set the leader preference for devices, right-click the required device and click the **Edit Details** options button.

2. The Device configuration quick view should appear on the right. Edit the Leader Preference in the text box.
3. Click **OK**.

NOTE: Most of the fields are read-only. You can change the cluster leader preference, as desired. Use preference settings from 10 to 100 for leader, standby, and member roles. Use preference settings from 1 to 9 for normal nodes that are excluded from taking the leader or standby role. GigaVUE TA Series nodes always have a preference of 1.

4. After saving your changes to the nodes, click **Update** to apply the changes to the cluster.

A Confirmation window appears advising that a backup file is generated with the updated traffic configurations. The configurations saved in the backup file must be applied manually to restore the traffic configurations after the cluster is up.

5. Click **Ok** to continue.
6. The Manage Cluster update notification window appears showing the status of each update activity on the nodes, cards, GigaStreams and stack links.
7. After the cluster update operation completes, a “Manage Cluster Completed” message appears.
8. Click **Go to Cluster** to view the updated cluster overview

Check Cluster Status

When a cluster is being created, you can check the status through cluster management events or audit log entries. Refer to the following sections:

- [Cluster Management Events](#)
- [Audit Logs](#)

Cluster Management Events

On the **Events** page, the following event types indicate the progress of the cluster as it is being formed:

- ClusterCreationStarted
- ClusterCreationCompleted
- ClusterCreationFailed

The following events indicate the status of nodes added to or removed from the cluster:

- NodeJoinedToCluster

- NodeFailedToJoinCluster
- NodeRemovedFromCluster
- NodeFailedToRemoveFromCluster

Figure 7 Node Joined to Cluster Event

Audit Logs

The following audit logs indicate the cluster management actions triggered by users from GigaVUE-FM:

- User <username> created cluster <clustername>
- User added device <device IP> to cluster <clustername>
- User removed device <device IP> from cluster <clustername>

Export Nodes and Clusters

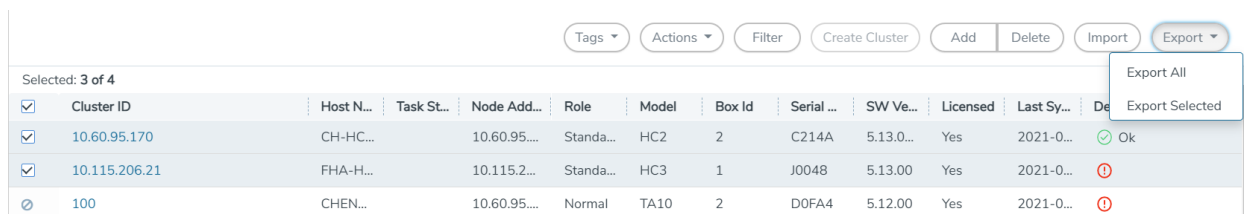
To export the nodes and clusters:

1. On the left navigation pane, go to **Inventory**  and select **Physical > Nodes**.
2. In the physical nodes page, select the nodes and clusters you want to export.
3. Click **Export > Export Selected**.

Click **Export All** to export the nodes in a table format.

To export selected nodes:

1. Click **Select All**.
2. Click **Export Selected** to export only the selected nodes.



Cluster ID	Host N...	Task St...	Node Add...	Role	Model	Box Id	Serial ...	SW Ve...	Licensed	Last Sy...	De
☒ 10.60.95.170	CH-HC...		10.60.95...	Standa...	HC2	2	C214A	5.13.0...	Yes	2021-0...	 Ok
☒ 10.115.206.21	FHA-H...		10.115.2...	Standa...	HC3	1	J0048	5.13.00	Yes	2021-0...	
☐ 100	CHEN...		10.60.95...	Normal	TA10	2	D0FA4	5.12.00	Yes	2021-0...	

However, the member nodes will not get downloaded as they do not get selected. To select and download the member nodes:

1. Enable **Device Level Tagging** option under the Tags menu.
2. Click **Export Selected** to export the selected nodes, including the member nodes.

				Tags ▾	Actions ▾	Filter	Create Cluster	Add	Delete	Import	Export ▾
Selected: 4 of 4				Add Delete Device Level Tagging ⓘ ☒ Export Tags for Selected Export Tag Resources for Selected							
Cluster ID	Host N...	Task St...	Node Add...								
☒ 10.60.95.170	CH-HC...		10.60.95...								
☒ 10.115.206.21	FHA-H...		10.115.2...								
☒ 100	CHEN...		10.60.95...								

Serial ...	SW Ve...	Licensed	Last Sy...	Device ...	T...	
214A	5.13.0...	Yes	2021-0...	Ok		
048	5.13.00	Yes	2021-0...			
0FA4	5.12.00	Yes	2021-0...			

Problems with SCP?

After upgrading GigaVUE-FM to a new release, under some circumstances you may find that a previously-managed H Series node no longer accepts SCP commands to backup or restore configuration files. This can happen when the SSH keys in use change, causing a mismatch between the keys stored on the H Series node and those presented by GigaVUE-FM. Use the following steps on the H Series node to remove the GigaVUE-FM server from the H Series node's list of addresses, resolving the issue:

1. Log in to the affected H Series node and switch to Configure mode.
2. Use the **ssh client user admin known-host?** command to discover the IP address for the GigaVUE-FM server. For example:
(config) # ssh client user admin known-host ? 10.150.100.23 10.150.100.77
3. The question mark (?) instructs the H Series node to list the known ssh clients. From the list of IP addresses returned by the CLI, identify the one belonging to GigaVUE-FM and remove it using the **remove** argument. For example, if 10.150.100.77 is the GigaVUE-FM server's IP address:

(config) # ssh client user admin known-host 10.150.100.77 remove

Return to GigaVUE-FM and attempt the configuration backup again.

Events

The Events page displays all the events that occur in the physical nodes or clusters. An event is an incident that occur at a specific point in time. Examples of events include:

- Device status change
- Stack image install status
- Fan tray changed

From the left navigation pane, go to **Inventory > Physical > Nodes..** On the Physical Nodes page click **Events** on the left navigation pane.

For information about the parameters for each event, refer to the “*Event Parameters*” section in the *GigaVUE Administration Guide*. For filtering the events, refer to the “*Filter Events*” section in the *GigaVUE Administration Guide*.

NOTE: The events can be purged or archived only from the Events page. For more information, refer to the “*Archive or Purge Event Records*” in the *GigaVUE Administration Guide*.

Alarms

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. Examples of alarms include:

- High or low port utilization
- High or low CPU utilization
- High exhaust temperature

The alarms broadly fall into the following categories: Critical, Major, Minor, or info.

Audit Logs

With Audit Logs, changes and activities that occurred in the physical nodes or clusters due to user actions can be easily tracked for auditing. The logs can also be further filtered to view specific information.

For information about the parameters in the audit log page, refer to the “*Overview of Audit Logs*” section in the *GigaVUE Administration Guide*. Filtering the audit logs allows you to display specific type of logs. For more information, refer to the “*Filtering Audit Logs*” section in the *GigaVUE Administration Guide*.

Search for Specific Nodes Using Keywords

The filter option provides a way for the users to narrow down the display using certain keywords such as Standalone, Clusters, H Series and others. As you click on the Filter button, you will see the quick view window pop-up.

The Filter quick view provides you filter criteria for your search. These options are available in the drop down menu under Criteria. You can further narrow the options using the Model, Software Version #, Cluster ID, Host Name, DNS Name, or Node IP. You are not required to fill in all these options to narrow your search. As you select these options in the quick view, you will see the options narrowing in the main window.

To clear or revert the search, do any of the following:

- To clear a part of the search, use backspace to clear the search entry and re-type a new option.
- To clear all the search criteria, use the Clear button on the top of the quick view window.
- To revert to the main window with the new searches, click on the **X** of the quick view window.

To revert to all nodes visible, you can use the clear filter option on top of the main window or the clear option in the quick view window. When no filters are in place, this option will no longer be visible in the main window.

Search for Ports on a GigaVUE Node

When viewing a node from GigaVUE-FM, you can use Port List Filter feature to display only certain ports that match specified criteria, such as only those ports that are used in a map.

To use the port list filter:

1. Select a physical node from the **Physical Nodes** page and then select the node to view.
2. Go to **Ports > Ports > All Ports**.
3. To filter the ports, click **Filter**. The Filter quick view is displayed.
4. Specify the criteria of the ports you want to filter.

The criteria that you can use to filter the port list is as follows:

Criteria	Description
Box/Slot ID	Display only those ports that match the specified box and slot IDs.
Port Alias	Display port with the specified alias.

Criteria	Description
Port ID	Display ports with specified number in the port ID. For example, if you specify 3 the result will also display ports that include the number 3, 13, 23, 30, and so on.
Type	Display ports with the specified port type. Select one of the following: ▪ Network ▪ Tool ▪ Inline Network ▪ Inline Tool ▪ GigaSMART ▪ Hybrid ▪ Stack
Port Used in Map(s)	Display ports based on their usage in maps. The possible selections are: ▪ All — display all ports either unused or in use by maps. This is the default. ▪ In Use — display ports that are in use by any map. ▪ Unused — display ports that are not use by any maps.
Admin Status	Display ports based on their current admin status. The possible selections are: ▪ All — display ports with a status of Enabled or Disabled. This is the default. ▪ Enabled — display ports with admin enabled. ▪ Disabled — display ports with admin disabled.
Speed	Display ports with the selected port speed. The port speeds available depend on the node.
Transceiver Type	Display ports with the selected transceiver type. The transceivers available selection depend on the type of transceivers connected to the ports.

To remove the filter selections, click **Clear**.

After the filter is applied, the Ports page displays only the ports that correspond to the selected filters and shows the total number of ports that meet the criteria. To clear the filters, select **Clear Filter**. The figure below shows the Port pages with two ports that correspond to the current filters: Network Type and Admin Status Enabled.

Total Filtered Ports : 2 Clear Filter					
☐	↑ Port Id	Alias	Type	Speed	Admin Enabled
☐	10/1/x1		N	10G	✓
☐	10/1/g1	1G	N	1G	✓

Overview Page

The **Overview** page displays general information on the specific H Series node, which includes System, Ports, Maps, and Traffic information.

GigaVUE-FM notifies you with a message when a node is down. Click **Proceed** to continue viewing the overview dashboard even when the node is unreachable.

Systems Information

Systems information is displayed on the System widgets.

The Systems widget displays general information about the specific device that you selected from the drop-down list at the top of the widget. If the system is a cluster, you can select a device in the cluster to display on the widget. This widget gives you a quick status if any issues are present in any of the device's components through color indicators; green (running), amber (warning), or red (alert).

NOTE: Ensure that all the nodes and clusters have a Box ID defined. If the Box ID is missing, the Systems widget may not display any information relating to the node.

NOTE: Red alert appears for cards not present.

Field	Description
Host Name	The host name of the box.
Hardware	The hardware type, (for example, GigaVUE-TA1).
Software	The version of the software running on the device.
Memory	Shows the amount of used and free memory.
Load Average	The average load on the system over the last 1 minute, 5 minutes, and 15 minutes.

Field	Description
	NOTE: When a new device is added to GigaVUE-FM, it takes one stats cycle for the average load value to be reflected in the GigaVUE-FM GUI.
Cards	Displays all slots for the specific hardware type including its slot number and the type of card it contains or not. Note: When you hover over the card slot, the temperature is displayed.
Fan Trays	Indicates that the Fans are On or Off.
Power Supply	Indicates that the power supply is On or Absent. NOTE: When one or more power supply units are down, red alert is displayed.

Failure to Authenticate

To view a physical node in the Dashboard System pane, your login credentials must have the appropriate permissions. Otherwise, GigaVUE-FM shows an error message.

There are two possibilities that caused a user authentication error:

- The login user credential for GigaVUE-FM is not “**admin**”.
- The password associated with the login user name for GigaVUE-FM is different for the physical device.

NOTE: When a “non-admin” user goes to Physical Nodes page, they are able to view displayed physical nodes with the status as Green, Amber or Red, this is because the physical node information is captured using the default “admin” user role.

Ports Information

The Overview page displays widgets that provide port information for the number of ports down, the number of ports with packet drops, and the number of over utilized receiving (Rx) ports and transmitting (Tx) ports. The ports widgets default to displaying a counter. Clicking on the icon in the upper right-hand corner displays the information as a table. The Ports with Packet drops and Over-Utilized Ports widgets are similar.

Traffic

The Traffic widget shows most-utilized ports and ordered by traffic count. Each displayed port is labeled with its location, whether it is a transmitting or receiving port, and its percentage of utilization.

NOTE: The Traffic pane is view-only. It reflects traffic activity with port ID at the time of discovery and does not immediately refresh.

Workflows

The Workflows page provides wizards for creating maps. These wizard step you through the work flow to make sure you configure all of the components necessary for configuring out-of-band and inline maps for traffic flow monitoring. The workflows keep track of each step so that you can stop and then return to where you left off in the workflow. However, you can only work on one workflow at a time.

Overview of Workflows

[Table 2: Map Types and Map Wizards](#) describes the maps that you can create with the wizards.

Table 2: Map Types and Map Wizards

Map Type	Map Wizard	Description
Out-of-Band maps	Map with rules	Walks you through the steps to select source and destinations ports, then create a Regular By Rule map with those ports.
	Pass-all map	Walks you through the steps to select source and destinations ports, then create a Pass All map with those ports.
	Collector map	Walks you through the steps to select source and destinations ports, then create a Collector map with those ports.
Inline maps	Map with rules	Walks you through the steps to select the destination and source, then use them in an Inline By Rule map. If the Inline Networks or Inline Network Groups have not been created yet, you can create them from the wizard. The wizard selects Symmetric for Traffic Type.
	Pass-all map	Walks you through the steps to select the destination and source port, then use them in an Inline Pass All map. If the Inline Networks or Inline Network Groups have not been created yet, you can create them from the wizard. The wizard selects Symmetric for Traffic Type.

Map Type	Map Wizard	Description
	Collector map	Walks you through the steps to select the destination and source ports, then use them in an Inline By Rule map. If the Inline Networks or Inline Network Groups have not been created yet, you can create them from the wizard. The wizard selects Symmetric for Traffic Type.
	Asymmetric Inline map	Walks you through the steps to select the destination and source ports, then use them in an Inline Pass All map. The source port must be an Inline Network port. The destination port must be an Inline Tool, an Inline Tool Group, or an Inline Serial Tool Group. If the Inline Networks or Inline Network Groups have not been created yet, you can create them from the wizard. The wizard selects Asymmetric for Traffic Type.
Basic out-of-band GigaSMART maps:	Map with GigaSMART Apps	Walks you through the steps to select a GigaSMART Group, GigaSMART operation, select the source and destination ports, and then create a Regular By Rule map. The wizard allows you to create the GigaSMART Group and GigaSMART operation if they do not already exist.
	First level map	Walks you through the steps to select or created the source port and select a or create a virtual port for the destination port, and then create a First Level By Rule map.
	Second level map	Walks you through the steps to select or created the virtual port for the source port and select a or create the port for the destination port, and then create a Second Level By Rule map.
Advanced out-of-band GigaSMART maps	Map with NetFlow	Walks you through the steps to select or create an IP interface; a NetFlow exporter, records, and monitor; a GigaSMART Group and Operation, source ports; and then created a Regular by Rule map.
	SSL-based map	Walks you through the steps to create or select a GigaSMART Group, configure SSL, create or select a GigaSMART Operation, and then create a Regular By Rule map.
	Map with ASF	Walks you through the steps to create or select a GigaSMART Group, virtual port, and GigaSMART Operation; configure GigaSMART Application Session Filter; and create the First and Second Level maps needed for implementing an ASF solution.

How to Use Workflows

To start a workflow, click on one of the links, such as **Map with Netflow**. When you click on the link, the Workflow page is displayed. The Workflow panel on the right shows the tasks in the workflow, indicating the current task.

While using workflows, you can only work on one workflow at a time. Also, you cannot roll back changes made to a node after canceling a workflow.

A task in the workflow allows you to select an item or create the item if one does not exist. For example, a GigaSMART Group needs to be selected if one does not exist. In this case, click **Create**. Clicking Create takes you to the GS Group configuration page. Configure the GigaSMART Group and click **Save**.

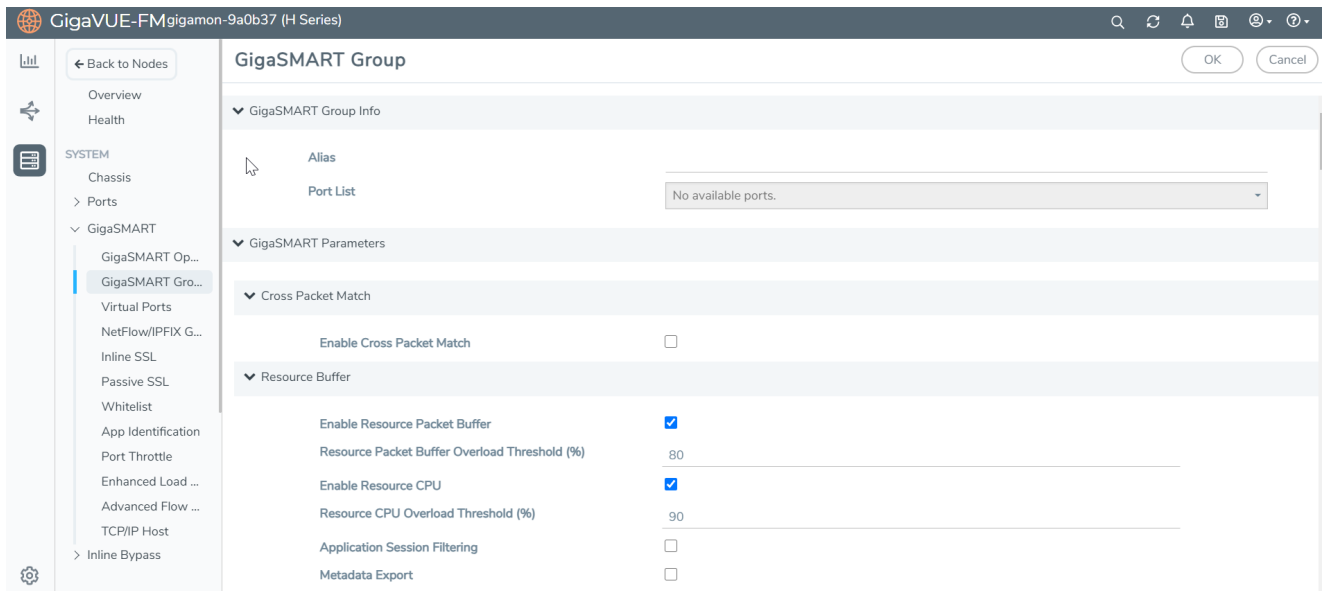


Figure 8 GS Group Configuration in Workflow

After saving the configuration, the Workflow moves to the next task and the Workflow panel indicates which tasks have been completed.

You can select a task in a different order than shown in the Workflow panel. For example, you can go to the NetFlow Monitor task. After completing the task, the Workflow returns you to the GS Group configuration page with the Monitor field completed.

Workflow allows you to leave the current workflow and return at anytime during a GigaVUE-FM session. The **In Progress** panel indicates the current workflow and the Workflow panel indicates the completed tasks. [Figure 9 Workflow in Progress](#) shows an example of workflow in progress. You can abandon a workflow by clicking the red x in the **In Progress** panel.

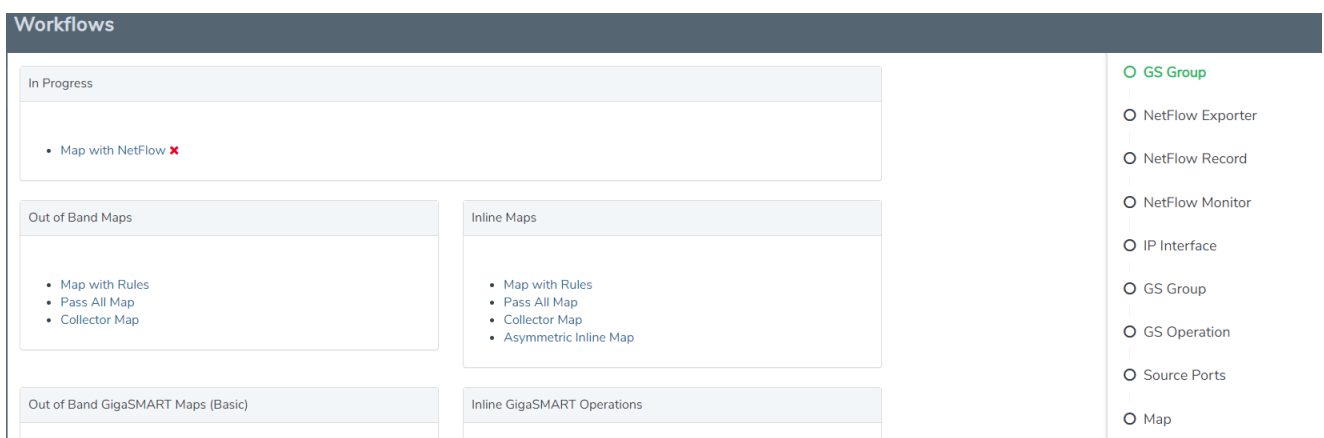


Figure 9 Workflow in Progress

When a workflow is completed, a page displays providing you with several choices for the next task. For example, when the Map with Rules workflow is completed, you can go to creating a collect map by clicking the **Create a Collector Map**, return to the Workflow page by clicking **To Work Flows**, or go to the Maps page by clicking **To Maps**.

Chassis Table View

When viewing the Chassis Table View managed from GigaVUE-FM, the Table View includes environment information about the chassis.

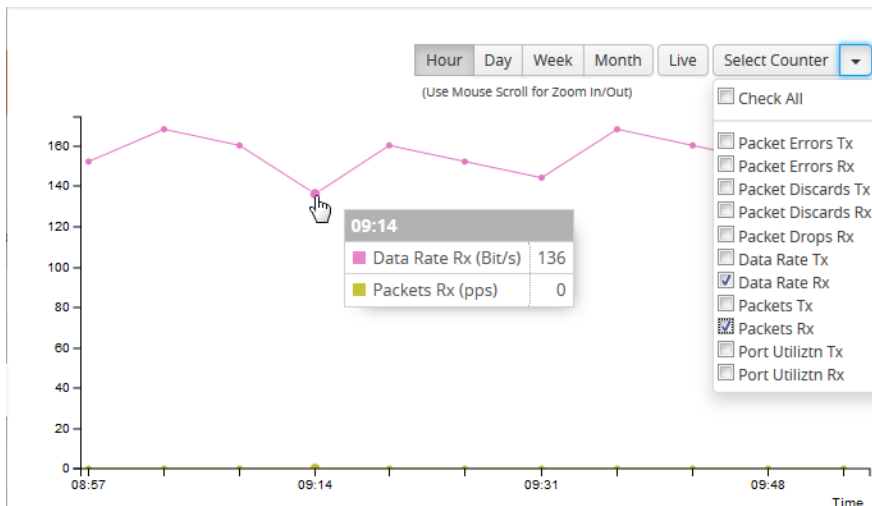
The Table View provides the following information about the chassis and its components:

Chassis Information	Description
Properties	Provides information about the chassis.
Cards	Describes the cards installed in each slot of the chassis, including its current status.
Environment	Provides temperature and voltage information about the chassis.
Power Supplies	Describes the power supplies installed in the chassis, including their current status.
Fan Trays	Describes the fan trays installed in the chassis, including their current status.
Fan RPM	Provides the current RMP of the each fan.

NOTE: When a new device is added to GigaVUE-FM, it takes one stats cycle for the following field values to be reflected in the GigaVUE-FM GUI: Environment, Power Supplies, Fan Trays, Fan RPM.

Live Graphing

When viewing ports on a node running GigaVUE-OS 4.6 or later from GigaVUE-FM, you can select to see the graph data display in real time by clicking **Live**. This changes the updating of the information in the graph from the default to every 10 seconds. You can also select the data to display on the graph by selecting an option from the Select Counter list. [Live Graphing](#)The following figure shows an example, where Live is selected and the Data Rate Rx and Packets Rx counters are selected.



Safe and Limited Modes

Starting in GigaVUE-OS software version 4.7, safe and limited modes are introduced to the cluster environment and standalone nodes.

During clustering operations, in rare scenarios, there can be unrecoverable system errors that can potentially put the cluster or the clustered nodes into unsafe or unstable states. Once in such a state, additional operations or configuration changes can cause the node to crash, the cluster to deform, and the data traffic to be impacted. For example, due to a node attempting to rejoin a cluster, a chassis can end up in a reboot loop. In previous software versions, there was no way to prevent entering the loop.

These modes provide notification, stop further operations from being performed, and give you time to troubleshoot and plan the recovery of the cluster or of any node in the cluster or standalone node.

Two modes are supported. The first is called safe mode and is triggered when the node detects unrecoverable errors, but the existing flow maps are not impacted. The second is called limited mode and is triggered when the node detects continuous system reboots. In this mode, the node will become standalone and only basic configuration will be allowed.

When a cluster is in safe mode, GigaVUE-FM displays a Safe Mode banner and message.

Safe Mode

A node enters safe mode when there are unrecoverable errors. Any node in a cluster can enter this mode.

Examples of unrecoverable errors are when there are inconsistencies between the system and the running configuration or when the cluster configuration did not merge properly with the existing configuration. A node will automatically enter safe mode.

As part of merge error recovery, nodes joining a cluster are automatically restarted so the merge error can be fixed.

When a node is in safe mode:

- The node displays a banner indicating it is in safe mode.
- An SNMP trap is sent to notify the user when the mode changes
- Traffic provisioning is not allowed on the affected node. Any other configuration remains as is.
- Configured traffic continues to be forwarded.
- If the standby node in the cluster is in safe mode, it can still become the leader if the current leader fails or switches over, but the database on the standby node may not be in sync, so it is not recommended to continue in that state. Instead, take immediate action to recover the node.
- In safe mode, the node does not process any incoming traffic configuration from the cluster leader.

When a node is in safe mode and you try to do any operations that are not allowed in safe mode, the UI displays the following message:

The system has restricted provisioning in safe mode. Contact Gigamon Support on how to troubleshoot and recover from safe mode.

Also, hovering over the status bubble of the nodes on the Physical Nodes page in GigaVUE-FM displays a message that the node is in Safe Mode.

To exit safe mode, reload the node.

Limited Mode

A node automatically enters limited mode when it detects repeated system crashes.

When a node is in limited mode:

- The node displays a banner indicating that it is in limited mode.
- An SNMP trap is sent to notify the user when the mode changes.

- Only basic system provisioning is allowed. Traffic provisioning is not allowed. Only commands that are related to image download, installation, next boot, and reboot are allowed.

Limited mode is triggered when there are three (3) failures/system crashes within 15 minutes. In limited mode, the cluster configuration is ignored. No cluster configuration or GigaVUE-OS configuration is accepted when the node is in limited mode.

When a node is in limited mode, a Limited Mode banner displays in GigaVUE-FM.

Enable SNMP Trap for Safe Mode and Limited Mode

Use the following steps to configure a notification that will be sent to all configured destinations when a node in the cluster changes from operational mode to safe mode or from operational mode to limited mode

The safe mode and limited mode capabilities are enabled through the SNMP trap event Operational Mode Change. To enable the trap on a node, do the following:

1. From the left navigation pane, go to **Inventory > Physical > Nodes**.. On the Physical Nodes page, select the node you want to configure.
2. Select **Settings > Global Settings > SNMP Traps**.
3. Click **Trap Settings**.
4. On the Edit SNMP Traps Settings page, select **Operational Mode Change**.
5. Click **Save**.

When the cluster leader enters safe mode, the SNMP trap will be sent and the leader will be identified as the local node in the trap.

When a node in a cluster enters safe mode, the SNMP trap will be sent and the node will be identified as the local node in the trap. In addition, a notification will be sent to the cluster leader. The node that entered safe mode will be identified by its box ID in the notification to the leader.

Log messages also provide information. The following is a sample log:

```
Jun 8 13:46:27 GC-TA10-N6 mgmtd[2400]: [mgmtd.INFO]: SAFE mode: Merge error detected !!  
Triggering SAFE mode ...
```

Collect Information for Technical Support

Collecting the following information can help Technical Support:

- sysdumps/debug dumps for all nodes in the cluster
- sysdumps for nodes that observed a crash entering safe or limited mode
- debug dumps for nodes that did not observe a crash
- gslogs for application information
- console logs
- CLI histories
- CLU or GigaVUE-FM screen captures
- SNMP captures

Manage Not-reachable Nodes in Cluster

GigaVUE-FM allows you to add and manage standalone nodes and clusters as described in [Manage GigaVUE® Nodes and Clusters](#). Occasionally, the nodes in a cluster may become unreachable due to various reasons.

Until software version 6.0.00, when a node in a cluster managed by GigaVUE-FM is removed from the cluster using the `no cluster enable` CLI command, or when any node becomes unreachable to the cluster leader due to other reasons such as power outage, the cluster leader marks the operational status of the node as 'Down' in CLI. After the next config sync cycle, GigaVUE-FM does not manage the node anymore. An event is triggered and corresponding alarms are raised. When a node in a cluster managed by GigaVUE-FM is removed using the GigaVUE-FM GUI (Edit Cluster page), GigaVUE-FM manages the node as a standalone node. The Operational Status of the node is marked as 'Down' in CLI.

When a cluster with one of the nodes with operational status 'Down' is added to GigaVUE-FM, GigaVUE-FM removes the node from the cluster and no longer manages the node. If the node comes up, the node is added to GigaVUE-FM, only if the node is not already managed by GigaVUE-FM. Otherwise, you must manually:

- Add the node as a stand-alone node in GigaVUE-FM
- Add the node to the cluster

Therefore, it is important to keep track of the events and alarms to know about the nodes that have been removed from the cluster, especially in large deployment scenarios.

Starting from software version 6.1.00, when a node become unreachable, the nodes are designated with the following operational statuses (depending on the reason):

Reasons for node becoming unreachable	Operational Status
Nodes in cluster is removed intentionally from the cluster: - Using the no cluster enable CLI command. - Using GigaVUE-FM GUI (by navigating to the Edit Cluster page)	Left
Nodes is offline due to issues such as power outage, management interface being down, or crash.	Not-reachable

GigaVUE-FM manages the not-reachable member nodes as part of the cluster and does not remove the nodes from the cluster, that is, GigaVUE-FM manages the not-reachable nodes in faulty/offline state. This allows easy management of the not-reachable nodes. GigaVUE-FM displays clusters with not-reachable nodes in the Physical Nodes page and in the Chassis page.

The screenshot shows the 'Physical Nodes' page in the GigaVUE-FM GUI. The table lists various nodes and clusters. The 'testvm1' cluster is selected, and a tooltip indicates it is 'Device not-reachable from cluster testvm1'.

Cluster ID	Host Name	Node Address	Role	Model	Bo...	Se...	SW Version	Lic...	La...	Health	T...
10.115.38.70	FM-TA200	10.115.38.70	Standalo...	TA200	20	RO...	6.1.00	Yes	20...	Ok	0
10.115.206.148	gigamon-a0f552	10.115.206.148	Standalo...	HC1	2	HF...	5.13.00	Yes	20...	Ok	0
ElzCluster	fm-hermes-hc2-23	10.115.47.45	Leader	HC2	23	CA...	6.1.00	Yes	20...	Ok	7
ElzCluster	fm-juno-ta200d-16	10.115.46.109	Normal	TA200	16	TE...	6.1.00	Yes	20...	Ok	7
ElzCluster	ElzCluster__24	ElzCluster__24	Unknown	UNKN...	24	CB...	NA	Yes	20...	Device not-reac...	7
testnormal1	Fm-HC2p	10.115.38.3	Leader	HC2	22	C3...	6.1.00	Yes	20...	At least 50 % of ...	9
testnormal1	Fm-HC2	10.115.38.14	Normal	HC2	2	C0...	6.1.00	Yes	20...	Ok	9
testnormal1	FM-HC3v2	10.115.38.85	Standby	HC3	3	J0...	6.1.00	Yes	20...	Ok	9
testvm1	FM-HC31	10.115.206.70	Leader	HC3	2	J4...	6.1.00	Yes	20...	Ok	6
testvm1	FM-HC32	10.115.207.94	Standby	HC3	3	JB...	6.1.00	Yes	20...	Ok	0
testvm1	FM-HC21	10.115.206.223	Unknown	HC2	1	C7...	6.1.00	Yes	20...	Device not-reac...	0

To view only clusters with not-reachable node from the Physical Nodes page:

1. Navigate to the Physical Nodes page.
2. Click the **Filter** button.
3. Scroll down and enable the following toggle option to view only the clusters with

not-reachable nodes:

Show only the clusters with not-reachable nodes

Refer to the following notes:

- If the node is already managed by GigaVUE-FM, then the Host Name and IP Address of the not-reachable nodes is displayed in the GUI.
- If you add a cluster with not-reachable node to GigaVUE-FM, then the IP address and Host Name of the not-reachable node will be displayed in the following format: **clusterid_boxid**. The IP address of the not-reachable node will get updated once the node becomes reachable. Role of the not-reachable node will be 'Unknown'. Software Version and other properties will be displayed as NA.

Rules, Notes, and Limitations

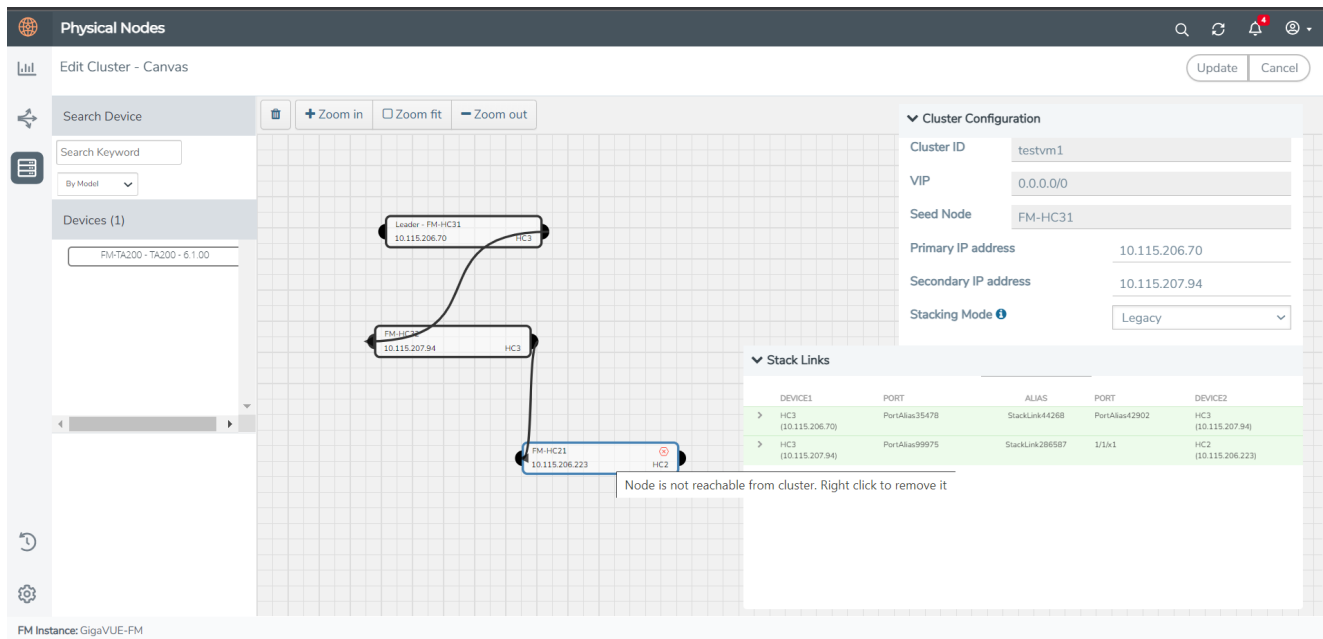
Refer to the following rules, notes and limitations:

- You can only remove the not-reachable member node from the cluster. You cannot perform any other write operation on the not-reachable node.
- You can configure Email notification (instant or digest) for the events triggered for the not-reachable nodes. Refer to the [Configure Email Notifications](#) section in the GigaVUE Administration Guide for details.
- The not-reachable member nodes are captured in the physical and Fabric Health Analytics dashboards.
- You can import and export clusters with not-reachable member nodes.
- You must perform a factory reset of the not-reachable nodes when:
 - removing a not-reachable node from a cluster and adding it to a new cluster
 - removing a not-reachable node from a cluster and adding it as a leader node of another cluster
- When rebooting a cluster with not-reachable nodes, GigaVUE-FM prompts you to skip the not-reachable nodes. Reboot will not proceed until you skip the not-reachable nodes.

Remove Offline Chassis

GigaVUE-FM allows you to remove the not-reachable nodes from the cluster. To remove the non-reachable nodes:

1. From the Physical Node page, select the required cluster from which you want to remove the not-reachable nodes.
2. Select **Actions > Edit Cluster**. The Edit Cluster - Canvas appears.
3. Right click on the not-reachable node, and click **Delete**.



To perform this action:

- You must be a read-write user with Infrastructure Management category.
- You must remove the associated ports and map configuration of the not-reachable member nodes before removing the nodes from the cluster. Without doing this, GigaVUE-FM does not allow you to remove the nodes.

Alarms and Health Status of Not-reachable Nodes

The following alarms are triggered in the Alarms page depending on the status of the not-reachable nodes:

State	Alarm
Member node in a cluster is not-reachable to the cluster leader. The alarm is cleared when the member node is reachable.	Cluster Member Not-Reachable
Member node is reachable by the cluster and added to the same cluster	Cluster Member Online

When a not-reachable node becomes part of another cluster:

- The config-sync operation fails.
- The cluster to which the node originally belonged to displays the member node as not-reachable.
- The health status of the new cluster becomes red.

You are responsible for removing the not-reachable member node from the cluster to which it originally belonged to only after which the config sync operation will succeed.

Upgrade Cluster with Not-reachable Nodes

When upgrading a cluster from software version 6.0.00 to 6.1.00:

Member nodes with Operational Status as Down: Cluster upgrade is successful in both CLI and GigaVUE-FM. After the upgrade, the operational status of the member nodes is *left*.

While upgrading a cluster from software version 6.1.00 to higher, if the cluster contains:

- **Member nodes with Operational Status as Not-reachable:** Cluster upgrade will not proceed until the not-reachable nodes are skipped. Refer to the following table for the various scenarios:

Type of Upgrade	Cluster State	Upgrade Status
Immediate Upgrade	All nodes in the cluster are reachable	Upgrade will succeed.
	One or more nodes in the cluster are not-reachable	Enable the "Skip not-reachable nodes to upgrade" check-box for the upgrade to succeed.
Scheduled Upgrade	All nodes in the cluster are reachable.	Upgrade will succeed.
	All nodes in the cluster are reachable. However, it is possible for the nodes to go to not-reachable state at the scheduled upgrade time.	Enable the "Skip not-reachable nodes to upgrade" check-box for the upgrade to succeed.
	One or more nodes in the cluster are not-reachable	Enable the "Skip not-reachable nodes to upgrade" check-box for the upgrade to succeed.

NOTE: After the cluster upgrade operation is completed, you must ensure to upgrade the not-reachable nodes to the required software version. Failure to do so will result in version mismatch conflict.

For GigaSMART Signature image upgrade, you must skip the not-reachable nodes for the upgrade to succeed.

Type of Upgrade	Cluster State	Upgrade Status
Immediate Upgrade	All nodes in the cluster are reachable	Upgrade will succeed.
Scheduled Upgrade	One or more nodes in the cluster are not-reachable	Enable the "Skip not-reachable nodes to upgrade" check-box for the upgrade to succeed.

Backup and Restore of Cluster with Not-reachable Nodes

During GigaVUE-FM backup and restore operation, if not-reachable nodes are part of the cluster:

- The not-reachable member nodes are also backedup. On restoring the backup file, the not-reachable member node will be restored to its original state.
- During the next config sync cycle after restore, GigaVUE-FM updates the status of the not-reachable member nodes and the cluster.

For cluster backup and restore operation, refer to the following table:

Operational State During backup	Operational State During Restore	Final Operational State
All nodes are in 'up' state	Few nodes are in 'left' or 'not-reachable' state	Operational status of the nodes in 'left' or 'not-reachable' state will remain as 'left' and 'not-reachable', respectively.
	Few nodes are removed using no chassis box id command	Operational status of the removed nodes is configured as 'left'.
Few nodes are in 'left' or 'not-reachable' state	Same state	No change.
	Few nodes are removed using no chassis box id command	Operational status of the removed nodes is configured as 'left'.
	Some nodes come up	Operational status of the nodes will show as up.

Multi-Path Leaf and Spine

This chapter describes the leaf and spine architecture with multiple paths for achieving high availability in a cluster environment. Refer to the following sections for details:

- [Introduction to Multi-Path Leaf and Spine](#)

- [Configuration Overview](#)
- [Leaf-Spine Cluster Deployment](#)

NOTE: Refer to [Regular Cluster Formation Workflow](#) for how to use the Regular Cluster workflow.

Introduction to Multi-Path Leaf and Spine

The leaf and spine architecture is a two-layer architecture used for network aggregation. There are two kinds of nodes in this architecture, as follows:

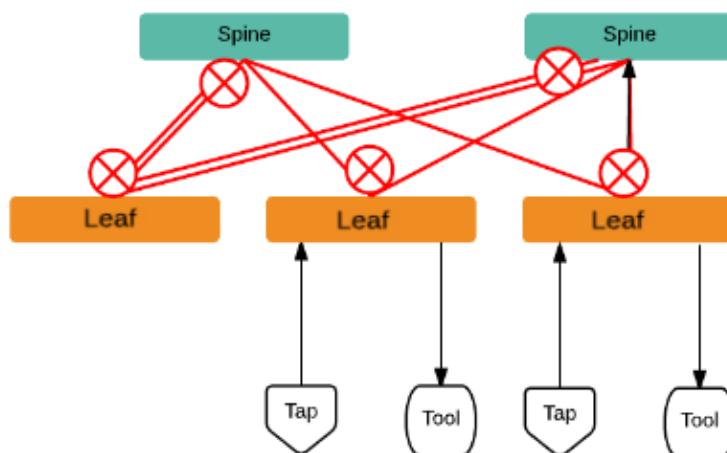
- leaf nodes, which are edge nodes and can also have TAPs or tools attached to them
- spine nodes, which are the nodes to which the leaf nodes attach

NOTE: The connections between leaf node and spine node is through

- stack GigaStreams configured on both the leaf and the spine nodes and
- spine links configured on the leaf side.

With multiple paths between the nodes in a cluster, the leaf and spine architecture protects against failures, such as stack link or spine node failures. In the event of a failure, the traffic fails-over to the other available path.

In this architecture, each leaf node connects to every spine node. This forms a mesh between the leaf and spine nodes. However, no leaf node directly connects to another leaf node and no spine node directly connects to another spine node. An example of a spine and leaf architecture is shown in the following figure.



In a cluster, the number of leaf nodes is typically greater than the number of spine nodes. In the above figure, there are three leaf nodes and two spine nodes. The leaf nodes aggregate to a fewer number of spine nodes.

The spine nodes are generally GigaVUE® TA Series nodes, such as GigaVUE-TA100, while the leaf nodes are GigaVUE® HC Series nodes, such as GigaVUE-HC1 and GigaVUE-HC3, which places the traffic intelligence at the edge.

The figure shows TAPs or tools connecting to the leaf nodes, and the leaf nodes connecting to the spine nodes. Note that TAPs or tools do not connect to the spine nodes.

Instead of one leaf node connecting to one spine node with a single link, in this architecture there are multiple links from the leaf nodes to the spine nodes. The leaf nodes connect to the spine nodes through at least two paths. Some leaf nodes with higher capacity, such as GigaVUE-TA100, can have more paths, as shown by double red lines in the figure.

Traffic between ports on a leaf node will be local to that leaf node, but traffic between leaf nodes will go through the spine nodes.

The traffic from a source leaf node to a destination leaf node flows as follows:

- From a TAP, traffic flows to the source leaf node
- From the source leaf node, traffic is load balanced to all spine nodes
- From a spine node, traffic flows to the destination leaf node
- From the destination leaf node, traffic flows to tool ports

Resiliency is achieved when there are multiple paths from the network to the tools across GigaVUE nodes.

Path Protection

The spine leaf architecture in the cluster environment provides failover for the following:

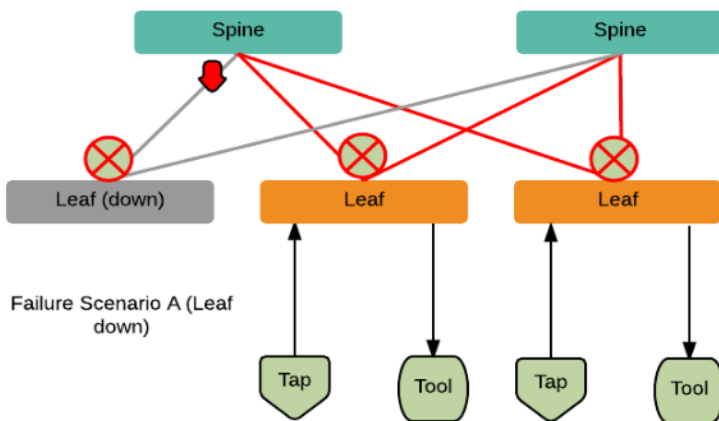
- leaf node failure. Refer to [Leaf Node Failure](#).
- stack link failure on a leaf node (not connected to a tool, but can be connected to a network TAP). Refer to [Stack Link Failure on Leaf \(TAP Connected\)](#).
- spine node failure. Refer to [Spine Node Failure](#).
- stack link failure on a leaf node (connected to a tool). Refer to [Stack Link Failure on Leaf \(Tool Connected\)](#).

Leaf Node Failure

Refer to the figure for a failure in which a leaf node is powered down or rebooted. The leaf node does not have a connected TAP or tool.

NOTE: In the following figures, red arrows indicate traffic direction.

With this type of failure, the stack links connected to the affected leaf node go down, which will be detected by the spine nodes. No action will be required at the spine nodes. Since the links are down, no traffic will be sent to the affected leaf node.



Restoration

Once the leaf node is powered up and booted, it will restore its traffic configuration.

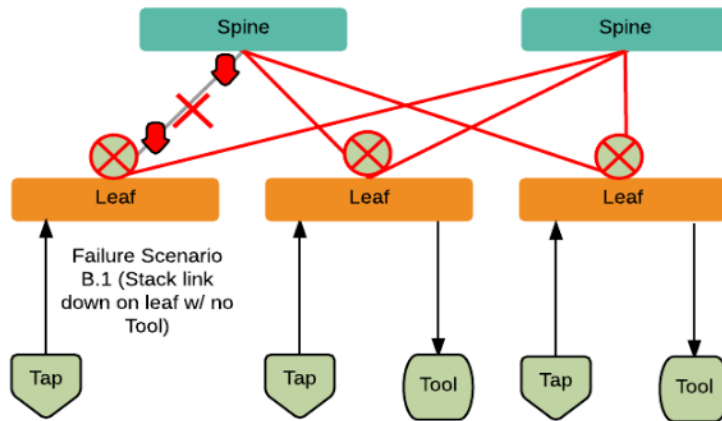
Affected Time

None. Traffic on other leaf nodes will not be affected.

Stack Link Failure on Leaf (TAP Connected)

Refer to the following figure for a failure in which a stack link on a leaf node fails and the leaf node is connected only to a TAP.

With this type of failure, the stack link between the leaf and spine nodes goes down. No action will be required at the spine node. At the leaf node, the affected link will be removed from the stack GigaStream. Traffic will be sent to the other spine node.



Restoration

When the link comes back up, the leaf node will put the link back into the GigaStream.

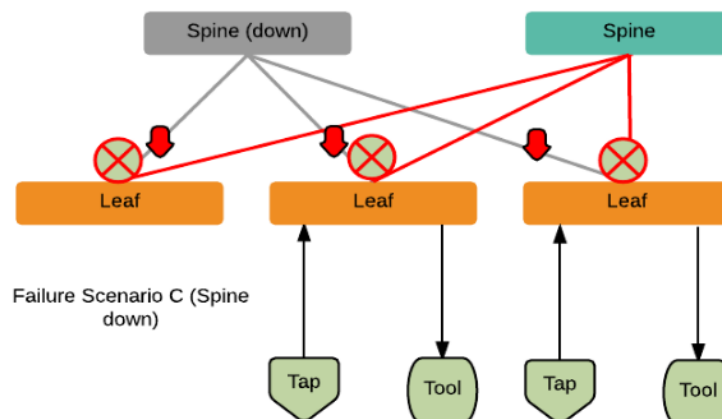
Affected Time

When the link is down, traffic recovers in a similar amount of time as a tool GigaStream.

Spine Node Failure

Refer to the following figure for a failure in which a spine node is powered down or rebooted.

With this type of failure, the stack link between the leaf and spine nodes goes down. The leaf nodes will detect that the stack link is down. The affected link will be removed from the stack GigaStream. Traffic will be load balanced to the other spine node.



Restoration

When the spine node reboots, the cluster will synchronize. When the node converges to the cluster and the configuration synchronizes, traffic will be restored.

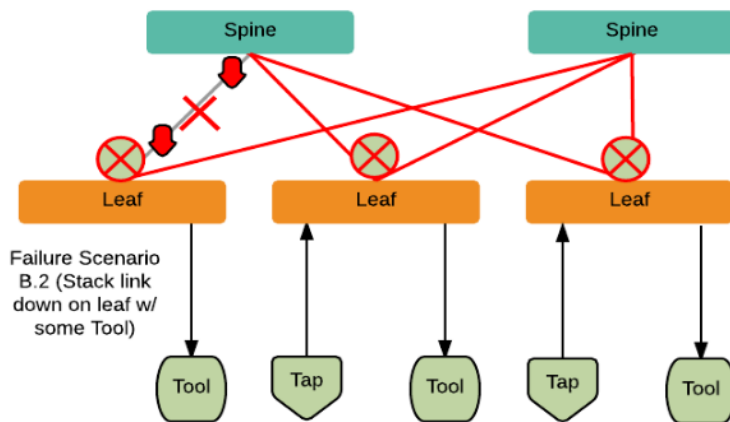
Affected Time

When the spine node is powered down or rebooted, traffic recovers in a similar amount of time as a tool GigaStream.

Stack Link Failure on Leaf (Tool Connected)

Refer to the following figure for a failure in which a stack link between the leaf and spine nodes fails and the leaf node is connected to a tool.

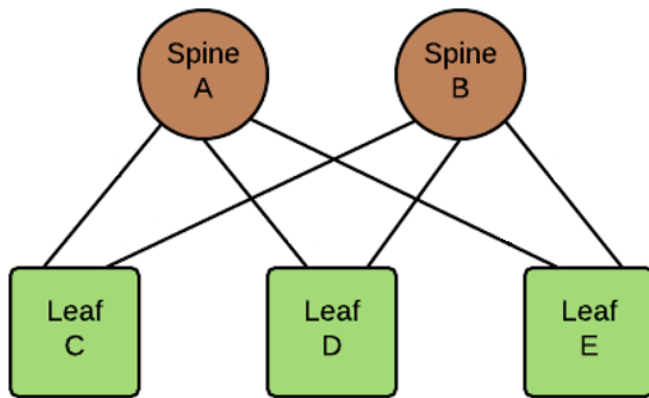
In the current software version, this type of failure is not supported.



Configuration Overview

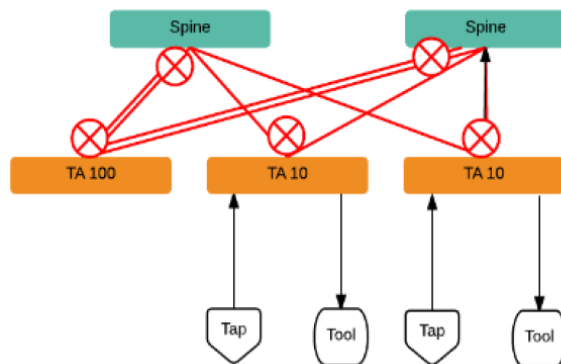
This section provides an overview of the configuration. The configuration is done from the leader in the cluster. Follow this configuration sequence to prevent loops.

This configuration connects nodes using multiple paths. For an example of the configuration, refer to the following figure.

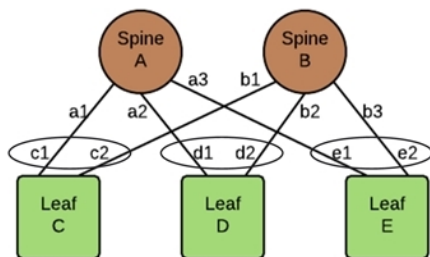


The configuration steps are as follows:

- Configure stack GigaStream. The stack GigaStream connect the spine and leaf nodes. In the following figure, the stack GigaStream are: a1, a2, a3, b1, b2, b3, c1, c2, d1, d2, e1, e2. Even if there is only one port that connects the nodes, you must still configure a stack GigaStream. With a configuration of two spine nodes and three leaf nodes, the number of stack GigaStream is 12.

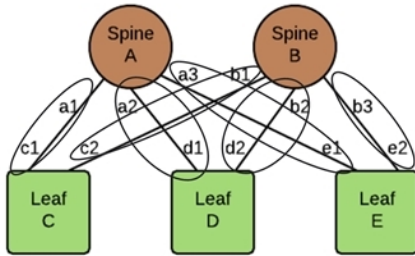


- Configure spine links. On each leaf node, there is one spine link that contains the list of GigaStream connecting the leaf nodes to the spine nodes. The spine links contain multiple stack GigaStream that are bundled together. The spine links are: {c1,c2}, {d1,d2}, and {e1,e2}. The total number of spine links is three for this configuration. The spine links are located at the leaf nodes. Across the spine link members, traffic is load balanced. For this part of the configuration, refer to the circles in the following figure.



NOTE: For the spine links, make sure that all paths are reachable.

- Configure stack links. The stack links are: {a1,c1}, {a2,d1}, {a3,e1}, {b1,c2}, {b2, d2}, and {b3, e2}. The total number of stack links is six for this configuration. For this part of the configuration, refer to the circles in the following figure.



These configuration steps ensure that the spine and leaf nodes are fully meshed.

Notes and Considerations

Refer to the following notes and considerations:

- The multi-path leaf and spine architecture is only supported in an out-of-band cluster.
- The spine link GigaStream must be of type stack. Stack GigaStream carry bi-directional traffic.
- All spine link GigaStream must have the same parameters, such as the same hash value and failover mode.
- Once a spine link is configured, editing of GigaStream parameters is not supported, except for editing the comment.
- Adding a new node to an existing leaf-spine topology is not supported. If you need to add a new node, ensure that you remove the existing configurations and reconfigure them for the new topology.
- GigaStream must be configured before spine links are configured.
- Once a GigaStream is configured in a spine link, it cannot be deleted. To delete a spine link, the stack links must first be deleted.
- A spine link cannot be deleted if a map is using the spine link.
- A spine link cannot be created if a map is using the GigaStream.

The number of spine and leaf nodes is not limited. The ratio of spine and leaf nodes are determined by the cluster traffic needed between the leaf nodes. Larger topologies have the same restrictions as the GigaVUE-OS as follows:

- the total number of nodes in a cluster, for example, 32

- the number of links in a GigaStream (which depends on the GigaVUE node and line card or module, for example, the PRT-HC3-X24 module on GigaVUE-HC3 can have 24 stack GigaStream)

Leaf-Spine Cluster Deployment

This section describes the steps and prerequisites to deploy a leaf-spine cluster.

Refer to [Introduction to Multi-Path Leaf and Spine](#) for a conceptual overview of the leaf-spine architecture.

Deployment Checklist

Before forming a Leaf-Spine Cluster, it is strongly recommended that you get familiar with the relevant documentation and review the deployment checklist to prepare for deployment.

Pre-deployment checklist

- Gigamon Fabric Management must be upgraded to GigaVUE-FM 5.3.00 or later
- Gigamon device must be upgraded to GigaVUE-OS 5.2.00 or later
- Advanced Features License must be installed in TA devices
- Physical connection must be established to create stack links
- Devices must have GDP enabled and be physically connected to create links among devices from GigaVUE-FM.

IMPORTANT: Recommendation is to use TA devices as SPINE Nodes and other devices as LEAF Nodes.

Formation Scenario

The Leaf-Spine cluster can be formed with different combinations of devices with four Spine and six Leaf nodes as a 10-node cluster.

The following configuration creates a leaf spine cluster with two spines and three leafs.

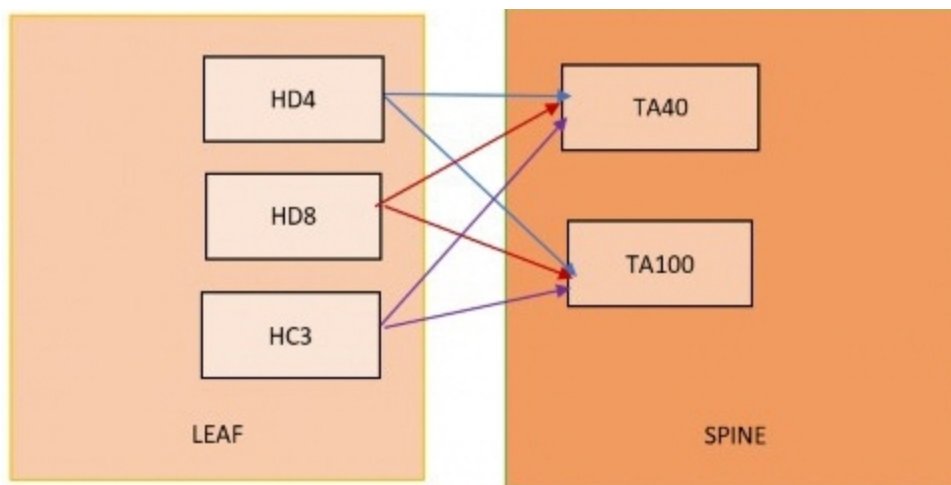


Figure 10 Leaf spine cluster overview,

NOTE: GigaStreams support different speeds, as indicated by the different colored connector lines in [Figure 10 Leaf spine cluster overview](#), .

Leaf-Spine Cluster Formation Workflow

GigaVUE-FM supports workflow-based configurations for forming a cluster. This workflow walks through the required steps to form a complete Leaf-Spine cluster. Additional procedures for editing and deleting cluster formations are also provided:

- [Create a Leaf-Spine Cluster](#)
- [Edit a Cluster](#)
- [Delete a Node from a Cluster](#)
- [How to Change the Leader Preference of a Device](#)

Create a Leaf-Spine Cluster

To create a Leaf-Spine cluster:

1. From the left navigation pane, go to **Inventory > Physical > Nodes**..
2. Click **Create Cluster**.

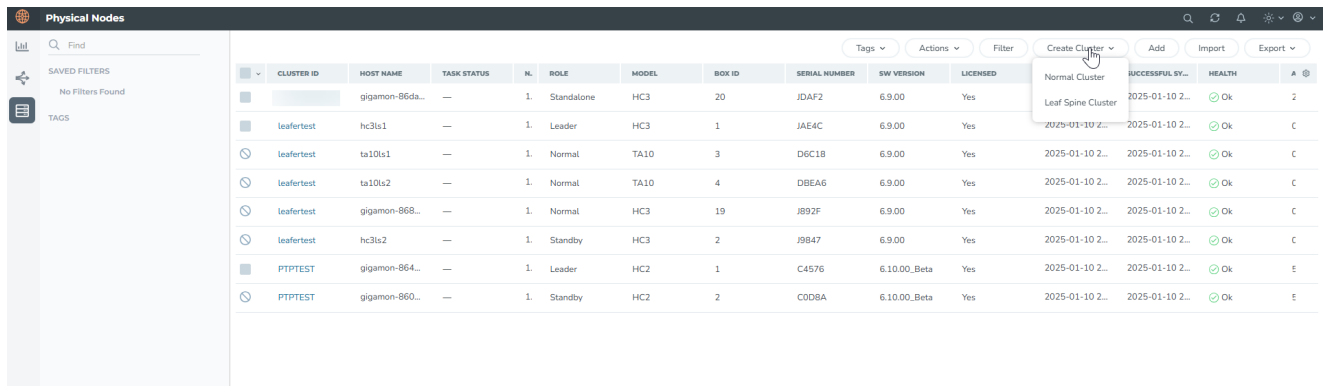


Figure 11 Create Cluster

- From the drop-down list, select **Leaf Spine Cluster**

A **Select Nodes** window appears as shown:

Select Nodes

1 — 2
 Select Nodes — Configure Cluster

i Select nodes and configure cluster to begin the cluster creation process.

Software Version: Select | Model: Select | Stacking Mode: Legacy | Protocol: IPv4 | Q Hostname/IP

	HOSTNAME	MODEL	SOFTWARE VERSION	IP
☐	gigamon-86956b	HC1	6.6.00	
☐	gigamon-86daf2	HC3	6.9.00	

⏪ ⏴ Go to page: 1 of 1 ⏵ ⏩

2 node(s) total

Cancel
Next

The first step is to select the devices in your cluster.

4. Filter the nodes based on the Software Version, Model, Stacking Mode, Hostname or IP address, and the Protocol through which the nodes communicate with each other.



Notes:

- GigaVUE-TA400 and GigaVUE-HCT devices are not supported in Legacy stacking mode.

5. Select the nodes to include in this cluster.
6. Click **Next**

Cluster Configuration

Use the Cluster Configuration window to configure cluster.

7. Enter a valid **Cluster ID** and Virtual IP (**VIP**) and select the leader in the **Seed Node** list.

NOTE: GigaVUE-TA devices cannot be a leader.

8. After completing the Cluster Configuration details, click **Go to Canvas**.

NOTE: Use the **Back** button to return to the Select Devices page to revise the selection of devices for this cluster.

Stack Links configuration

Finally, customize the stack links to define how the nodes should be connected.

9. If GDP (Gigamon Discovery Protocol) is enabled at the device chassis level, then the corresponding ports used to create links and ports should be admin enabled. If a physical connection exists in the device, then the links will be shown.
10. If GDP is not enabled in the ports, then the links need to be drawn to connect the devices.

Connect Leaf devices with Spine devices to create a stack link between them.

Click the tip of the node and drag your cursor to the second node tip to create a link. After you create the link, a dotted line illustrates the connection.



11. Configure the formed links in the Stack Links Configuration pane:
 - a. Select a port from each device that are compatible to create a port stack link, for example: x-x ports ,x-q ports, q-c ports, x-c ports.
 - b. Select one or more ports from each device to create a stack GigaStream stack link.
 - c. Click **Save**.

GigaVUE-FM generates the aliases for each Port stack link and GigaStream stack link as needed.

NOTE: While creating cluster, click **View** stacklinks on the right corner of the canvas to view the details of the stacklinks.. Click **Edit** to edit the details of the devices.

12. Click **Create** to start the cluster creation process.

The Creating Cluster progress message appears as the cluster is being created.

The screenshot shows the 'Physical Nodes' interface. On the left is a sidebar with 'SAVED FILTERS' (No Filters Found) and 'TAGS'. The main area displays a table of nodes with columns: CLUSTER ID, HOST NAME, TASK STATUS, N., ROLE, MODEL, BOX ID, SERIAL NUMBER, SW VERSION, LICENSED, and ATTEMPTED SYN. The table lists 8 nodes, including 'gigamon-860...', 'gigamon-864...', 'gigamon-86da...', and 'leafertest' nodes with roles like Standalone, Leader, Normal, and Standby. At the bottom right, a 'Create Cluster' progress window is visible, showing 'Configuring Cluster [PTPTTEST] on Seed Device [gigamon-864576]' with a progress bar at 1%.

CLUSTER ID	HOST NAME	TASK STATUS	N.	ROLE	MODEL	BOX ID	SERIAL NUMBER	SW VERSION	LICENSED	ATTEMPTED SYN.
gigamon-860...		—	1	Standalone	HC2	2	C0D8A	6.10.00_Beta	Yes	2025-01-10 1.
gigamon-864...		—	1	Standalone	HC2	1	C4576	6.10.00_Beta	Yes	2025-01-10 1.
gigamon-86da...		—	1	Standalone	HC3	20	JDAF2	6.9.00	Yes	2025-01-10 1.
leafertest	hc3ls1	—	1	Leader	HC3	1	JAE4C	6.9.00	Yes	2025-01-10 1.
leafertest	ta10ls1	—	1	Normal	TA10	3	D6C18	6.9.00	Yes	2025-01-10 1.
leafertest	ta10ls2	—	1	Normal	TA10	4	DBEA6	6.9.00	Yes	2025-01-10 1.
leafertest	gigamon-868...	—	1	Normal	HC3	19	J892F	6.9.00	Yes	2025-01-10 1.
leafertest	hc3ls2	—	1	Standby	HC3	2	J9847	6.9.00	Yes	2025-01-10 1.

The Create Cluster progress window in the lower right corner of the page shows the status of every node as it joins the cluster. It takes a few minutes for the cluster to form. The cluster creation process involves the following steps:

- Cluster[clusterName] Creation Successful followed by Seed device
- Verifying Nodes[Will display HostName of all devices]
- Adding Node[HostName] to cluster [clusterName]
- Node[HostName] successfully joined to the cluster.
- Configuring cards for cluster[clusterName]
- Rediscovering cluster[clusterName]
- Configuring ports for cluster[clusterName].
- Configuring ports will display the status of each stack link and GigaStream whether the creation is successful or not.

When the cluster formation process is complete, a notification window confirms the successful creation of the cluster.

13. Click **Go to Cluster** to view the cluster overview.

Edit a Cluster

The Edit cluster option supports only the following operations to the existing cluster:

- Multiple devices can be added to the existing cluster in a single update operation.
- Multiple devices can be added as Leaf, Spine, Leaflet.
- Stack links can be created only from the new device which is added into the cluster wizard.

- Leader preferences can be changed only to device (except) through edit cluster option.
- Stack link alias and GigaStream alias can be edited for newly created links.
- Stacking mode can be changed from Legacy to Default and vice versa.

**Notes:**

- You cannot change the stacking mode and also add or remove a device simultaneously. Only one task can be performed at a time.

NOTE:

- No option to remove the existing stack links through cluster canvas.
- No option to create links in existing devices.
- Addition and deletion of devices in a single update operation should not be appreciated.
- No option to edit the existing stack link alias and GigaStream alias.

Prerequisites

Standalone devices that have maps cannot be added to cluster if ports used in maps overwrites with the selected ports in stack link table.

This workflow describes how to add a node to a existing cluster.

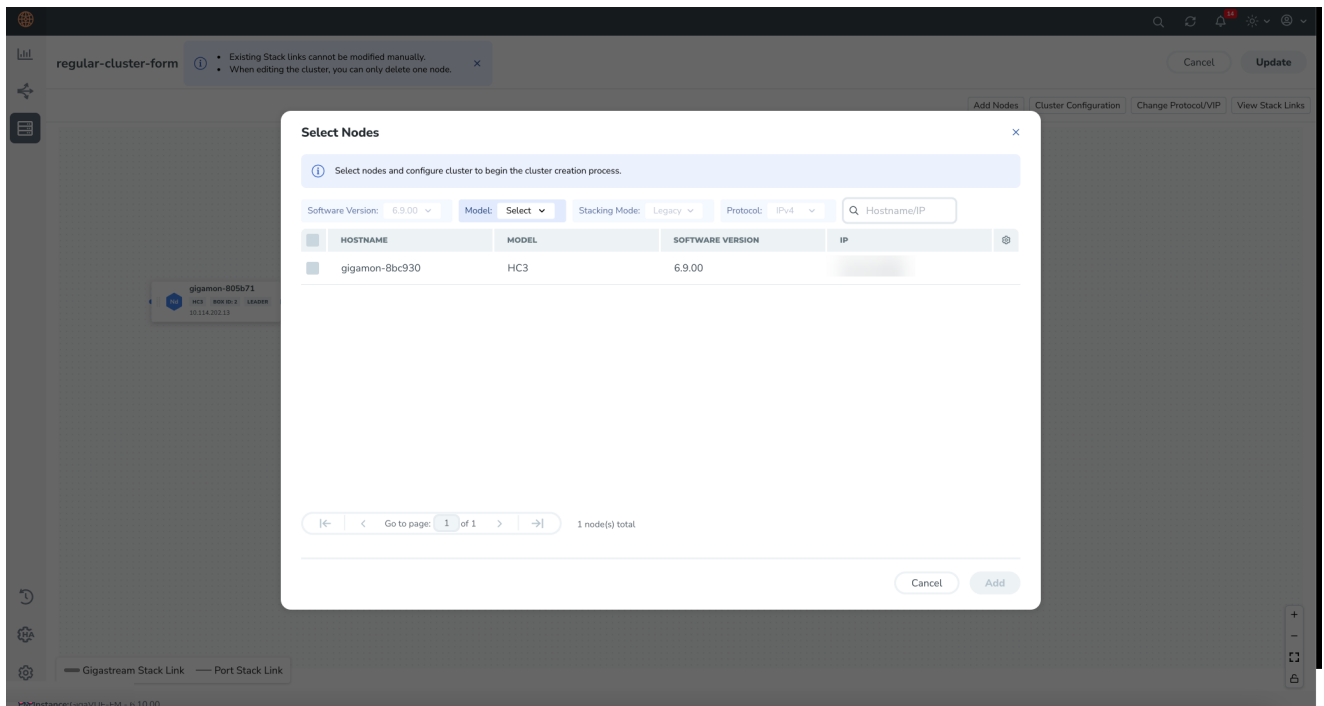
1. Select a cluster and choose **Actions > Edit cluster**.

The screenshot shows the 'Physical Nodes' interface. A table lists nodes with columns: CLUSTER ID, HOST NAME, TASK STATUS, NO..., ROLE, MODEL, SERIAL NUMBER, SW VERSION, LICENSED, and ATTEMPTED SYN. The 'regular-cluster-form' node is selected. The 'Actions' dropdown menu is open, and 'Edit Cluster' is highlighted.

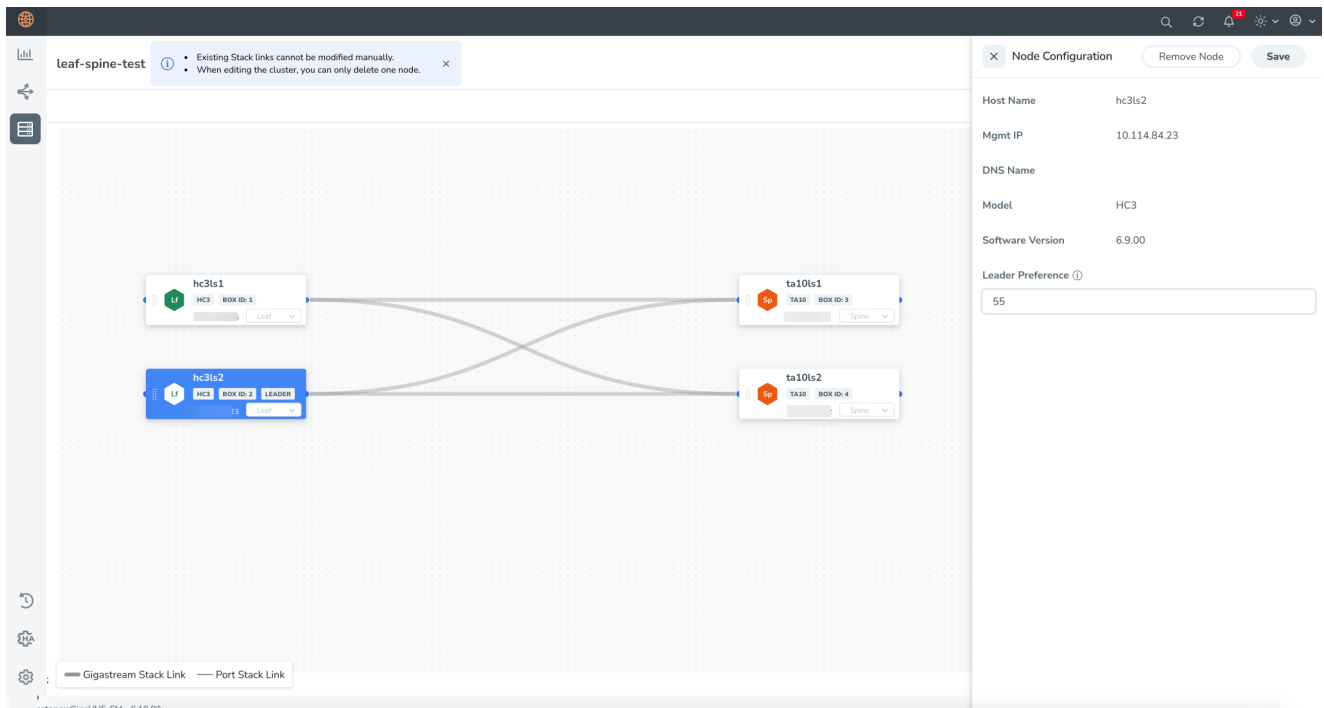
CLUSTER ID	HOST NAME	TASK STATUS	NO...	ROLE	MODEL	SERIAL NUMBER	SW VERSION	LICENSED	ATTEMPTED SYN.
leaf-spine-test	hc3ls2	—	fca...	Leader	HC3	347	6.9.00	Yes	2025-01-22 1..
leaf-spine-test	ta10ls1	—	fca...	Normal	TA10	3C18	6.9.00	Yes	2025-01-22 1..
leaf-spine-test	ta10ls2	—	fca...	Normal	TA10	3EA6	6.9.00	Yes	2025-01-22 1..
leaf-spine-test	hc3ls1	—	fca...	Standby	HC3	3E4C	6.9.00	Yes	2025-01-22 1..
regular-cluster-form	gigamon-805...	—	10...	Leader	HC3	3B71	6.9.00	Yes	2025-01-22 1..
regular-cluster-form	gigamon-805...	—	10...	Standby	HC3	3BE2	6.9.00	Yes	2025-01-22 1..

1 of 6 nodes selected

2. The Edit Leaf Spine Cluster Canvas displays the existing stack link configuration details in the cluster canvas. Click **Add Nodes** to view the standalone devices.
3. Select the required devices from the table in the **Select Nodes** window and click **Add**.



4. In the canvas, draw the links between the newly added device. (**NOTE:** no new link is created for the existing device.)



- Configure the stack link details in the stack link table.
- Click **Save**.
- Change the stacking mode as required.
- Click **Update** to initiate the update process. A confirmation window appears advising that a backup file is generated with the updated traffic configurations. The configurations saved in the backup file must be applied manually to restore the traffic configurations.
- Click **OK** to run the cluster update.

When the cluster update operation starts, a notification window appears at the right corner of the GigaVUE-FM window to show the status progression of each node, card, GigaStream and stack link.

When the cluster update operation is complete, a notification window confirms the completion of the cluster updates.

- Click **Go to Cluster** to go to view the cluster overview.

The screenshot displays the 'Physical Nodes' page in GigaVUE-FM. It features a table with columns: CLUSTER ID, HOST NAME, TASK STATUS, N., ROLE, MODEL, BOX ID, SERIAL NUMBER, SW VERSION, LICENSED, and ATTEMPTED SYN. The table lists several nodes, including 'demo' and 'leafertest'. A confirmation dialog titled 'Update Cluster' is visible in the bottom right corner, showing 'leafertest updated successfully' with a progress bar at 100%. The dialog includes buttons for 'View Logs' and 'Go To Cluster', with the latter highlighted by a red rectangle. The footer of the page indicates 'FM Instance: GigaVUE-FM - 6.10.00' and 'Last Updated At Jan 10, 2025 17:58:01'.

CLUSTER ID	HOST NAME	TASK STATUS	N.	ROLE	MODEL	BOX ID	SERIAL NUMBER	SW VERSION	LICENSED	ATTEMPTED SYN.
5	gigamon-86da...	—	1	Standalone	HC3	20	JDAF2	6.9.00	Yes	2025-01-10 1..
demo	gigamon-860...	—	1	Leader	HC2	2	C0DBA	6.10.00_Beta	Yes	2025-01-10 1..
demo	gigamon-864...	—	1	Standby	HC2	1	C4576	6.10.00_Beta	Yes	2025-01-10 1..
leafertest	hc3ls1	—	1	Leader	HC3	1	JAE4C	6.9.00	Yes	2025-01-10 1..
leafertest	ta10ls1	—	1	Normal	TA10	3	D6C18	6.9.00	Yes	2025-01-10 1..
leafertest	ta10ls2	—	1	Normal	TA10	4	DBEA6	6.9.00	Yes	2025-01-10 1..
leafertest	gigamon-868...	—	1	Normal	HC3	19	J892F	6.9.00	Yes	2025-01-10 1..
leafertest	hc3ls2	—	1	Standby	HC3	2	J9847	6.9.00	Yes	2025-01-10 1..

The created GigaStreams appears in the device Port Groups page, and the created stack links appear in the device Stack Links page.

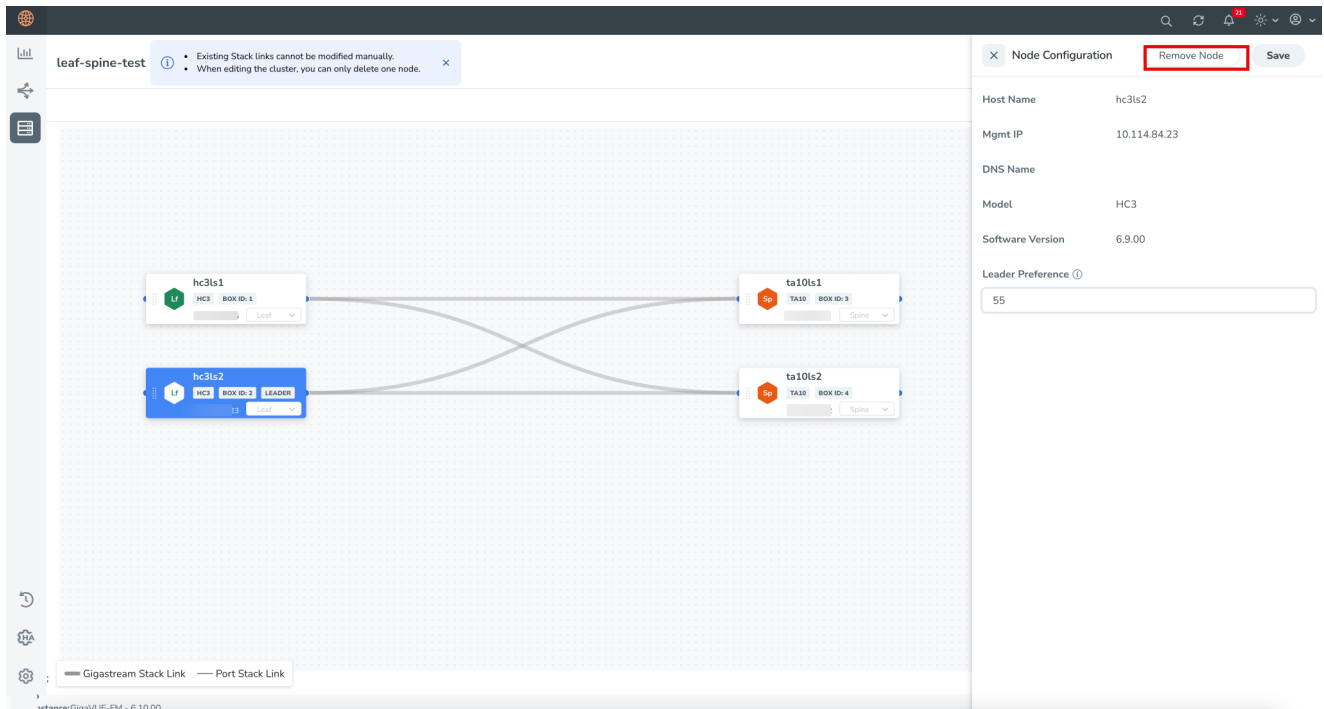
Delete a Node from a Cluster

This workflow describes how to remove a device node from a cluster.

NOTE: Only one device can be removed from the cluster per update operation.

The device should not contain any map configurations in a cluster. Those devices cannot be removed until the maps are present.

1. Select a cluster and choose **Actions > Edit cluster**. Only one device can be deleted from the canvas. It can be either Leaf, Spine or Leaflet.
2. To remove a device, click the device to be removed from the canvas and click **Remove Node**.



The removed device will be deleted from canvas.

3. Click **Update** to initiate the cluster-update operation.

The Manage Cluster notification window shows the progress of nodes being removed from the cluster. When the device is successfully removed from the cluster, a notification window confirms the successful deletion of the cluster.

4. Click **Go To Cluster** to go into device overview page and see the cluster details.

How to Change the Leader Preference of a Device

This workflow describes how to change the device's leader preference.

1. Select a cluster and choose **Edit cluster** under Actions.
2. To set the leader preference for a device, click the device and update the **Leader Preference** details in the **Node Configuration** quick view that appears in the side pane.

leaf-spine-test

Existing Stack links cannot be modified manually.
When editing the cluster, you can only delete one node.

Node Configuration

Host Name: hc3ls2
Mgmt IP: 10.114.84.23
DNS Name:
Model: HC3
Software Version: 6.9.00

Leader Preference ①
55

Legend: Gigastream Stack Link, Port Stack Link

Instance: GigaVUE-FM - 6.10.00

- Update the leader preference text box and click **Update** to proceed.

The Update Cluster notification appears to show the progress of the cluster update. When the process is complete, **Cluster updation completed**, message appears in the notification window.

- Click **Go To Cluster** to go to the device overview page and see the cluster details.

leafertest hc3ls1 > Overview

Back to Nodes

Overview

Health

Save Configuration

SYSTEM

Chassis

Ports

GigaSMART

Inline Bypass

TRAFFIC

Maps

SETTINGS

Settings

Roles and Users

SUPPORT

Logs

Debug

About

SYSTEM

#1: hc3ls1

Host Name: hc3ls1
Hardware: HC3-Chassis
Mode: Normal
Software: GigaVUE-OS6.9.002024-12-06 05:21:40
Memory: 802MB free of 1842MB
Load Average: 0.2/0.16/0.06

Cards

ID	STATUS	TYPE	CONFIGURED
cc1	✓	HC3-Main-Board	✓
1	✓	PRT-HC3-X24	✓
2	✓	PRT-HC3-C08Q08	✓
3	✓	SMT-HC3-C05	✓
4	✓	SMT-HC3-C08	✓

Fan Trays

ID	STATUS	TYPE
1	✓	FAN-HC3-001
2	✓	FAN-HC3-001
3	✓	FAN-HC3-001
4	✓	FAN-HC3-001

PORTS DOWN

0

PORTS WITH PACKET DROPS

0

OVER-UTILIZED PORTS

0 Rx ports 0 Tx ports

UNDER-UTILIZED PORTS

0 Rx ports 0 Tx ports

TRAFFIC UTILIZATION FOR TOP 20 PORTS

average over last hour

Direction: All

Port	Tx	Rx
19/1/x10	0%	0%
19/1/x10	0%	0%
19/1/x11	0%	0%
19/1/x11	0%	0%
19/1/x12	0%	0%
19/1/x12	0%	0%
19/1/x13	0%	0%
19/1/x13	0%	0%
19/1/x14	0%	0%
19/1/x14	0%	0%
19/1/x15	0%	0%
19/1/x15	0%	0%
19/1/x16	0%	0%
19/1/x16	0%	0%
19/1/x17	0%	0%
19/1/x17	0%	0%
19/1/x18	0%	0%
19/1/x18	0%	0%
19/1/x19	0%	0%
19/1/x19	0%	0%

FM Instance: GigaVUE-FM - 6.10.00

Device version: 6.9.00

Attempted Sync Time: Jan 10, 2025 17:46:00

Successful Sync Time: Jan 10, 2025 17:46:00

Last Updated At: Jan 10, 2025 18:04:24

Spine to Spine and Leaf

This chapter describes the Spine to Spine and Leaf architecture for achieving high availability in a cluster environment. Refer to the following sections for details:

- [Introduction to Spine to Spine and Leaf](#)
- [Configuration Overview](#)
- [Configuration of Spine to Spine and Leaf Architecture](#)
- [Leaf-Spine Cluster Deployment](#)

NOTE: Refer to [Regular Cluster Formation Workflow](#) for how to use the Regular Cluster workflow.

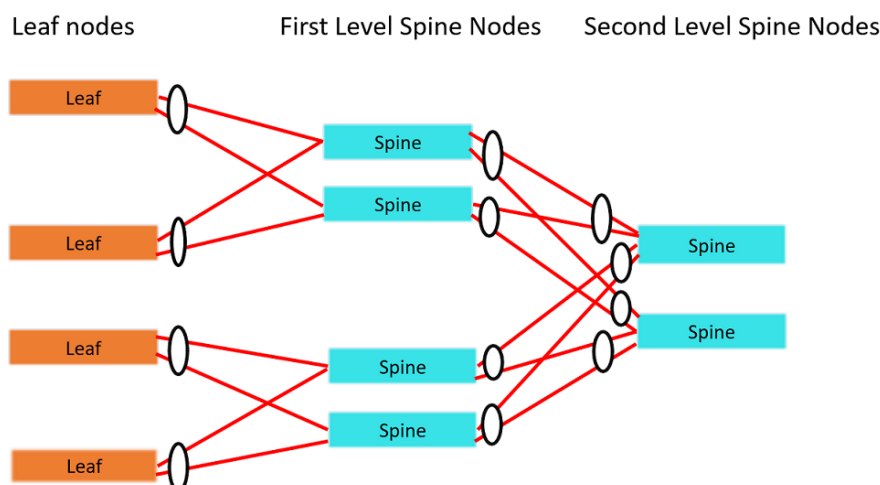
Introduction to Spine to Spine and Leaf

The Spine to Spine and Leaf architecture is a multi-layer architecture used for network aggregation. This architecture supports leaf nodes and multiple levels of spine nodes. In Spine to Spine and Leaf architecture, connect the leaf and spine as follows:

- 1Leaf nodes to the TAPs or tools.
- 2First level spine nodes to the leaf nodes and the second level spine nodes.
- 3Second level spine nodes to all first level spine nodes.

With multiple paths between the nodes in a cluster, the spine to spine and leaf architecture protects against traffic congestion, failures, such as stack link or spine node failures. In the event of a failure, the traffic on one path fails over to the other path. This architecture provides resiliency to the network.

An example of a Spine to Spine and Leaf architecture is shown in the figure.



In a Spine-Leaf cluster, the number of leaf nodes is typically higher than the number of spine nodes. In the figure, there are four leaf nodes, four first level spine nodes, and two second level spine nodes. The leaf nodes aggregate to a fewer number of spine nodes.

For more information on Spine to Leaf architecture, refer to [Multi-Path Leaf and Spine](#).

In the figure, the spine nodes are GigaVUE® TA Series nodes, such as GigaVUE-TA100 or TA200 while the leaf nodes are GigaVUE® HC Series nodes, GigaVUE-HC3 which places the traffic intelligence at the edge.

Traffic between ports on the same leaf node will be local to that leaf node, but traffic between different leaf nodes will go through the spine nodes.

The traffic from a source leaf node to a destination leaf node flows as follows:

- From a TAP, traffic flows to the source leaf node.
- From the source leaf node, traffic is load balanced to the connected spine nodes.
- From the spine node, depending on the configuration, traffic flows to the next level of spines or the destination leaf node.
- From the destination leaf node, traffic flows to the tool ports.

Resiliency is achieved when there are multiple paths from the network to the tools across GigaVUE nodes.

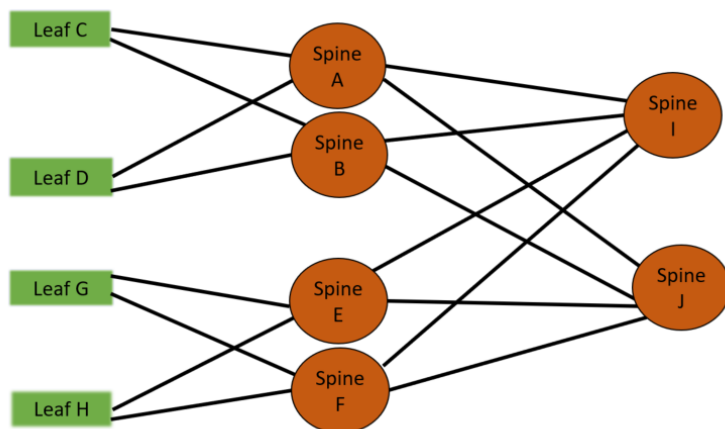
Refer to [Path Protection](#) for the leaf node failure, stack link failure on a leaf node or spine node.

Configuration Overview

This section provides an overview of the configuration. You must perform the configuration from the leader in the cluster. Follow this configuration sequence to prevent loops:

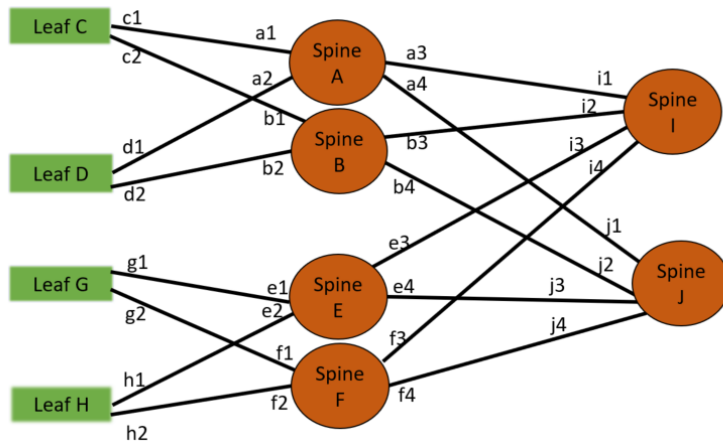
1. [Configure Stack GigaStream](#)
2. [Configure Spine Links](#)
3. [Configure Stack Links](#)

This configuration connects nodes using multiple paths. Refer to the following figure for an example of the configuration.



Configure Stack GigaStream

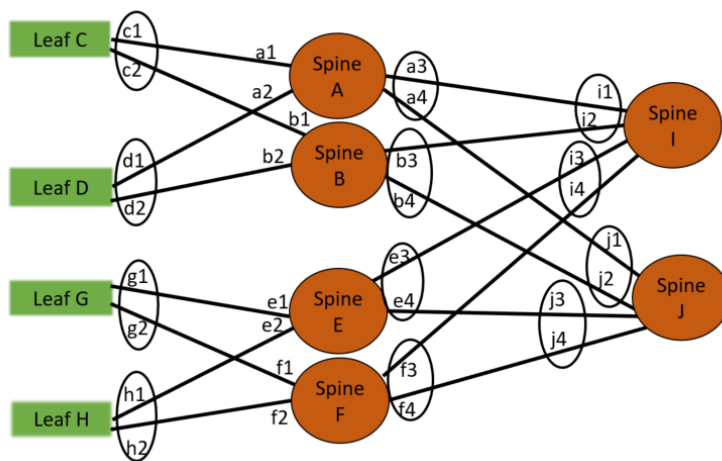
The stack GigaStream connect the spine and leaf nodes. In the following figure, the stack GigaStream are: a1, a2, a3, a4, b1, b2, b3, b4, c1, c2, d1, d2, e1, e2, e3, e4, f1, f2, f3, f4, g1, g2, h1, h2, i1, i2, i3, i4, j1, j2, j3, j4. Even if there is only one port that connects the nodes, you must still configure a stack GigaStream. With a configuration of 6 spine nodes and 4 leaf nodes, the number of stack GigaStream is 32.



Configure Spine Links

On each leaf node, there is one spine link that contains the list of GigaStream connecting the leaf nodes to the spine nodes. The spine links contain multiple stack GigaStream bundled together. The spine links on the leaf nodes are: {c1,c2}, {d1,d2}, {g1, g2} and {h1, h2}.

The spine node also contains the spine links. A spine node connecting to another spine node has a spine link. The spine links on the spine nodes are: {a3, a4}, {b3, b4}, {e3, e4}, {f3, f4}, {i1, i2}, {i3, i4}, {j1, j2}, and {j3, j4}. The total number of spine links is twelve for this configuration. Across the spine link members, traffic is load balanced. For this part of the configuration, refer to the circles in the figure.



NOTE: You must not configure any spine links from spine nodes to leaf nodes. For example, in the figure, a1 and a2 should not be configured as spine links.

Configure Stack Links

The stack links are: {a1,c1}, {a2,d1}, {a3,i1}, {a4,j1}, {b1,c2}, {b2, d2}, {b3, i2}, {b4, j2}, {e1, g1}, {e2, h1}, {e3, i3}, {e4, j3}, {f1, g2}, {f2, h2}, {f3, i4}, {f4, j4}. The total number of stack links is sixteen for this configuration. For this part of the configuration, refer to the circles in the above figure.[Configuration Overview](#).

These configuration steps ensure that the spine and leaf nodes are fully meshed.

Notes and Considerations

For the limitations and considerations, refer the Notes and Considerations in Page 8.

Configuration of Spine to Spine and Leaf Architecture

To configure Spine to Spine and Leaf Architecture, follow these steps:

1. Configure Leaf-Spine Cluster formation workflow. To configure, refer [Leaf-Spine Cluster Formation Workflow](#).
2. Execute the Gigamon Automation GigaVUE-FM SDK to establish the connection between the first level of spines and the second level of spines.
3. View the renewed topology in GigaVUE-FM, and reorder them if required.
4. Verify the configurations performed.

You can view the updated topology in GigaVUE-FM only after the execution of the Gigamon Automation GigaVUE-FM SDK to establish the connection between the first level and second level spines.

Limitations

- It is not recommended to have network and tool in one segment and GSOP in other segment. You must follow any one of the below arrangements:
 - Network and GSOP in one segment of the spine, and the tool in other segment of the spine.
 - Network in one segment of the spine, and GSOP and tool in other segment of the spine.
- If the network port is in first level spine of segment 1, then the leaf should be in the leaf of segment 2.

- If the network port is in first level spine of segment 2, then the leaf should be in the leaf of segment 1.

Leaf-Spine Cluster Deployment

This section describes the steps and prerequisites to deploy a leaf-spine cluster.

Refer to [Introduction to Spine to Spine and Leaf](#) for a conceptual overview of the leaf-spine architecture.

Deployment Checklist

Before forming a Leaf-Spine Cluster, it is strongly recommended that you get familiar with the relevant documentation and review the deployment checklist to prepare for deployment.

Documentation

- Review the **GigaVUE-FM Release Notes** to familiarize yourself with the functionality around creating and managing clusters.
- Review the “Multi-Path Leaf and Spine” chapter to familiarize yourself with leaf and spine architecture.
- Review the **GigaVUE-FM Release Notes** for any known issue that may impact your use case.

Pre-deployment checklist

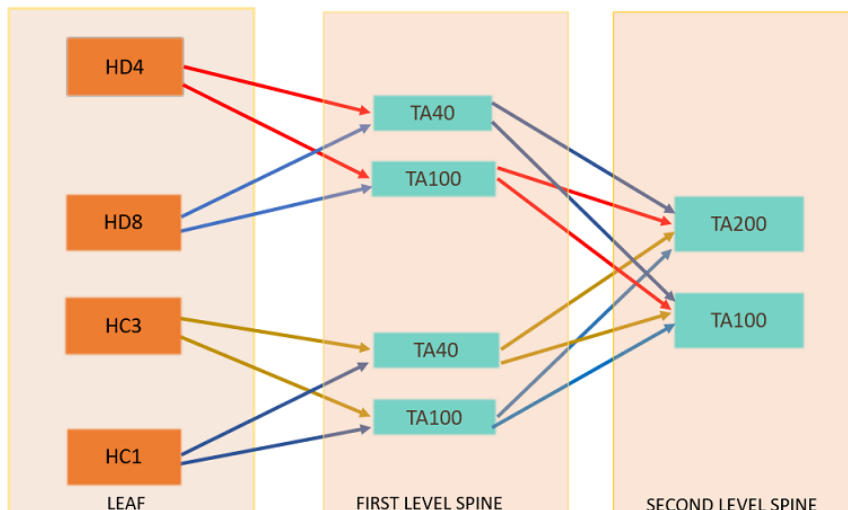
- Gigamon Fabric Management must be upgraded to Gigamon 5.4.01 or later.
- Gigamon device must be upgraded to GigaVUE-OS 5.4.00 or later.
- Advanced Features License must be installed in TA devices.
- Physical connection must be established to create stack links.
- Devices must have GDP enabled and be physically connected to create links among devices from Gigamon.

IMPORTANT: Recommendation is to use TA devices as SPINE Nodes and other devices as LEAF Nodes.

Formation Scenario

The Spine to Spine and Leaf cluster is formed with different combinations of devices with Spine and Leaf nodes as a node cluster.

The following configuration creates a leaf-spine cluster with four leaves, four first level spines, and two second level spines.



NOTE: GigaStreams support different speeds, as indicated by the different colored connector lines in the figure.

Fabric Statistics

This chapter provides the statistics of all types of ports available in GigaVUE H series and TA series.

Refer to the following sections for details:

- [About Fabric Statistics](#)
- [Display Fabric Statistics for All Ports](#)
- [Display Fabric Statistics for a Single Port](#)
- [Export Fabric Statistics](#)
- [Filter Fabric Statistics](#)
- [Clear Fabric Statistics Counters](#)

About Fabric Statistics

GigaVUE-FM provides the ability to view detailed information about the packets dropped, packets discarded, and packets received and transmitted by the following ports:

- Network ports

- Tool ports
- Hybrid ports
- Circuit ports
- Inline-network ports
- Inline-tool ports
- GigaSMART engine ports
- Backplane ports
- XAUII ports
- Stack ports

Network ports, tool ports, hybrid ports, circuit ports, inline-network ports, and inline-tool ports are also called front panel ports. These are the ports that are visible on the front view of the GigaVUE node.

The backplane ports on the control card are connected to the backplane ports on the line card or GigaSMART engine ports. They allow packets to move from card to card, for example, from line card to control card and control card to GigaSMART card. If there are packet errors in the backplane ports, this information can be viewed in the Fabric Statistics page. The format used to represent a backplane port is <box ID>/<slot ID>/<port ID>. For example, 1/1/s1 where s1 refers to port s1.

GigaVUE-FM also collects statistics of XAUII links on the GigaSMART engine ports. Each GigaSMART engine port is made up of 2 to 4 XAUII links, depending upon the platform. They are considered as the child ports of GigaSMART engine ports. The format used to represent a XAUII port is <box ID>/<slot ID>/<port ID>. For example, 1/5/e1x0 where e1x0 refers to the first XAUII port on engine 1.

Display Fabric Statistics for All Ports

Using the Fabric Statistics page, you can view the statistics associated with the port types. If there are packet drops in the ports, click on the port and drill down further to investigate the cause of the packet drops.

To view the Fabric Statistics page:

1. From the left navigation pane, go to **Inventory > Physical > Nodes**. and click on a GigaVUE node.
2. Select **Ports > Ports > Fabric Statistics**.

[Table 3: Fabric Statistics Definitions](#) describes the columns in the Fabric Statistics table.

Table 3: Fabric Statistics Definitions

Counter	Definition	Notes
Port ID	Port ID in the format <box id/slot id/port id>	
Alias	Alias of the port	
Unicast Packets Rx	Total unicast packets received	Excludes multicast packets, broadcast packets, packets with FCS/CRC errors, MTU exceeded errors, oversize packets, and pause packets.
Unicast Packets Tx	Total unicast packets transmitted	Excludes multicast packets, broadcast packets, packets with FCS/CRC errors, MTU exceeded errors, oversize packets, and pause packets.
Packets/sec Rx	Total packets received per second Excludes multicast packets, broadcast packets, packets with FCS/CRC errors, MTU exceeded errors, oversize packets, and pause packets.	Excludes packets with FCS/CRC errors.
Packets/sec Tx	Total packets transmitted per second	Excludes multicast packets, broadcast packets, packets with FCS/CRC errors, MTU exceeded errors, oversize packets, and pause packets.
Octets/sec Rx	Total bytes received per second This indicates the rate of incoming bytes in the last second.	
Octets/sec Tx	Total bytes transmitted per second This indicates the rate of incoming bytes in the last second.	
Bits/sec	Total bits transmitted per second.	
Utilization Rx	Percentage of port utilization by packets received	
Utilization Tx	Percentage of port utilization by packets transmitted	
Link Speed	Maximum link speed of the port	
Type	Type of port	
Octets Rx	Total bytes received Includes all valid and error frames with the exceptions noted in the adjacent columns.	Excludes undersize frames.
Tx drop count	Total packets dropped in the Tx packets.	
Tx drop percentage	Total packets dropped in the Tx packets in percentage.	
Error count	The count of error packet received.	
Error percentage	The percentage of error packets received.	
Octets Tx	Total bytes transmitted	Excludes undersize frames.

Counter	Definition	Notes
	Includes all valid and error frames with the exceptions noted in the adjacent columns.	
Non-unicast Packets Rx	Total Broadcast and Multicast packets received	
Non-unicast Packets Tx	Total Broadcast and Multicast packets transmitted	
Rx Drops count	Total received packets dropped	Packets are dropped when a tool port's bandwidth is exceeded due to oversubscription. Packets are dropped when they reach the tool port but before they are sent out.
Tx Drops count	Total transmitted packets dropped	Packets are dropped when a tool port's bandwidth is exceeded due to oversubscription. Packets are dropped when they reach the tool port but before they are sent out.
Discards Rx	Total received packets discarded	This counter increments when a packet is discarded at a tool port due to a tool port map rule.
Discards Tx	Total transmitted packets discarded	This counter increments when a packet is discarded at a tool port due to a tool port map rule.
Error Rx	Total error packets received Error packets include undersize, FCS/CRC, MTU exceeded, fragments, and oversize packets. All packets that list under this counter are discarded and not processed further.	Excludes oversize packets without FCS/CRC. Packets larger than the MTU setting arriving on a network port are counted twice in the counter. So 1000 oversize packets would show up as 2000. This double-counting only happens with Oversize error packets.
Error Tx	Total error packets transmitted Error packets include undersize, FCS/CRC, MTU exceeded, fragments, and oversize packets. All packets that list under this counter are discarded and not processed further.	Excludes oversize packets without FCS/CRC. Packets larger than the MTU setting arriving on a network port are counted twice in the counter. So 1000 oversize packets would show up as 2000. This double-counting only happens with Oversize error packets.

The port types in the Fabric Statistics table are represented as follows:

Table 4: Port Types

Port	Port Type
Network Port	N
Tool Port	T
Hybrid Port	H
Circuit Port	C
Inline Network Port	iN

Port	Port Type
Inline Tool Port	iT
GigaSMART Engine Port	E (bigger size)
Backplane Port	BP
XAUII Port	E (smaller size)
Stack Port	S

Display Fabric Statistics for a Single Port

To view the Fabric Statistics of a single port:

1. On the Fabric Statistics page, select any port (except for backplane and XAUII).
2. Click on the Port ID field. The port quick view is displayed.

The port quick view provides information about a specific port. Each field is color-coded in the graphical representation.

Port Quick View

The port quick view provides a graphical view of the port statistics. You can choose to view the statistics based on an hour, a day, a week, a month, or live to see the real-time data. The quick view also provides information about port properties, statistics about the traffic received (Rx) and transmitted (Tx), and alarms information. Click Counters drop-down list to select other options.

The following table describes the parameters displayed in the Port quick view:

Field	Description
Port Info	Displays the port information such as the name of the port, if any.
Parameters	Displays information about the current link status of the port, admin status, port type, port speed, port's duplex configuration, auto negotiation configuration, and the force link up configuration.
Transceiver	Displays the transceiver type connected to the port, optical input power, vendor from where the transceiver is purchased, product number, serial number, and temperature.

Field	Description
Filters	Displays the number of filters, pass rules, and drop rules applied to the port.
Port Discovery	Displays the discovery protocol information (GDP, CDP, LLDP) and neighbor device information.
Alarms	Displays the buffer threshold percentage on the ports in the Rx and Tx directions, high and low utilization threshold percentage, and the port utilization in the Rx and Tx directions.
Permissions	Displays the roles and permissions associated with the port, users with permission to lock the port, and users to whom the port is shared.
Related Maps	Displays the related maps associated with the port.
Tags	Displays the port level tag which is configured by GigaVUE-FM user.

Export Fabric Statistics

To export the fabric statistics, click any one of the options as required:

- **Export All** - Exports statistics of all the maps.
- **Export Selected** -Exports statistics of selected maps.

The Statistics table is downloaded in either CSV or XLSX format.

Filter Fabric Statistics

Using filters, you can search and narrow down the ports displayed in the Fabric Statistics page. To filter the fabric statistics, click **Filter**. A filter quick view appears as shown in [Figure 12Fabric Statistics Filter](#). Specify the criteria to filter the ports.

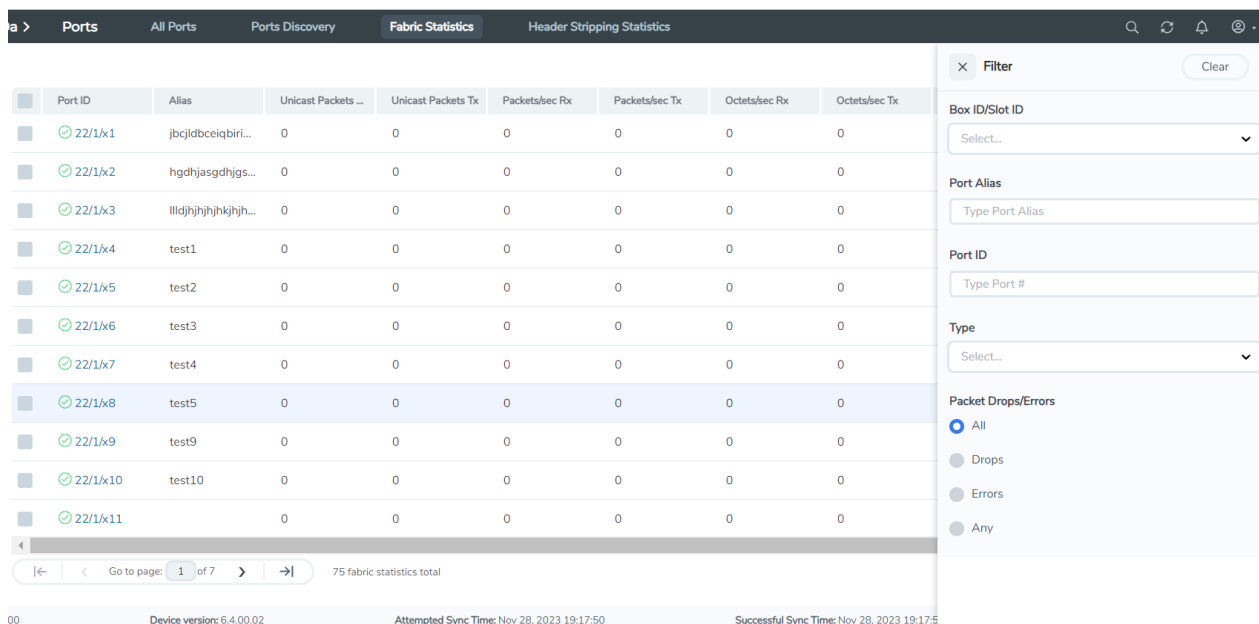


Figure 12 *Fabric Statistics Filter*

The criteria that you can use to filter the fabric statistics is as follows:

Criteria	Description
Box/Slot ID	Displays only those ports that match the specified box and slot IDs.
Port Alias	Displays a port with specified alias.
Port ID	Displays ports with specified port ID. For example, if you specify 3 as the port ID, the result will display ports that include the number 3, 13, 23, 30, and so on.
Type	Displays ports with specified port type. Select one of the following: - Network - Tool - Inline Network - Circuit port - Inline Tool - GigaSMART - Hybrid - Stack - Backplane - XAUUI
Packet Drops/Errors	Displays only those ports with packet drops or errors or both.

Criteria	Description
	Select one of the following: ▪ All — displays ports with both packet drops and errors. This is the default. ▪ Drops — displays ports with only packet drops. ▪ Errors — displays ports with only packet errors. ▪ Any — displays ports with either packet drops or packet errors.

Clear Fabric Statistics Counters

To clear the fabric statistics counters:

1. Select the required port ids for which you need to clear the counters.
2. Click **Clear**. A confirmation message pops-up asking if the statistical counters must be cleared for the selected port ids.
3. Click **Ok**.

Enable Discovery Protocols

You must enable the discovery protocols at the chassis level and at the port level for the nodes and clusters to be discovered.

- Refer to [Enable Gigamon Discovery on Chassis](#) for enabling Gigamon Discovery Protocol at the chassis level.
- Refer to [Enable LLDP and CDP on Chassis](#) for enabling other discovery protocols at the chassis level.
- Refer to [Enable LLDP, CDP, and Gigamon Discovery on Ports](#) for enabling the discovery protocols at the port level.

NOTE: Use the Port Discovery page to bulk configure the discovery protocols (GDP, CDP and LLDP) on all the ports across the devices. Refer to [Port Discovery](#) section for more details.

Enable Gigamon Discovery on Chassis

Gigamon discovery is disabled on chassis and ports. The Gigamon discovery packets are transmitted only when Gigamon Discovery is enabled on chassis as well ports.

To enable Gigamon discovery on chassis:

1. From the left navigation pane, go to **Inventory > Physical > Nodes..**
2. Click on a node on which you want to enable Gigamon Discovery. The Overview page of the node is displayed.
3. In the left navigation pane, click **Chassis**.
4. Switch the Chassis view to List View.
5. Under Properties, select the Box ID for which you want to enable Gigamon Discovery.
6. Click **Actions** and select **Enable Gigamon Discovery**.

NOTE: Refer to the [Enable LLDP, CDP, and Gigamon Discovery on Ports](#) section for details on how to enable the discovery protocols on ports. Use the Port Discovery page to bulk configure the discovery protocols (GDP, CDP and LLDP) on all the ports across the devices. Refer to [Port Discovery](#) section for more details.

Enable LLDP and CDP on Chassis

You can choose to enable LLDP and CDP on the management interface of a GigaVUE HC Series or GigaVUE TA Series device. This will allow the device to discover neighboring devices in a network.

To enable LLDP and CDP on the management interface of a device:

1. From the left navigation pane, go to **Inventory > Physical > Nodes..**
2. Click on a node on which you want to enable LLDP and CDP. The Overview page of the node appears.
3. In the left navigation pane, select **Settings > Interface > Protocol Configuration**.
4. Select the box ID on which you want to enable LLDP and CDP, and then click **Edit**.

5. Select the **Discovery Protocols** check box, and then select one of the following: **LLDP**, or **CDP**.
6. Click **OK**. The selected discovery protocol is enabled on the management interface of the device.

NOTE: Refer to the [Enable LLDP, CDP, and Gigamon Discovery on Ports](#) section for details on how to enable the discovery protocols on ports. Use the Port Discovery page to bulk configure the discovery protocols (GDP, CDP and LLDP) on all the ports across the devices. Refer to [Port Discovery](#) section for more details.

Enable LLDP, CDP, and Gigamon Discovery on Ports

To enable LLDP, CDP, and Gigamon Discovery on ports:

1. From the left navigation pane, go to **Inventory > Physical > Nodes..**
2. Click on a node on which you want to enable LLDP and CDP. The Overview page of the node appears.
3. In the left navigation pane, select **Ports > All Ports**.
4. On the Ports page, select the Port ID on which you want to enable LLDP, CDP, and Gigamon Discovery. Click **Edit**.
5. Under **Device Discovery**, enable the checkbox for the required discovery protocols. Enable all three checkboxes to enable all protocols.
6. Click **OK**.
7. Click **Save**.
8. Click the **Device Discovery** tab. For each port on which the ports discovery is enabled, the neighbor information is displayed.



Refer to:

- [Enable Gigamon Discovery on Chassis](#) for enabling Gigamon Discovery protocol at the chassis level.
- [Enable LLDP and CDP on Chassis](#) for enabling other discovery protocols at the chassis level.
- [Port Discovery](#) for bulk configuring the discovery protocols on all the ports across the devices in GigaVUE-FM.

Limitations of Discovery

The following limitations apply to Gigamon Discovery:

- Gigamon discovery is not supported on inline-tool and inline-network port type.
- For stack ports, Gigamon discovery will work only if both ends of the link are of type stack.
- If a pass-all map is configured for Gigamon discovery enabled ports, the show map stats command will show an increment in the map rule counter for Gigamon discovery packets although the Gigamon discovery packets are not sent to the tool ports.
- If Gigamon discovery is enabled on a port, for example port 9/3/x1, and the port type is changed to an unsupported port types such as inline-network, Gigamon discovery is immediately disabled, and the following message is displayed:

(config) # ! GDP is not supported with port type inline-network. Disabling gdp on port 9/3/x1

Similarly, if the port type is changed to inline-tool, the following message is displayed:

(config) # ! GDP is not supported with port type inline-tool. Disabling gdp on port 9/3/x1

- The hybrid ports, tool-mirror source ports, and ports configured with force link up are operated in loopback mode. So, when Gigamon discovery is enabled, these port show themselves as neighbors.

The following limitation applies to CDP and LLDP Discovery:

- You cannot change the port type if CDP and LLDP Discovery are enabled. To change the port type, you must first disable CDP and LLDP Discovery on the port.

(config) # ! Cannot change port type with discovery configured. Disable discovery on port 1/1/x1 before changing type.

Topology Visualization

The Topology page provides enhanced visualization of the nodes, thereby improving the usability of the page. The nodes are grouped based on pre-defined tags. The Topology page provides the following views:

- **Tagged Layout Topology:** The topology layout is based on predefined tags created by the user. Refer to [Tagged Layout Topology](#) section. The nodes can be grouped based on:
 - **Nature of deployment:** Location of nodes such as region, state, city, data center.
 - **Placement:** Aggregation nodes, leaf nodes, spine nodes.

- **Smart Layout Topology:** For smaller deployments, GigaVUE-FM creates predefined tags to group the nodes. Refer to the [Smart Layout Topology](#) section.

You can use the device level tagging to associate tags to the devices individually, as against the cluster-level tagging option. Refer to [Device Level Tagging](#) section for more details.

NOTE: Classic Topology page is deprecated from software version 6.2.00.

Supported Devices

Topology Visualization is supported in the following devices:

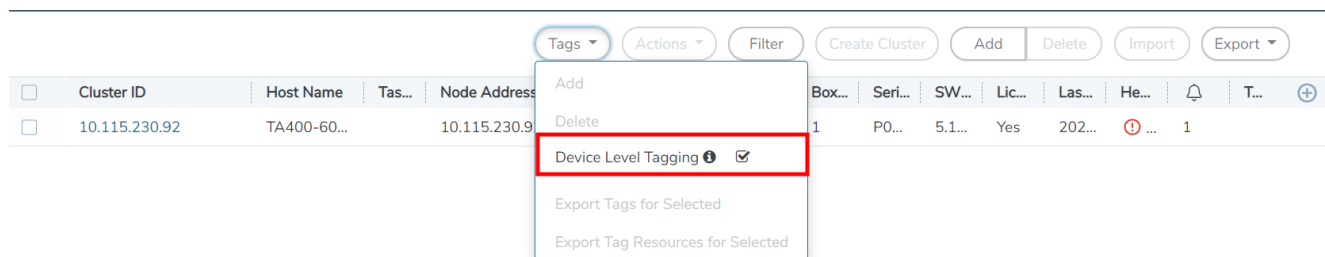
- GigaVUE-HC1 and GigaVUE-HC3
- GigaVUE TA Series devices
- Tool Devices discovered through CDP/LLDP and manual Tool Devices

Device Level Tagging

Each of the individual nodes in a cluster can be associated with a tag key and a tag value. To assign a tag key to a device:

1. On the left navigation pane, go to **Inventory**  go to **Physical > Nodes**.
2. Click on **Tags** and enable the **Device Level Tagging** option.
3. Select the required node(s). Click **Tags** and select **Add**. The **Add Tags to Resources** page appears.
4. Select the required tag key and the tag value to which the nodes must be tagged.
5. Click **OK**.

NOTE: Only aggregation tags can be configured to the devices.



The nodes in a cluster are now associated to tags which can be used for creating the required topology.

Smart Layout Topology

The **Topology** page displays smart layout topology for smaller deployments, in which the number of devices is less than or equal to fifty. GigaVUE-FM constructs the smart layout topology based on the port configuration. GigaVUE-FM applies the following types of tags to the devices:

- **NETWORK DEVICES:** External network devices are grouped under NETWORK DEVICES. By default, this is disabled. You must manually enable it to view the network nodes.
- **GTAP NODES:** Devices with internal tag value of GTAP_Nodes are grouped under GTAP NODES.

NOTE: GTAP NODES column is displayed only if GTAP is configured in GigaVUE-FM.

- **TAP NODES:** Devices with maximum number of network ports are grouped under TAP NODES.
- **CORE NODES:** Devices with maximum number of stack and circuit ports are grouped under CORE NODES.
- **TOOL NODES:** Devices with maximum number of tool ports are grouped under TOOL NODES.
- **EXTERNAL TOOLS:** External tools connected to the devices are grouped under EXTERNAL TOOLS.
- **LEAF NODES:** Leaf nodes in a leaf-spine cluster are grouped under LEAF NODES.
- **SPINE NODES:** Spine nodes in a leaf-spine cluster are grouped under SPINE NODES.

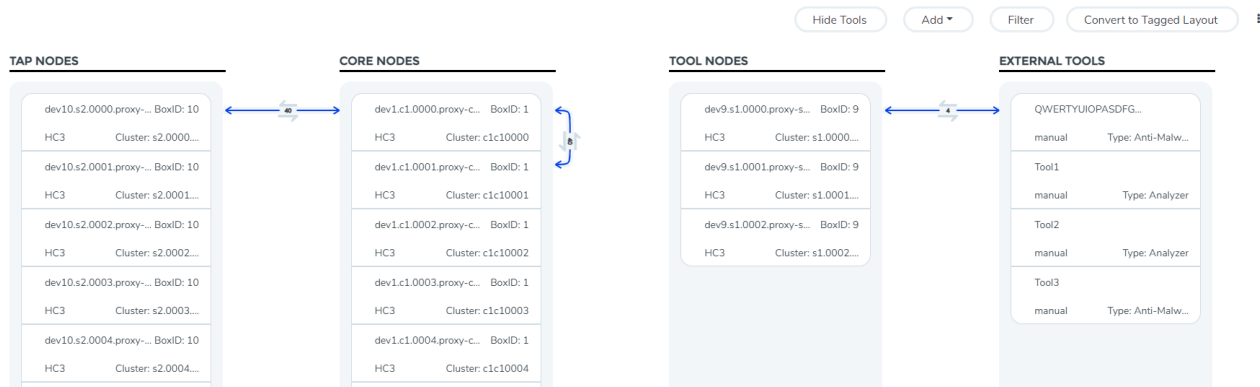
NOTE: Use the **Show Tools/Hide Tools** option to display the external tools in the Topology page.

The devices that do not belong to either the TAP NODES or the TOOL NODES will be included in the CORE NODES category.

The edit option allows you to change the display names (default names) with the names of your choice for the following categories:

- TAP NODES
- CORE NODES
- TOOL NODES

You cannot edit the display name for the external tools.



- Click on a link or a device. The **Connections Nodes and Analytics** pane is displayed at the bottom. Refer to [Smart Layout Topology](#) section for details.



Notes:

- You can drag and drop the devices across the columns to adjust the position of the nodes. The tags will get automatically updated.
- If the number of nodes exceeds 55:** GigaVUE-FM prompts you with a message indicating that the smart layout topology is applicable only up to 75 nodes. You can either retain the existing layout or click **Convert to Tagged Layout** to create tagged layout topology. This option is available only for admin users with read-write access to the Infrastructure Management resource category.
- If 76th node is added to GigaVUE-FM:** The newly added node will not be visible in the smart layout topology.
- If you switch to tagged layout topology:** You cannot switch back to smart layout topology unless the device count becomes less than 50.

Tagged Layout Topology

Tagged layout topology uses tags for grouping the nodes based on the following criteria:

- Hierarchical tags for grouping based on deployment:** This allows you to drill down from a top-level hierarchical view to a lower-level detailed view.
- Placement tags for placement of nodes:** This allows the you to see a detailed view of the devices from a left to right, source to tool view. Only single-valued tags can be used for this configuration.

When you first switch to tagged layout topology, if the devices have not been associated with tags, GigaVUE-FM prompts an error message to tag the devices from the physical nodes page.

**Note:**

- Only users with read-write access to the Infrastructure Management category can configure the required topology using tags. Refer to the 'Tags' section in the *GigaVUE Administration Guide* for detailed steps on how to create tags and how to associate the clusters/devices to tags.
- GigaVUE-FM allows you to configure tags for the individual nodes in a cluster using the Device Level Tagging option. This allows tags to be associated at the device level and allows the devices to be grouped for visualizing the topology. Only aggregation tag type is allowed for tagging of the devices.

Hierarchical View using Hierarchical Tags

Using Hierarchy Tags you can group the nodes based on a specific hierarchical view. For example to create a hierarchy based on the location of the nodes, you must create the following tags ids and tag values:

Hierarchy Level	Tag ID	Tag Values
I	Region	North, East, South, West
II	State	California, New York, Washington
III	City	San Francisco, Los Angeles, Albany,
IV	Data Centers	DC1, DC2 in San Francisco DC3 in Los Angeles DC4 in Albany DC5 DC6 in Rochester DC7 DC8, DC9 in Seattle

You are responsible for creating the appropriate tag keys and tag values and associate the nodes to the correct tag key and tag value to get the required hierarchical view of the tags. The tags can be either RBAC tags with hierarchical property set to True, or Aggregation tags.

NOTE: GigaVUE-FM does not validate the tag values assigned to the tag keys that are selected for hierarchical tag views. You are responsible for associating the correct tag keys and tag values to the nodes, so that the nodes are grouped appropriately.

Tagged Layout View using Single-valued Placement Tags

Using placement tags, you can place the nodes in distinct columns. For example, to place the nodes based on the type of the node, the tag key must be 'Node Type' and the tag values can be one of the following:

- Tap_processing_node
- Tool_node
- Leaf_node
- Spine_node

NOTE: Only aggregation tags can be configured at the node level tags.

Configure Topologies

To configure tagged layout topologies based on hierarchical and placements view, refer to the following sections:

- [Rules and Notes](#)
- [Steps](#)

Rules and Notes

Keep in mind the following rules and notes while creating tagged layout topology:

- The tag keys and the tag values required for the hierarchical view and placement view must be created in advance.
- The devices must be associated to the appropriate tag keys and tag values for visualizing the topology.
- Topology configurations related to subgrouping, color customization, alias names are user-specific configurations. That is, configurations done by you will not affect the views of other users.
- Gigamon Discovery Protocol (GDP) must be enabled on the nodes to visualize the links. For bulk configuration of GDP, refer to the [Port Discovery](#) page in the *GigaVUE Administration Guide*.

- The 'Device Level Node ID' allows you to associate tags to the devices, as against cluster-level tagging.
- You cannot drag and drop the devices across the hierarchical columns. That is, you cannot move the devices across the regions which is logically not possible from GigaVUE-FM GUI. However, you can drag and drop the devices within the same row. That is, you can move the placements of the devices within the same location.

Steps

1. On the left navigation pane, go to **Inventory**  go to **Physical > Topology**.
2. Click **Edit Configured Tags**. This option is available only for admin users with read-write access to the Infrastructure Management resource category. The Topology Tag Configurator page appears.
 - For Hierarchy Tags: Select the required Tag Keys that need to be added to the Selected Hierarchy Tags and click **Add**. Add the Tag Keys in the order based on which you want to drill down.
 - For Placement Tags: Select the required single-valued tags that need to be added to the Placement tags and click **Add**. Add the Tag Values in the order based on which you want to view the nodes in a row.
3. Click **Save**. The configuration is saved and the topology is displayed.



The Physical connections between the nodes across the groups are represented by a single consolidated line. Click on a specific node to view the physical connections of that node with other nodes.

Edit Topologies

To edit the topologies:

1. Click **Edit**.
2. Drag and drop the devices across the hierarchical columns.
3. Click **Save** to save the changes.

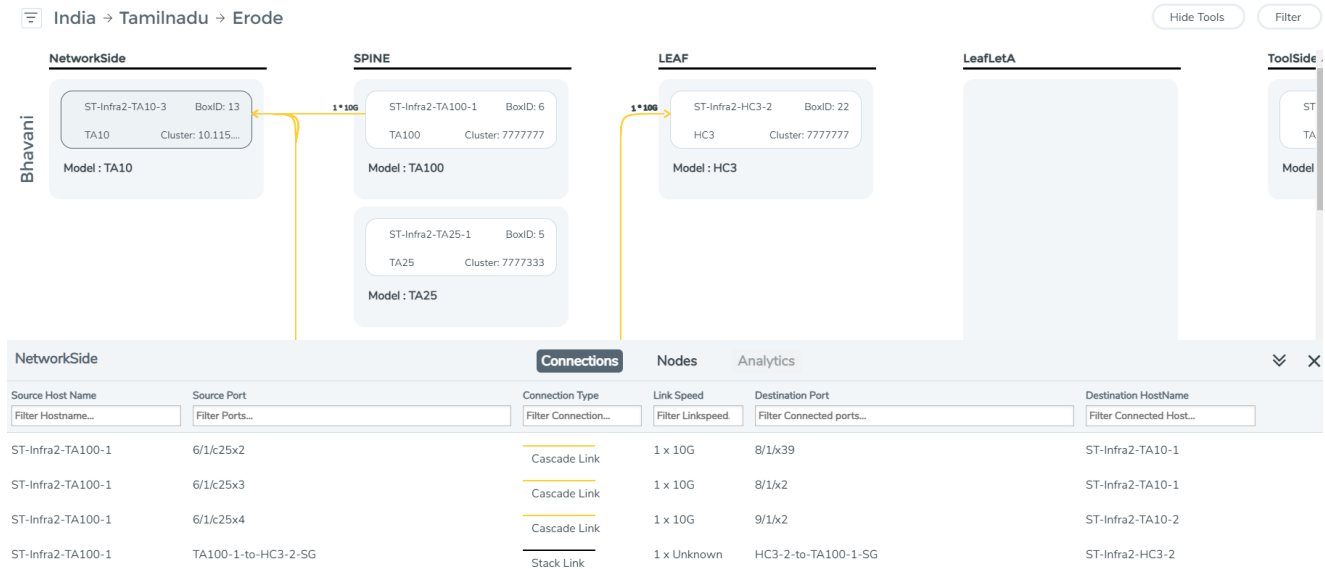
The Edit Configured Tags option is also displayed under the edit option.

View Consolidated Links

From the Topology page you can view the details of the devices and the connections associated with the devices for both smart layout and tagged layout topologies. Click on a link in the Topology page to view the following:

- **Nodes:** Displays details about the connected devices such as Cluster ID, Host name, Node IP, Model, Role, Box ID, and other such details.
- **Connections:** Displays details about the links connecting the Devices such as the host name, port or GigaStream Alias, Type of Connection, Link Speed and other details associated to the connection.
- Hover over the port id to view the health status of the port.
- **Analytics:** Displays the statistical details of the devices and the connections. Click on a specific device or a connection for which you need to view the details. The Analytics tab displays top 5 RX/TX packet drop, Data Rate (Octets) and utilization for a particular column, device or connection based on selection.

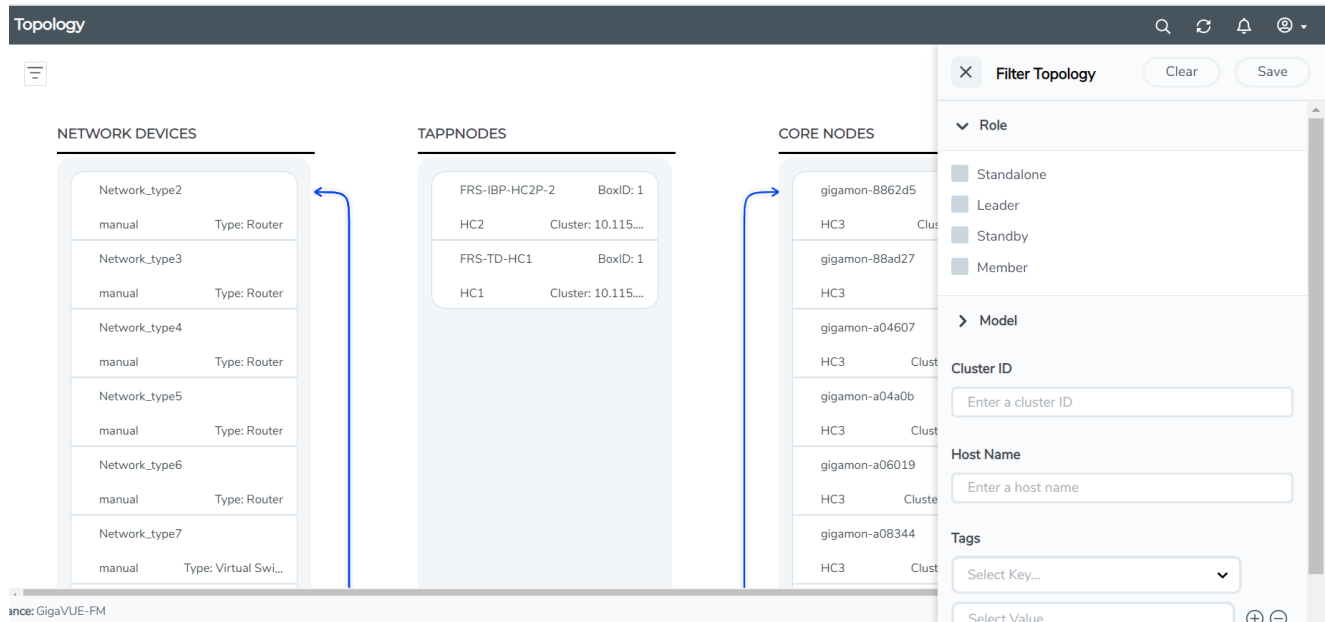
NOTE: For tagged layout topologies, the Analytics tab is enabled only for the tags at the last hierarchical level.



How to Filter

The **Filter** button allows you to filter the devices in the Topology page based on the following criteria:

- **Role:** Select one of the following options:
 - Standalone
 - leader
 - Standby
 - Member
- Model
- Cluster ID
- Host Name
- Tags



The selected filter criteria appear as info panes on the topology page and the filtered node(s) will get highlighted. Click **Save** to save the filter. Click **Clear** to clear the filter.

Use the **Show Unmatched/Hide Unmatched** buttons to show or hide the unmatched nodes and clusters.

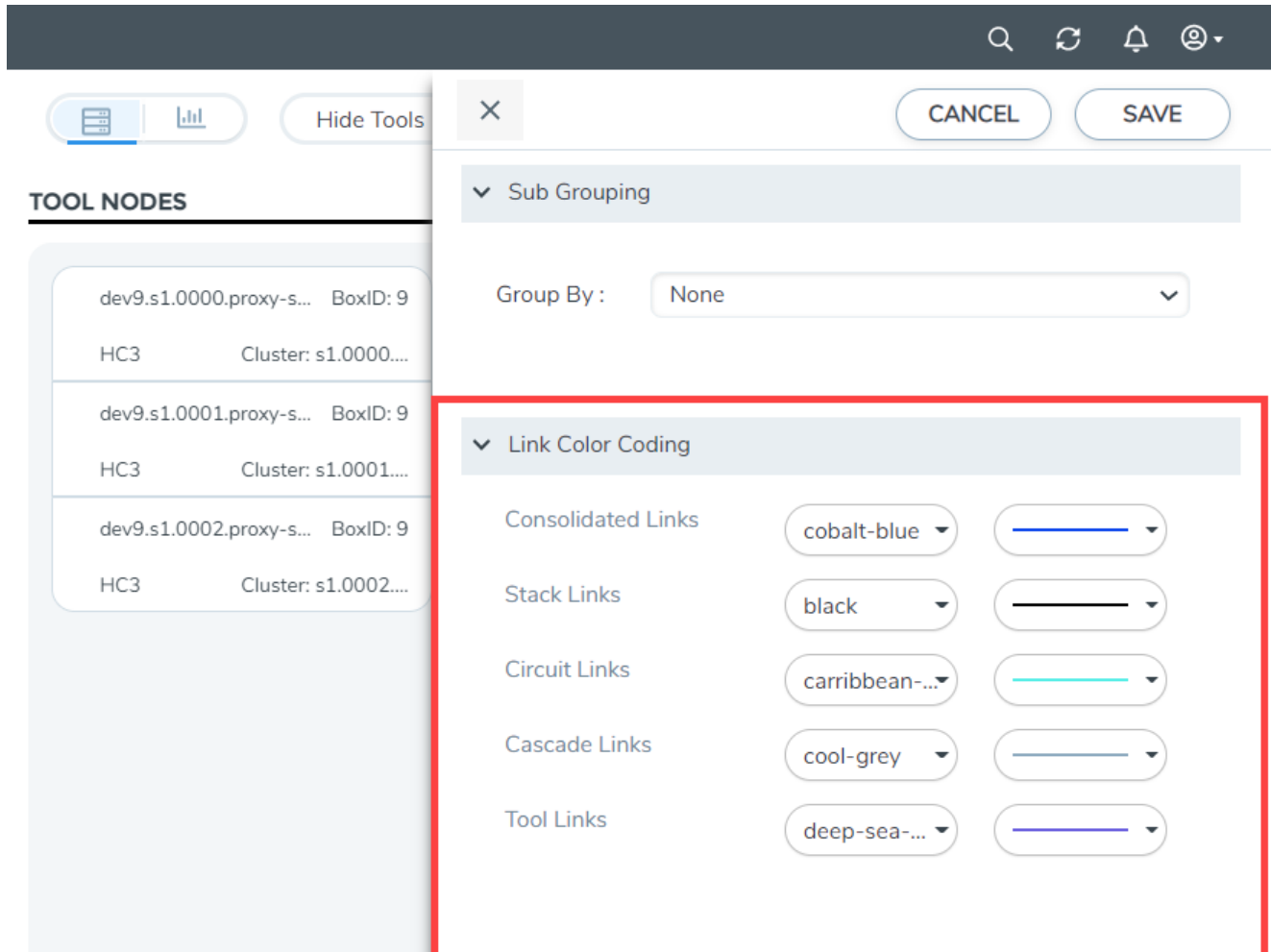
How to Customize the Colors in a Connection

The colors and the format of the connections in the Topology page can be configured as follows:

1. Click the ellipsis on the top right corner of the topology page.
2. Use the **Link Color Coding** option to edit the colors and formats of the following types of connections:
 - Consolidated Links
 - Stack Links
 - Circuit Links
 - Cascade Links
 - Tool Links

The changes are saved and will be applied for the connections when a new topology is created.

NOTE: Some of the colors available in the previous versions have been removed in software version 5.13.00. If you have used those colors in the previous versions, then on upgrading to software version 5.13.00, those colors will be replaced with the supported colors.

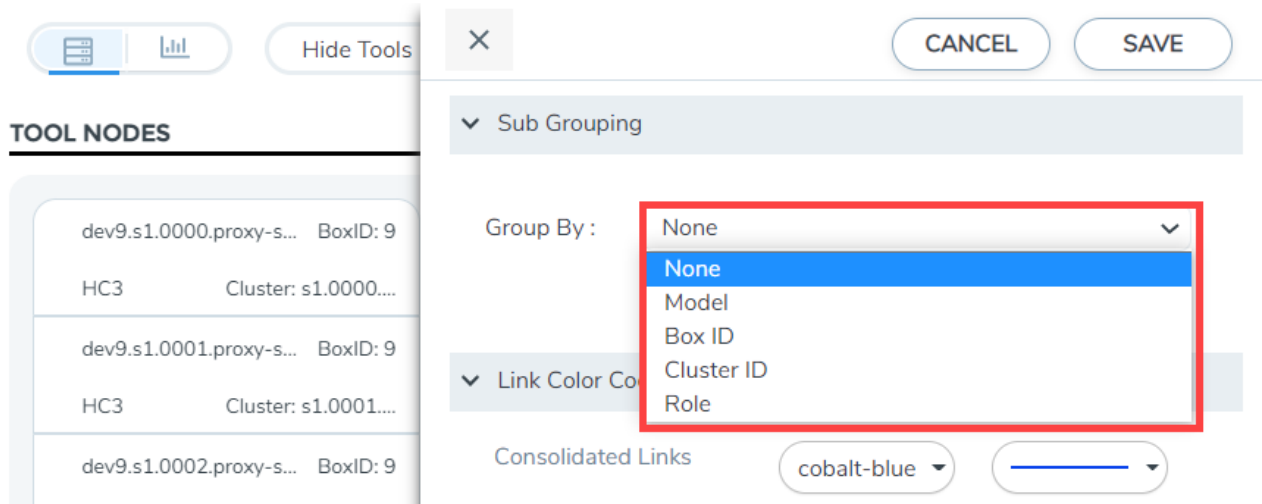


Sub-Grouping of Nodes

The Sub-Grouping option allows you to group the nodes in the Topology page:

1. Click the ellipsis on the top right corner of the topology page.
2. Use the **Sub Grouping** option to select the criteria based on which the nodes must be grouped:
 - Model
 - Cluster Id
 - Box Id
 - Role

The nodes can be grouped in both smart and tagged layouts topology.



Based on the current user who has logged in, the sub-grouping is saved.

External Tool Links and Manual Device Links

The Topology page displays the links between the nodes and the external tools. The tools can be either manually added or discovered through CDP/LLDP by the tool port:

To add devices and links refer to the following section.

Add Devices and Links

To add devices:

1. Select **Add > Add Device(s)**
2. You can add additional nodes by clicking the **+** button. To remove a node, click the **-** button.
3. Enter the following information for the node:
 - **Name**—the name of the node.
 - **Vendor**—the node's manufacturer. For Gigamon nodes, you cannot edit this field.
 - **Model**—the model number of the node.
 - **Description**—optional description or additional information about the node.
 - **Max Throughput** - the maximum throughput traffic currently being sent to this tool.
 - **Storage Capacity** - the total processing capacity dedicated to all Gigamon ports physically connect to the tool.

NOTE: This field is not displayed when selecting a device type **Network**.

The information entered for the node displays when hovering over the icon on the topology. Also, the type selected determines the icon.

4. Click in the **Type** field to select the type of device, either Network or Tool. Depending on your selection, the following icons are displayed:

Type		Icon
Network	Router	
	Switch	
	Virtual Switch	
	Load Balancer	
	Firewall	
	VOIP	
	Cloud	

Type		Icon
Tool	Analyzer	
	Anti-Malware	
	Customer Experience Management	
	Application Performance Management	
	Data Loss Prevention (DLP)	
	Forensics	
	Intrusion Detection System (IDS)	
	Intrusion Prevention System (IPS)	
	Next Generation Firewall (NGFW)	
	SIEM	
	Other	

5. Click **Submit**.

You can also add devices from the Network Devices page. Refer to the [Configure Network Devices](#) section for more details.

To add links:

To add a link or links between nodes:

1. Click **Add Links**.
2. Select the **Source** device and the required source port from the drop-down list.
3. Select the **Destination** device and the required destination port from the drop-down list.

NOTE: You can also select GigaStream as source or destination for the topology and select the required ports.

4. Click **Submit**.

You can also add links from the Connections page. Refer to [Configure Connections](#) section for details.

Recently Viewed

The **Recently Viewed** pane allows you to view the list of recently viewed topologies. Use the **Find** in **Recently Viewed** to find the topologies that you last searched for.

Configure Network Devices

The Network Devices page displays a list network devices configured in GigaVUE-FM.

To view the network devices, log into GigaVUE-FM. On the left navigation pane, go to **Inventory**  and under **Physical**, select **Network Devices**.

The Network Devices page displays the following information:

Field	Description
Network Name	Name of the network

Field	Description
Vendor	Vendor name
Type	Type of device
Model	Model of the device
Description	Brief description about the device
Discover Type	Type of discovery
System Name	Name of the system (only for CDP/LLDP links from external device)
System Description	Brief description about the system
Platform	System platform
Software version	Software version of the network device

NOTE: The columns in the Network Devices page can be customized based on the type of content you want to view in the table. For customizing the columns, refer to [Table View Customization](#).

Use the following buttons to manage the network devices in GigaVUE-FM:

Button	Description
Filter	Use to filter the network devices. You can filter the devices based on the following fields: • Network Name • Vendor • Type • Model • Discovery Type
Add	Use to add new network devices. Enter the following information: • Name • Vendor • Type • Model • Description You can also add Links when adding the manual devices. Refer to the Configure Connections section for more details.

Button	Description
Actions	Use to Edit/Delete the existing manual devices
Import	Use to import the network devices in to GigaVUE-FM. You can only import .CSV files. NOTE: You can only import .CSV files. After the file is imported, a pop-up message appears that shows the number of devices that were successfully imported and the number of devices that failed to import. For failed devices, click on the link in the message, and you will be navigated to the Events page.
Export	Use to export the devices from GigaVUE-FM, either in .CSV or .XLSX format. You can export all the devices or only the selected devices.

Configure Connections

The Connections page displays the links and connections in the topology page.

To view the connections, log into GigaVUE-FM. On the left navigation pane, go to **Inventory**  and under **Physical**, select **Connections**.

The Connections page displays the following information:

Field	Description
Source Host Name	Name of the source host
Source Port	Port ID/Alias of the source port. Hover over the port id. A pop-up appears that displays the following details: • Destination Port ID/Alias • Health State • Link State • Destination Port ID/Alias • Health State
Connection Type	Type of connection
Connection Speed	Speed of connection
Connection Source	Source of connection

Field	Description
Destination Port	Port ID/Alias of the source port. Hover over the port id. A pop-up appears that displays the following details: • Destination Port ID/Alias • Health State • Link State • Destination Port ID/Alias • Health State
Destination Host Name	Name of the destination host.

Use the following buttons in the Connections page, as required:

Button	Description
Filter	Use to filter the connections listed in the connections page. You can filter the links based on any of the fields.
Add	Use to add new links/connections. Enter the following information: • Source Device • Destination Device • Source Port • Destination Port
Actions	Use to delete or edit the connection.
Import	Use to import the connections in to GigaVUE-FM. Note: You can only import .CSV files. The Source Cluster ID and Destination Cluster ID fields are mandatory in the .CSV file. After the file is imported, a pop-up message appears that shows the number of connections that were successfully imported and the number of connections that failed to import. For failed connections, click on the link in the message, you will be navigated to the Events page.
Export	Use to export the connection details from GigaVUE-FM, either in .CSV or .XLSX format. You can export all the connections or only the selected connection.

Configure Tools

The Tools page displays the list tools configured in GigaVUE-FM.

To view the Tools:

1. Log into GigaVUE-FM.
2. On the left navigation pane, go to **Inventory**  and under **Physical**, select **Tools**.

The Tools page displays the following information:

Field	Description
Tool Name	Name of the tool.
Vendor	Vendor name.
Type	Type of tool.
Model	Model of the tool.
Description	Brief description about the tool.
Total Ports	Ports associated with tool.
Number of Maps	Number of maps involving the tool port.
Max Throughput	Maximum throughput sent to this tool.
Storage Capacity	Total processing capacity dedicated to all Gigamon ports physically connected to the tool.
Wrap Around Time	Total Storage (User entered data for the Tool)/Current Throughput
Throughput	Traffic throughput.
Compression Ratio	Compression ratio.
Discovery Type	Discovery type.
System Name	System name.
System Description	System description.
Platform	Platform.
Software Version	Software version.

NOTE: The columns in the Tools page can be customized based on the type of content you want to view in the table. For customizing the columns, refer to [Table View Customization](#).

Use the following buttons to manage the tools in GigaVUE-FM:

Button	Description
Filter	Use to filter the tools. You can filter the tools based on the following fields: • Tool Name • Vendor • Type • Model • Description • Ports • Tags
New Device(s)	Use to add new tools. Enter the following information: • Name • Vendor • Type • Model • Description • Max Throughput • Storage Capacity • Compression Ratio • Add Links You can also add Links when adding the tools. Refer to the Configure Connections section for more details.
Actions	Use to perform the following actions: • Edit • Delete • View Details • View Statistics Graph
Import	Use to import the tools in to GigaVUE-FM. NOTE: You can only import .XLS files. You cannot import more than 50 tools at a time. On successfully importing the tools, a notification pops up. A notification also pops-up when the import operation fails.
Export	Use to export the tools from GigaVUE-FM, either in .CSV or .XLSX format. You can export all the tools or only the selected tools.

Flows

This chapter describes what is a flow and how to quickly view the packet drops and packet errors that causes the flow to be unhealthy.

Considering the system resources needed for its calculation, flows is disabled by default in GigaVUE-FM. However, you can enable flows if required. For larger deployments, exercise caution before enabling flows.

To enable Flows:

1. Go to **Settings** and select **System > Preferences**.
2. Click **Edit**.
3. On the Edit Preferences page, under **Flows**, change the status to Enabled.

PreferencesEdit

My Profile

Username	admin
Groups	Super Admin Group
Email	
Password	change password

Display

NOC View Mode	Off
---------------	-----

Session ⓘ

Screen Refresh Rate (min)	0.5
Auto-Logout (min)	30

General

Items displayed per page	30
FM Instance Name	-
Login Banner	Placeholder for a customizable pre-login banner. Refer to the online help or user guide for customizing this banner

Flows ⓘ

Status	Disabled ☐
--------	-----------------------------------

NOTE: You cannot disable flows once it is enabled. Contact Customer Support to disable Flows.

Refer to the following sections for details:

- [About Flows](#)
- [View Flows](#)
- [View the Flow Summary and Statistics](#)
- [How to Change the Flow Layout](#)
- [How to Update Flows](#)

- [View Events](#)
- [Set Notifications](#)
- [Limitations of Flows](#)

About Flows

Flows provide the ability to view the traffic flowing from a network port that receives the traffic from a network TAP to the tool port that sends the traffic to the tools.

A flow is constructed by traversing backward starting from the egress tool port connected to the monitoring tools all the way up to the network ports that receive the traffic from a network TAP. If there are five egress tool ports sending the traffic out to the monitoring tools, there will be five flows displayed in the Flows page.

Figure 13 [Flow - All Sites](#) shows an example of a flow. It illustrates the network ports that receive the packets from different sources, a set of map rules that filter the packets, and the egress tool port that sends the packets to the monitoring tools. A flow name is determined by the egress tool port ID or alias. In this example, the flow name is SPEGE0070_Te5, which is the name of the egress tool port.

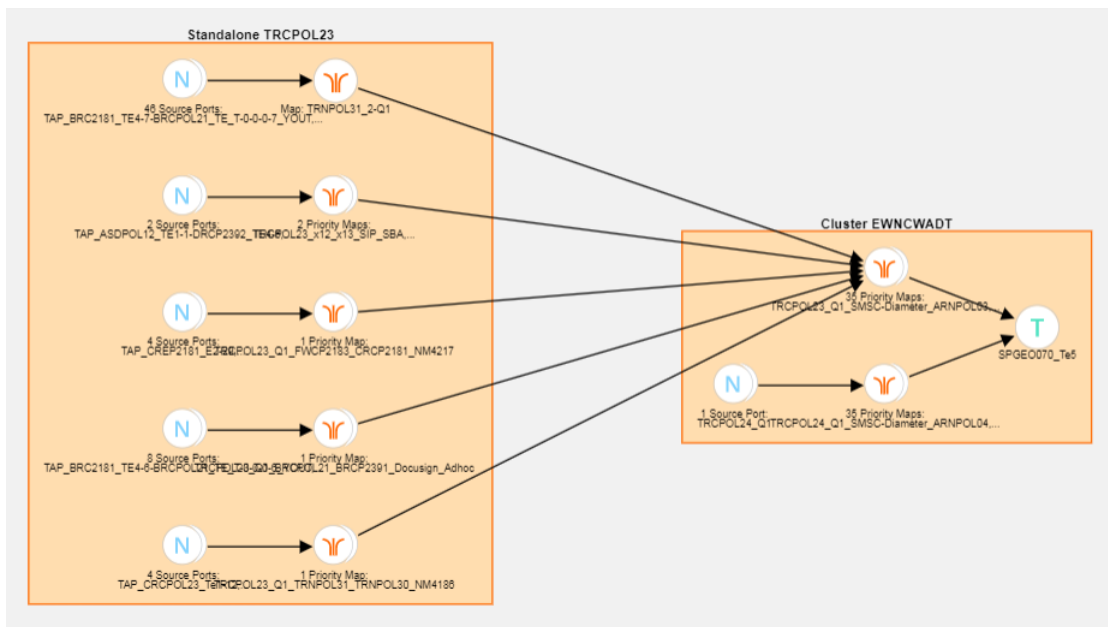


Figure 13 *Flow - All Sites*

Figure 14 [Standalone GigaVUE Nodes](#) shows a number of GigaVUE nodes in the Topology page that are not connected to each other.

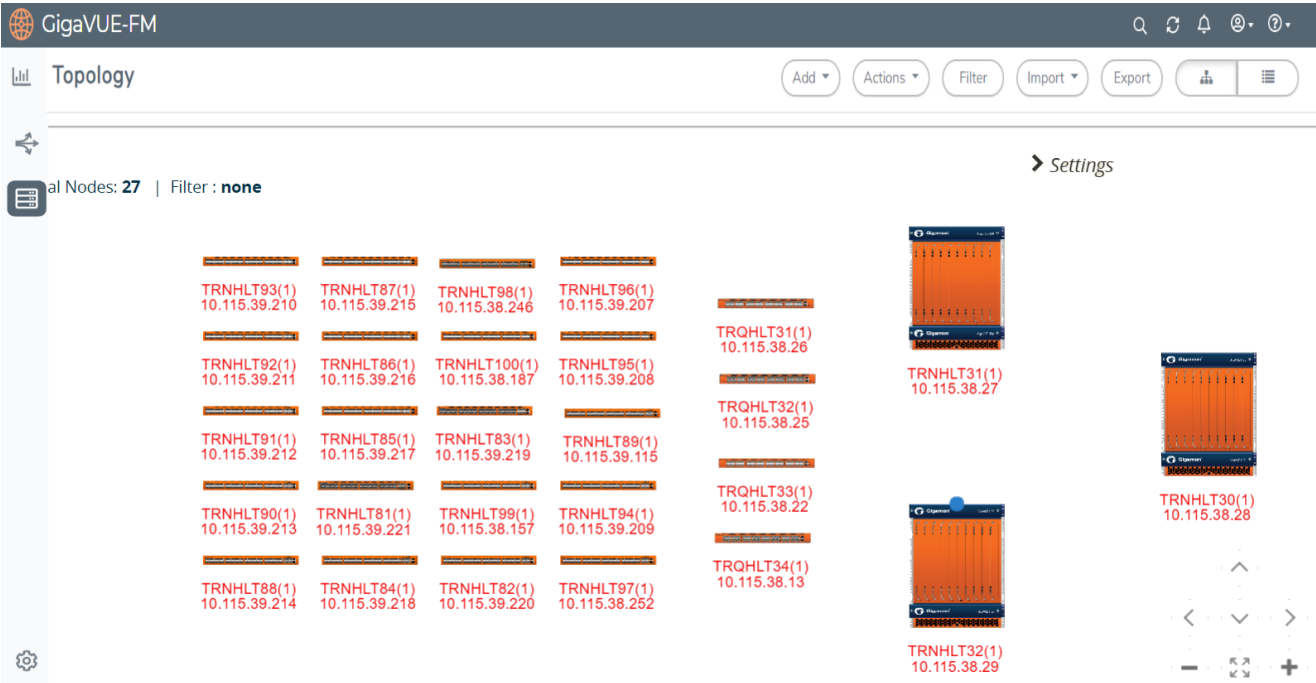


Figure 14 Standalone GigaVUE Nodes

Each node seen in [Figure 14 Standalone GigaVUE Nodes](#) is represented as a separate flow in the Flows page.

Total Flows: 33						
☐	Name	Status	Total Ports	Total Unhealthy Ports	Total Maps	Total Unhealthy Maps
☐	TRQHLT31_TRNFHLT32	Flow is healthy	12	0	10	0
☐	TRNHLT87_TRQHLT31-34	Flow is healthy	36	0	2	0
☐	DAMHLT_Te1&Tel2	Flow is healthy	9	0	1	0
☐	TRNHLT94_TRQHLT31-34	Flow is healthy	36	0	2	0
☐	TRNHLT88_TRQHLT31-34	Flow is healthy	36	0	2	0
☐	TRNHLT90_TRQHLT31-34	Flow is healthy	36	0	2	0
☐	TRNHLT85_TRQHLT31-34	Flow is healthy	36	0	2	0
☐	TRNHLT93_TRQHLT31-34	Flow is healthy	36	0	2	0
☐	TRQHLT32_TRNFHLT32	Flow is healthy	12	0	10	0

Figure 15 Flows Representing the Standalone Nodes

When those GigaVUE nodes are connected using manual links or Gigamon Discovery links, the number of flows created depends on the number of egress tool ports sending the traffic out to tools. In this example, three flows are created as shown in [Figure 14 Standalone GigaVUE Nodes](#).

Total Flows: 3

☐	Name	Status	Total Ports	Total Unhealthy Ports	Total Maps	Total Unhealthy Maps
☐	DAMHLT_Te1&Tel2	 Maps [TRNHLT81_1Q1Q2_TRNHLT31_1Q7Q8_GTP-DCPCF001, TRNHLT81_1Q1Q2_TRNHLT31_1Q7Q8_Permanent] in the flow are unhealthy	843	2	125	2
☐	DAMHLT02_Te1	 Maps [TRNHLT81_1Q1Q2_TRNHLT31_1Q7Q8_GTP-DCPCF001, TRNHLT81_1Q1Q2_TRNHLT31_1Q7Q8_Permanent] in the flow are unhealthy	426	2	63	2
☐	DAMHLT01_Te1	 Flow is healthy	426	0	63	0

Figure 16 Healthy Flows - sample illustration of flows after connections are made

NOTE: Gigamon Discovery is supported only from GigaVUE-FM 5.2 and above.

Figure 22 Unhealthy priority Maps shows how unhealthy priority maps are illustrated in a flow view page.

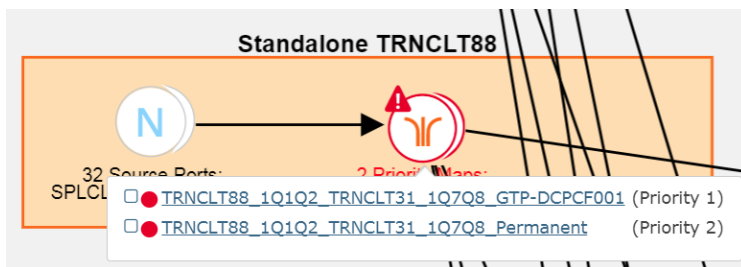


Figure 17 Unhealthy Maps

Using flows, you can perform the following:

- Quickly identify the maps and ports that are unhealthy.
- Quickly drill down the unhealthy map to investigate the cause of failure.
- Export a list of unhealthy ports and maps.
- View the data traffic across the flow, starting from the egress tool port that sends the traffic to the monitoring tool to the ingress network ports that receives the traffic from the network taps or span/mirror ports. The arrows in the flow indicate the path of the traffic flow.
- View the pass all maps and the priority maps. A priority map set contains multiple maps configured with the same source ports in the port list.
- Select multiple maps and view the statistics to verify if the traffic is flowing as expected.
- Filter flows by Flow Name, Status or Cluster ID.
- Update flows.

A flow is automatically constructed every 24 hours, and flow health is calculated every 5 minutes. You can also manually trigger flow and graph calculations on demand.

The following components affect the health of a flow:

- Manual links or Gigamon Discovery links that connect the GigaVUE nodes.
- Maps that are participating in the flow.
- Health status of all the underlying components of a map such as GigaStream, port group, GigaSMART group, and vport.

For information on flow health status, refer to [Flow Health Status](#). For instructions on updating flows, see [How to Update Flows](#).

View Flows



On the left navigation pane, click on  select **Physical > Orchestrated Flows > Flow Maps**, and then select the required cluster or node ID to view a Flow. The Flows page provides a summary of the flow name, cluster, host name, status, total ports, total unhealthy ports, total maps, total unhealthy maps and last computed time.

Table 5: Flows Summary Page

Option	Description
Name	Name of the flow.
Cluster	Where a specific flow is ending. Cluster ID
Host Name	Host name of the cluster.
Status	The Health status of the flow.
Total Ports	The total number of ports involved in the flow are displayed in the Total Ports link.
Unhealthy Ports	Total number of ports that are unhealthy. If there are unhealthy ports, click the Unhealthy Ports link to view the related ports that are unhealthy.
Total Maps	Total number of maps participating in the flow. Click the Related Maps link to view the related maps in the flow.
Unhealthy Maps	Total number of maps that are unhealthy. If there are unhealthy maps, click the Unhealthy Maps link to view the related maps that are unhealthy.
Last Computed Time	

1. Click the numbers under Total Ports, Total Unhealthy Ports, Total Maps, and Total Unhealthy Maps to view detailed information about the maps and ports participating in the flow. Refer to [View Maps and Ports](#).
2. To open a flow, select a flow and click **Actions** > **Open Flow**. Alternatively, click a flow.

View the Flow Summary and Statistics

A flow can display all maps that are created for managing the packet distribution in the GigaVUE nodes. A flow summary provides information only about the total number of maps and ports participating in the flow along with the total number of unhealthy maps and ports in the flow. You can also select multiple maps and view the statistics to check how exactly the packets are flowing.

To view the flow summary:

1. Follow steps 1 to 3 as described in [View Flows](#).
2. In the Flows page, click a flow that you want to view. Alternatively, select a flow and click **Actions** > **Open Flow**. The flow view page is displayed.

The following table describes the information provided in the Summary tab:

Table 6: Flow Summary

Option	Description
Related Ports	Total number of ports participating in the flow. Click the Related Ports link to view the related ports in the flow. Refer to View Total Ports. NOTE: V ports and GigaSMART ports are not considered.
Unhealthy Ports	Total number of related ports that are unhealthy. If there are unhealthy ports, click the Unhealthy Ports link to view the related ports that are unhealthy. Refer to View Total Unhealthy Ports. To know more about how the health of a port is calculated, refer to Port Health Status.

Option	Description
Related Maps	Total number of maps participating in the flow. Click the Related Maps link to view the related maps in the flow. Refer to View Total Maps .
Unhealthy Maps	Total number of related maps that are unhealthy. If there are unhealthy maps, click the Unhealthy Maps link to view the related maps that are unhealthy. Refer to View Unhealthy Maps . To know more about how the health of a map is calculated, refer to Map Health Status .

- To view the statistics, select the maps. To select the maps, follow one of the following methods:

Method 1:

- Click on a map. A list of priority maps are displayed. Refer to [Figure 18Selecting Maps From Maps List](#).

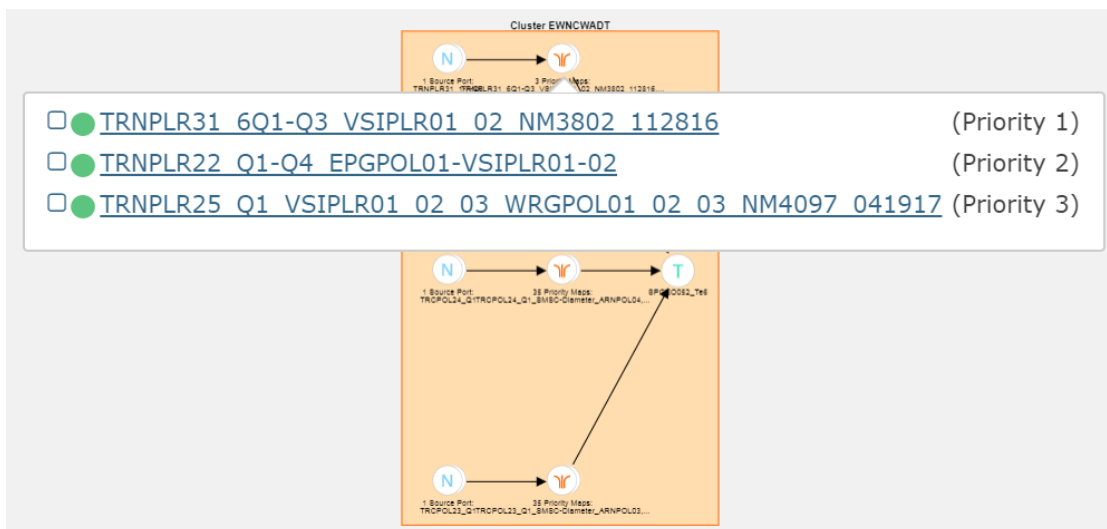


Figure 18 *Selecting Maps From Maps List*

- Click the check box next to the priority map. The selected map is displayed in the **Items Selected** pop-up. Refer to [Figure 19Selected Maps in Items Selected Pop-up](#).

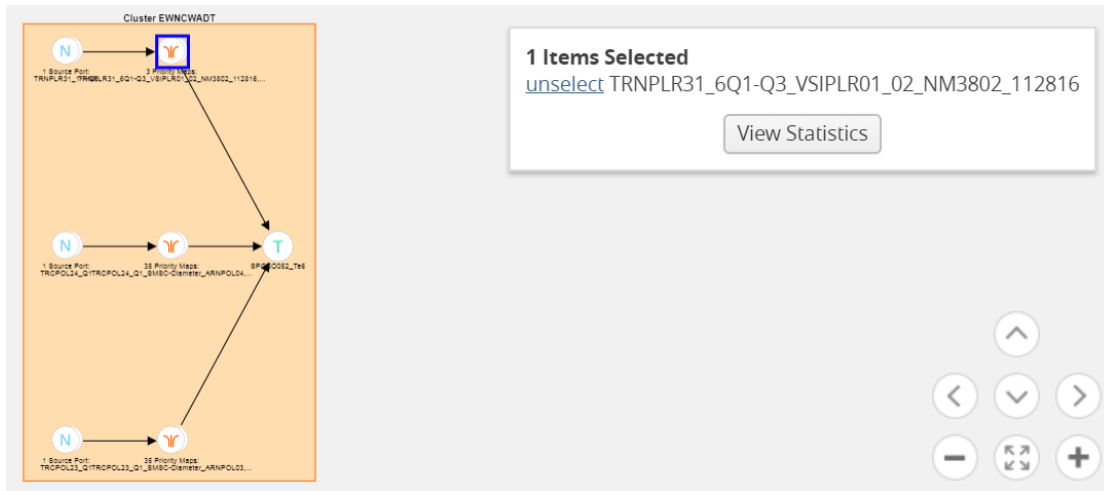


Figure 19 Selected Maps in Items Selected Pop-up

- c. Repeat step a and b for selecting multiple maps.

Method 2:

- a. In the flow view page, double-click on a map. A list of priority maps are displayed. Refer to [Figure 20 List of Priority Maps](#).



Figure 20 List of Priority Maps

- b. Click on a map. The map is selected and is simultaneously displayed in the **Items Selected** pop-up. Refer to [Figure 21 Maps Selected](#).

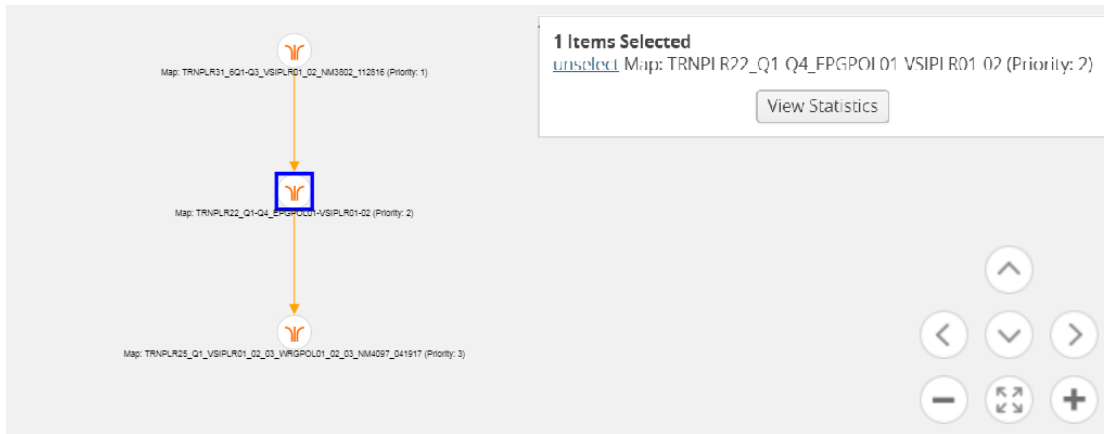


Figure 21 Maps Selected

- c. Repeat step b to select multiple maps.
4. In the **Items Selected** pop-up, click **View Statistics**. Alternatively, select the **Statistics** tab and click **View Statistics**. The **Statistics** tab displays a graph to show how the packets are flowing from the selected maps.

View Maps and Ports

Figure 22 Unhealthy priority Maps shows how unhealthy priority maps are illustrated in a flow view page.

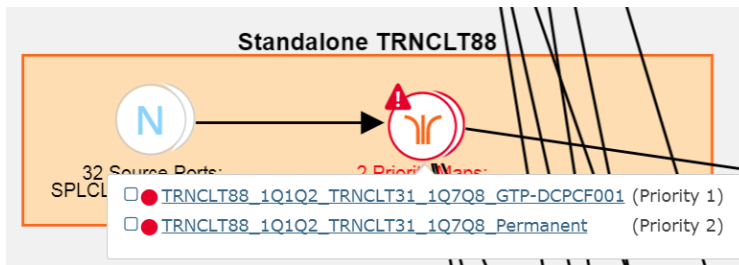


Figure 22 Unhealthy priority Maps

Figure 23 Unhealthy Pass-all Map shows how a pass-all map is illustrated in a flow view page.

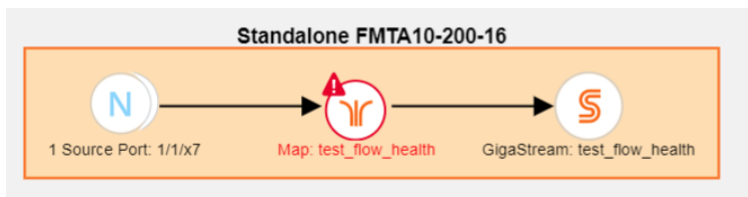


Figure 23 Unhealthy Pass-all Map

A priority map set as illustrated in [Figure 22Unhealthy priority Maps](#) can contain one or more maps configured with the same source ports. The health of this map is determined by the aggregated health of the priority maps in the map set. Sometimes, this map might be unhealthy because a map that is not participating in the flow is unhealthy. The overall health status of a flow is determined based on the aggregated health of all the maps that are involved in the flow.

There are two ways to view the total number of maps and ports that are healthy and unhealthy.

- In the Flows page, click the total number of ports, unhealthy ports, total maps, and total unhealthy maps to view detailed information about the maps and ports involved in the respective flow.
- Click a flow in the Flows page. In the Summary tab, click the Related Ports, Total Unhealthy Ports, Related Maps, and Total Unhealthy Maps links to view detailed information about the maps and ports involved in the selected flow.

View Total Ports

The total number of ports involved in the flow are displayed in the Total Ports link.

To view the total ports involved in the flow:

1. In the Flows page, click the **Total Ports** link. The All Ports quick view displays a list of all ports that are involved in the flow. It also provides information such as port ID or alias, type, port health status, and the node on which the port is configured.
2. In the All Ports quick view, click a Port ID to open the Port quick view.
3. To return to the All Ports quick view, click **Back**.
4. In the All Ports quick view, click a node under the Node column to open the Overview page.

View Total Unhealthy Ports

The total number of unhealthy ports involved in the flow are displayed in the Total Unhealthy Ports link.

To view the unhealthy ports:

1. In the Flows page, click the **Total Unhealthy Ports** link. The Unhealthy Ports quick view displays a list of unhealthy ports that are involved in the flow. It also provides information such as port ID or alias, type, port health status, and the node on which the port is configured.

2. In the Unhealthy Ports quick view, click a Port ID to open the Port quick view.
3. Click a node under the Node column to open the node's Overview page.

View Total Maps

The total number of maps involved in the flow are displayed in the Total Maps link.

1. In the Flows page, click the **Total Maps** link. The All Maps quick view displays a list of all maps that are involved in the flow. It also provides information such as map ID or alias, type, map health status, and the priority node on which the map is configured.
2. In the All Maps quick view, click a Map alias to open the Map quick view.

View Unhealthy Maps

The total number of unhealthy maps involved in the flow are displayed in the Total Unhealthy Maps link.

In the Flows page, click the **Total Unhealthy Maps** link.

The Unhealthy Maps quick view displays a list of all unhealthy maps that are involved in the flow. It also provides information such as map alias, type, map health status, and the priority node on which the map is configured.

In the Unhealthy Maps quick view you can:

- Click **Export** to export an Excel report listing the unhealthy maps.
- Click a map alias link in the Alias column to open the Map quick view. Refer to [View Total Maps](#).
- Click a node under the Node column to open the Overview page.

Filter Flows

To filter flows by name, do the following:

1. On the left navigation pane, click on  select **Physical > Orchestrated Flows > Flow Maps**, and then select the required cluster or node ID.
2. Click the **Filter** button at the top of the pane. The Filter panel displays.

3. Start typing the first few characters of the name of a flow you wish to filter on. The flow list is sorted and all the flows containing the characters you entered displays in order at the top on the page.

To filter flows based on their status:

4. Click the **Status** drop down and select one of the Status colors to display only those flows that correspond to the color selected.

To filter flows based on the Cluster ID:

5. Click the **Cluster ID** drop down and select one of the Cluster IDs to display only those flows that correspond to the Cluster ID you selected.

How to Change the Flow Layout

By default, a flow layout is arranged in a directional flow. The ingress network port receiving the traffic from the network TAP is aligned to the left and the tool port sending the traffic to the monitoring tool is aligned to the right. The maps configured on the standalone nodes and clusters are displayed within the respective containers. The arrows in the layout shows the direction in which the packets are moving from network ports to tool ports. You can drag and drop the cluster or node containers to change the alignment. You can also drag and drop the ports and maps within the container to change the layout.

To reset, save, or restore the layout:

1. In the Flow view page, click and drag a port or a map to change the layout as desired.
2. To save the new flow layout, click **Actions > Save current layout**. The current alignment of the flow is saved.
3. To align the layout to default, click **Actions > Automatically align layout**. The layout is automatically set to the default.
4. To restore the saved layout, click **Actions > Restore saved layout**.

How to Update Flows

Flows are computed based on the Gigamon discovery or manual links connecting the GigaVUE nodes and the maps participating in the flow. The changes made to the flow are not seen unless they are automatically updated after every 24 hours or manual updated from the Flows page.

To manually update a flow:

1. On the left navigation pane, click on  select **Physical > Orchestrated Flows > Flow Maps**, and then select the required cluster or node ID.
2. Click **Actions > Update**. A message is displayed to indicate that the flow calculation is in progress. The check boxes to select a flow disappear when the flow is being updated. They slowly start appearing when the update is completed for that particular flow.

Flows - SITE_ONE							Actions
Total Flows: 33							
☐	Name	Status	Total Ports	Total Unhealthy Ports	Total Maps	Total Unhealthy Maps	
	TRQHILT31_TRNFHILT32	● Flow is healthy	12	0	10	0	
	TRNHILT87_TRQHILT31-34	● Flow is healthy	36	0	2	0	
	DAMHILT_Te1&Tel2	● Flow is healthy	9	0	1	0	
	TRNHILT82_TRQHILT31-34	● Maps [TRNHILT82_1Q1Q2_TRNHILT31_1Q7Q8_GTP-DCPCF001, TRNHILT82_1Q1Q2_TRNHILT31_1Q7Q8_Permanent] in the flow are unhealthy	36	4	2	2	
	TRNHILT94_TRQHILT31-34	● Flow is healthy	36	0	2	0	
	TRNHILT88_TRQHILT31-34	● Flow is healthy	36	0	2	0	

View Events

On the Events page, the FlowHealthStateChange event type indicates that there is a change in the health status of a flow. For more information about Events, refer to the “Events” section in the *GigaVUE Administration Guide*.

Refer to the figure for the flow health change event on the **Events** page.

Source	Time	Scope	Event Type	Severity	Description	Device IP	Host Name
FM	2017-11-07 05:41:05	FM	FlowHealthStateChange	Info	Flow 4090clustertrafficport1 ...		FMTA10-200-10
FM	2017-11-07 05:41:05	FM	FlowHealthStateChange	Info	Flow ewe is healthy		FMTA10-200-10
FM	2017-11-07 05:41:05	FM	FlowHealthStateChange	Info	Flow testtoolalias is healthy		FMTA10-200-10

Set Notifications

On the Notifications page, the email notification for the **Flow Health State Changed** event type can be configured to automatically send emails to the specified addresses when there is a change in the health of any of the flows managed by GigaVUE-FM. For more information about configuring notifications, refer to the “Notifications” section in the *GigaVUE Administration Guide*.

Refer to [Figure 24Flow Health State Changed Notification](#) for the flow health state changed notification on the **Notifications** page.

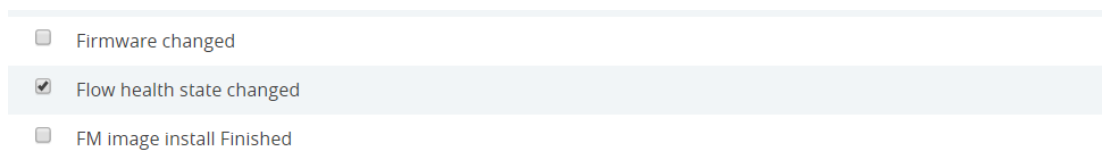


Figure 24 *Flow Health State Changed Notification*

Limitations of Flows

If Gigamon Discovery is enabled on GigaVUE nodes and a link is created between a source and a destination node that are of hybrid port types, the flow ends at the source node hybrid port. As hybrid port acts as an indirect traffic source port and as a tool port, the flow construction fails to identify the direction of the traffic flow. The workaround is to add a manual link to indicate the direction of the traffic flow.

Device Logs and Event Notifications

This chapter describes how to view the logs for the selected node.

By default, GigaVUE-FM acts as a syslog server. However, you can use your own syslog collector instead of using GigaVUE-FM. This optimizes the performance of GigaVUE-FM.

Refer to the following sections:

- [Stream Device Logs to GigaVUE-FM](#)
- [View Device Logs](#)
- [Device Log Host Servers](#)
- [Storage Management for Device Logs](#)
- [Manage Device Log Output](#)

Stream Device Logs to GigaVUE-FM

GigaVUE HC Series device/cluster nodes provide comprehensive logging capabilities to keep track of system activity. Logging is particularly useful for troubleshooting system issues, as well as maintaining an audit trail. You can specify what types of events are logged, view log records by priority, date, or name, and upload log files to a remote host for external troubleshooting.

When HC Series devices are added to GigaVUE-FM, the default settings ensure that log records stream to the GigaVUE-FM server and are written on the device's file system in a messages file. Log records can be used to analyze the system behavior directly from the GigaVUE-FM interface instead of needing to sign in to each device.

External third-party servers can also be added to host the streamed logs. Refer to [Add an External Logging Host Server to a Node](#).

In this section:

- [Cluster Behavior](#)
- [Standardized Logs](#)
- [Device Log Categories](#)
- [Device Log Message Types](#)
- [Device Logging Levels](#)
- [Device Logging Processes](#)

Cluster Behavior

Logging configuration is local to the node. Each node has its own logging configuration.

Important: This is a different behavior than in software versions prior to 5.3 in which the logging configuration on the leader was synchronized to the other nodes in the cluster.

Standardized Logs

Standardized log messages can be streamed to GigaVUE-FM. The log messages follow the industry standard described in RFC5424. The format includes structured data, timestamp, version, and message ID. The timestamp includes milliseconds for increased accuracy.

In GigaVUE-FM, the log information is displayed in a table with configurable, sortable columns and extensive filter options.

Refer to [View Device Logs](#) for information about viewing and filtering logs in GigaVUE-FM.

Refer to the **GigaVUE-OS-CLI User's Guide** for information about the standardized log message format in the CLI view.

Device Log Categories

[Table 7: Device Log Categories](#) describes the categories in device/cluster log messages as per the standardized log format. Refer to [Standardized Logs](#) for standardization information.

Table 7: Device Log Categories

Message ID	Description
GENERAL-ERR	Errors that are common across applications
HIGH-TEMPERATURE	High Temperature
PACKETDROP	Packet Drop
LINK	Link
INIT	Initialization
RESOURCE-UTIL	Resource Utilization
REQUEST	Query system information

Device Log Message Types

[Table 8: Device Log Message Types](#) describes the message types in device/cluster log messages as per the standardized log format. Refer to [Standardized Logs](#) for standardization information.

Table 8: Device Log Message Types

Message ID	Description
memoryAllocError	Memory allocation error
memoryAccessError	Unexpected NULL access
fileAccessError	File access error
switchCpuHighTemperature	High Switch CPU Temperature
opticsHighTemperature	High Optics Temperature
gigasmartCpuHighTemperature	High GigaSMART CPU Temperature

Message ID	Description
ambientCpuHighTemperature	High Ambient CPU Temperature
exhaustCpuHighTemperature	High Exhaust CPU Temperature
egressPacketDrop	Packet Drop at Egress
ingressPacketDrop	Packet Drop at Ingress
linkChangeNotify	Link Change Notification
mgmtModule	Failed to load mgmt module
systemCpuUtil	High System CPU Utilization
systemMemoryUtil	High System Memory utilization
processCpuUtil	High CPU Consumption by a process
processMemoryUtil	High Memory Consumption by a process
processAccessError	Process access errors
systemAccessError	Process access errors
queryFail	Failed to fetch system data
moduleInitFail	Failed to load a cli module

Device Logging Levels

Table 9: Logging Levels shows the standard logging levels that are used to rank logged events by degree of severity. When configuring the device/cluster logs to stream, the highest severity level will capture fewer logs than the lowest severity. For example, if the lowest level (info or debug) is selected in your configuration, all levels of logs, from the selected level up to the highest level, will be streamed. If the highest level (emergency) is selected, only emergency logs will be streamed.

NOTE: If you change the logging severity of the nodes through GigaVUE-OS CLI, then the same will not be reflected in GigaVUE-FM. Therefore, it is recommended to change the logging severity of the nodes through GigaVUE-FM.

Table 9: Logging Levels

Log-Level	Description
emergency	Emergency – the system is unusable. The severity level with the least logging – only emergency level events/commands are logged.
alert	Action must be taken immediately.
critical	Critical conditions.
error	Error conditions.

Log-Level	Description
warning	Warning conditions.
notice	Normal but significant condition.
info	Informational messages.
debug	Debug-level messages. Authorized for factory use only.

Device Logging Processes

Logs that are specific to a process are logged with the process ID. [Table 10: Logging Processes](#) provides a list of logging processes and their descriptions.

Table 10: Logging Processes

Logging Process	Description
acctd	AAA Accounting daemon
avd	Active Visibility daemon
cli	Command Line Interface
clusterd	Cluster daemon
debuggabilityd	Debuggability daemon
frm	Foreign Resource Manager
gsd	GigaSMART daemon
gprof	Profiler
httpd	HTTP daemon
licd	License daemon
mgmtd	Management daemon
ndiscd	Network Discovery daemon
netdevd	Netdev daemon
notf_mgr	Notification Manager
ntpd	Network Time Protocol daemon
peripd	Peripheral daemon
persistd	Persistence daemon

Logging Process	Description
pm	Process Manager
ptpd	PTP Protocol daemon
restapid	REST API daemon
sched	Scheduler daemon
snmpd	SNMP daemon
statsd	Statistics daemon
syncd	Sync daemon
sysht	System Health
ugwd	Unified Gateway daemon
wizard	Wizard
wsmd	Web session Manager daemon
xd	XML Gateway
xinetd	Extended Internet Service daemon

View Device Logs

GigaVUE-FM provides the ability to view logs for each device/cluster node. These logs list all the user events and enable Gigamon Technical Support to troubleshoot in case of any problems.

NOTE: Log streaming is supported on GigaVUE HC Series devices only.

In addition to describing how to view logs, this section describes the following supported functionality related to understanding and configuring the Logs view.

- [Arrange Columns in the Logs View](#)

To view the logs of a single node:

1. On the left navigation pane, go to **Inventory**  and select **Nodes** which displays the list of physical nodes managed by GigaVUE-FM.
2. Select a node. The Single Node view displays overview statistics about the selected node.
3. In the left navigation pane, click **Logs**.

Time	Host Name	Device IP	Process	Log Level	Category	Type	Affected ...	Affected ...	Description	Additional...	Priority	Ver...
2023-06-...	gigamon-...	10.115.46...		ERR					rsyslogd.E...		43	1
2023-06-...	gigamon-...	10.115.46...	mgmtd	WARNING					License ex...		172	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	mgmtd	WARNING					License ex...		172	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	mgmtd	WARNING					License ex...		172	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1
2023-06-...	gigamon-...	10.115.46...	licd	WARNING					Got respo...		156	1

The Logs view displays the latest log information for the selected GigaVUE-OS node in table format.

- (Optional) Click the heading cell for any column to sort the list by that attribute. Refer to [Arrange Columns in the Logs View](#) for details.
- (Optional) Click **Filter** to refine the list of logs by any of the available attributes. The Filter quick view displays the attributes of the logs.
 - Enter a value in any of the available attribute fields to narrow the list of logs according to that value.

Filterable Attributes	Description
Host Name	Enter a hostname or partial host name.
Device IP	Enter a device IP address or partial address.
Time	Specify a start date and time and an end date and time to define a time period. IMPORTANT: Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured timezone.
Process	Specify a process to target, such as clusterd, httpd, ntpd, restapid, snmpd, sshd, ugwd, or wsmd. Partial text entries are acceptable. Refer to Device Logging Processes

Filterable Attributes	Description
Log Level	Select one from the list of log levels, which are ranked by degree of severity. Refer to Device Logging Levels .
Category	Select a category of issue from the list of values, such as: High Temperature, Link, Packet Drop, or Resource Utilization. Refer to Device Log Categories .
Priority	Enter a priority number as defined by RFC 5424.
Version	Enter a version number.
Type	Select an event type from the list of values, such as CPU utilization high, memory utilization high, egress or ingress packet drop, and so on. Refer to Device Log Message Types .
Affected Entity Type	Select an affected entity type from the list of values. Options are: CPU, Memory, Port, or Optics
Affected Entity	Enter a specific affected entity

- b. Click **Filter** to apply the filter on the current list of logs.
The list of logs is now limited to the set matching your filter criteria.
- c. To clear the filter, click **Clear** in the Filter dialog.

Arrange Columns in the Logs View

The Logs view has sortable, configurable columns. The options below describe how to use these options to personalize your view of the logs:

- Click the heading cell for any column to sort the list by that attribute.
- To move the order of a column, click the heading cell for that column and drag it to the location you prefer, then release the mouse click to drop it in the new location.
- Configure the columns to display in this view:
 - a. Click **+** icon on the right above the table.
 - b. The Column option appears.
 - c. Amend your column settings:

To add or remove a column, click the column label for the column to get selected and unselected accordingly.

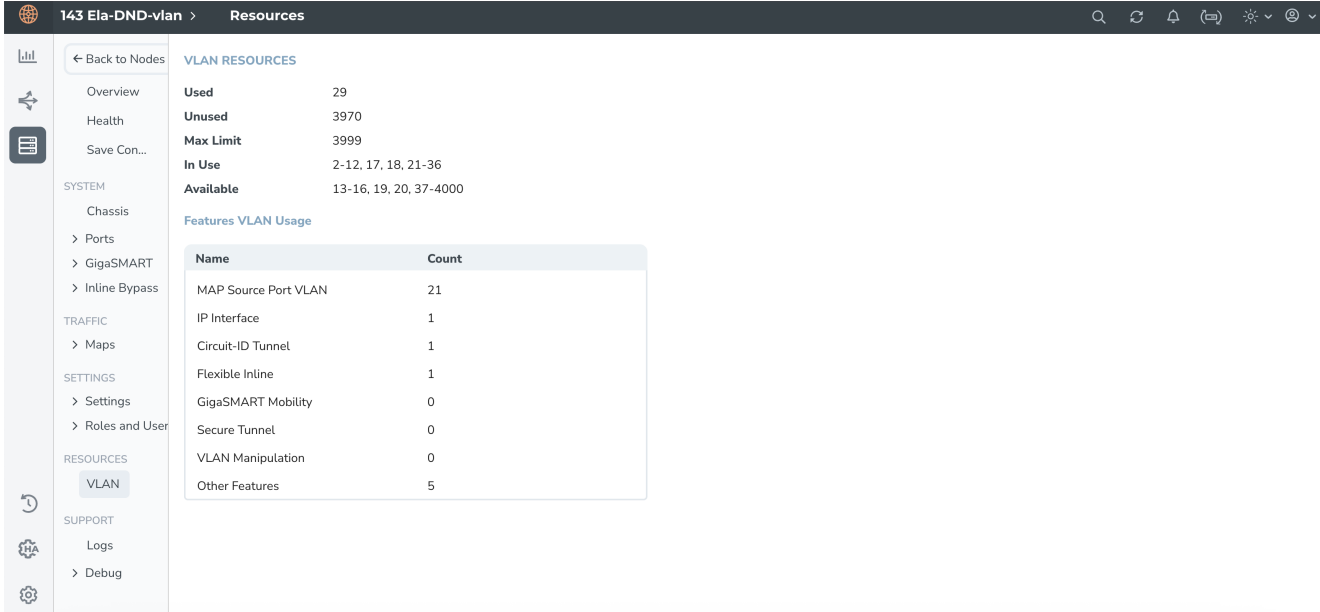
To revert to the GigaVUE-FM default setting, click **Reset Columns to Defaults**.

VLAN Resources

GigaVUE-FM displays the VLAN resources that are used, and available. It also displays feature-wise VLAN usage.

To view the vlan resources:

1. On the left navigation pane, go to **Inventory**  and select **Nodes** which displays the list of physical nodes managed by GigaVUE-FM.
2. Select a node.
3. In the left navigation pane, click **Resources > VLAN**.



143 Ela-DND-vlan > Resources

VLAN RESOURCES

Used	29
Unused	3970
Max Limit	3999
In Use	2-12, 17, 18, 21-36
Available	13-16, 19, 20, 37-4000

Features VLAN Usage

Name	Count
MAP Source Port VLAN	21
IP Interface	1
Circuit-ID Tunnel	1
Flexible Inline	1
GigaSMART Mobility	0
Secure Tunnel	0
VLAN Manipulation	0
Other Features	5

The VLAN view presents the most recent information on VLAN resources for the selected GigaVUE-OS node, as illustrated above.

The following are the details of the different features and functionalities for which internal VLANs are allocated:

MAP Source Port VLAN: VLANs allocated to each network port of a flow map, the ports belonging to inline-network, inline-tool, and port-pair.

IP Interface VLAN: VLANs allocated for IP Interfaces.

Circuit-ID Tunnel VLAN: VLANs allocated for circuit-ID tunnels, which are used in fabric maps.

Flexible Inline VLANs: VLANs allocated for flexible inline solution deployments.

GigaSMART Mobility: VLANs allocated for GigaSMART mobility feature.

Secure Tunnel VLANs: VLANs allocated to the secure tunnels.

VLAN Manipulation VLANs: VLANs allocated for advanced VLAN manipulation feature.

Other Features: VLANs are allocated for GigaSMART operations on GigaVUE-HC1-Plus, GigaVUE-HCT, GigaVUE-TA25, and GigaVUE-TA25E platforms. This includes those assigned to network ports that are currently not part of any MAPs. Refer to [show vlan-resource](#).

Device Log Host Servers

All device/cluster log messages for all H Series nodes are streamed to the GigaVUE-FM server by default and are written on the device's file system in a messages file.

NOTE: Starting in software version 5.11.00, you can choose to have GigaVUE-FM as the syslog server or you can configure external syslog servers.

External third-party servers, like Splunk, can be added to host the streamed logs. You may want to have certain types of log messages streamed to different servers for different purposes. The Log Settings enable you to add additional host servers for the log streams and to configure the type of logs each server will host.

When an external server is specified, the GigaVUE® HC Series node will send logged events through UDP, TCP, or SSH to the specified destination.

In this section:

- [Add an External Logging Host Server to a Node](#)
- [Edit Host Server Settings](#)

NOTE: For a description of log levels, refer to [Logging Levels](#). For a description of Syslog Server configuration options, refer to [Host Server Options](#).

Add an External Logging Host Server to a Node

This topic describes how to configure a system log server as a destination for logging in GigaVUE-FM.

To add a host server:

1. On the left navigation pane, go to **Inventory**  navigate to **Physical > Nodes** and select a node.
2. Click **Logs** from the Single Node view.
3. Click **Log Setting**.

The Log Settings view appears.

4. Click **Add Server**.

The Add Log Server quick view appears.

5. Specify the server attributes of the log server you wish to add. The parameters vary depending on the protocol you select.

Select the logging protocol: **UDP**, **TCP (default)**, or **SSH**.

For **UDP**, do the following:

- a. Enter the external server's IP address in the **Server Address** field.
- b. Enter the port number in the **Port Number** field.
- c. Select the required host from the **Hosts** drop-down.

For **TCP**, do the following:

- a. Enter the external server's IP address in the **Server Address** field.
- b. Enter the port number in the **Port** field.
- c. Select the required host from the **Hosts** drop-down.

For **SSH**, do the following:

- a. **Enter the external server's IP address in the Server Address** field.
 - b. Enter the port number in the **Port Number** field.
 - c. Enter the user name in the Username field.
 - d. Select the required host from the **Hosts** drop-down.
 6. Click **OK** to save the settings and add the server.
- The additional server appears in the server list.
7. Specify the optional settings for the server. Refer to [Host Server Options](#) for a description of the options.
 8. Click **OK** to save the settings.

Host Server Options

The following table describes the optional host server settings for device logs.

Table 11: Syslog Server Settings

Setting	Description
Logging	This option enables or disable the server.

Setting	Description
	- Click Enable to enable the server. (Default) - Click Disabled to disable the server. - Click Delete to remove the server from this node.
Server Log Level	Select the level of alert you wish to tack on this server: - Info - Notice - Warning (default) - Error - Alert - Critical - Emergency Note: Refer to Device Logging Levels.
Protocol	Select the protocol for communicating with this server: - TCP - UDP (default) Note: GigaVUE-FM can receive logs in TCP as well as UDP on port 5672. However by default it is UDP.
Port	Enter the Port Number.
Ssh Enabled	Check the Ssh Enabled check box to enable Ssh on this server.

Edit Host Server Settings

To edit log settings:

- On the left navigation pane, go to **Inventory**  and navigate to **Nodes** and select a node.
- Click **Logs** from the Single Node view.
- Click **Settings**.
The Log Settings view appears.
The top portion of the Logs Setting page shows the global Storage Management settings. The table in the lower portion lists the servers
- Edit the settings for the server directly in the server list table. Refer to [Host Server Options](#) for a description of the options.
- Click **OK** to save the settings.

Storage Management for Device Logs

Device/cluster log messages for HC Series nodes in GigaVUE-FM are continuously being recorded. As a result, the logs can take up a lot of storage space over time. You may want to delete old records on a regular basis to clear-up storage space. You may want to export log records as a back-up before performing a delete operation or to preserve for external analysis.

GigaVUE-FM Storage Management allows you to define how the stored logs are managed. You can specify a schedule for purging old device logs. You can also specify an SFTP server to export the log records prior to purging.

NOTE: GigaVUE-FM Storage Management is used for all storage settings, including device logs, alarm/event notifications, and statistics. This topic, however, describes the storage management for device logs, in particular.

Access Storage Management

There are two ways to access the Storage Management settings for device logs. These paths are described in [Accessing Storage Management](#).

Table 12: Accessing Storage Management

Path	Steps
From  :	1. Click . 2. Select System > Storage Management. Refer to the Storage Management section in the GigaVUE Administration Guide for more details.
From the device logs page:	1. From the left navigation pane, go to Inventory > Physical > Nodes.. 2. Select a node. 3. Click Logs from the left navigation pane in the node view. 4. Click Settings. 5. The Storage Management page under GigaVUE-FM settings appears. Note: To perform a one-time manual clean-up of old logs on a specific node, refer to Manage Device Log Output.

The configurations performed from this page is applied globally across all the nodes managed by GigaVUE-FM.

Manage Device Log Output

Log management allows you to export and delete logs that are stored in GigaVUE-FM. Use this process to manually clean-up old logs on a specific node before a specified cut-off date and time. You can also specify an SFTP server and file path to export the records prior to purging.

NOTE: Refer to [Storage Management for Device Logs](#) for global Storage Management settings that control purging of old logs on a scheduled basis across all devices.

To edit the log management settings:

1. On the left navigation pane, go to **Inventory**  and navigate to **Physical Nodes** and select a node.
2. Click **Logs** from the node view.
3. Click **Manage**.
The Manage Logs view appears.
4. Complete the fields on this page to specify how to manage the logs:

Setting		Description
Time Range		
	Select records older than	Specify a cut-off date and time for deleting log records. Log records that were created prior to the specified date and time will be deleted. The time is based on the current timezone in GigaVUE-FM.
Export Records To		
	SFTP Server Address	The records are exported to a CSV file. Specify the ftp/sftp location to send the CSV files. For example: sftp://username@121.0.0.1/path/directory
	Username and Password	If this is a secure server, which is recommended, specify the username and password for accessing the server.
	File Path	Specify the path on the server to store the file. For example: /root/dir/archive.zip
Purge Selected Records		
	Check this check box to enable purging the selected records.	

Setting	Description
	Important: If this option is selected, records will be deleted immediately when you click OK .

5. Click **OK** to save the settings.

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)