Riverbed SteelCentral AppResponse with Gigamon Visibility Platform Deployment Guide

COPYRIGHT

TRADEMARK ATTRIBUTIONS

Table of Contents

1 Overview

Riverbed's SteelCentral™ AppResponse delivers full stack application analysis—from packets to pages to end-user experience – letting you observe all network and application interactions as they cross the wire. Using powerful, flexible network and application analytics and workflows, AppResponse speeds problem diagnosis and resolution, helping you get to answers fast. Available as an appliance, virtual machine, or AWS cloud-ready solution, SteelCentral AppResponse combines network forensics, application analytics, and end-user experience monitoring in a single solution.

AppResponse passively monitors the network and collects packet data for continuous, real-time and historical monitoring plus fast troubleshooting. It indexes and stores the packets in such a way that there is no need for file transfers when performing forensic analysis. By continuously recording the packets traversing the network, rich troubleshooting details are always available when you need them. This speeds problem diagnosis and remediation. As a result, there are fewer business-stopping slowdowns and outages, saving you time and money.

Gigamon Visibility Platform comprises of various hardware and software components and the area of interest for this guide is the visibility node GigaVUE HC2 series running the GigaVUE-OS software. The Riverbed solution for network-based application performance monitoring utilizes the patented flow-mapping technology that Gigamon offers, combined with powerful load-balancing capability with the GigaStream feature. Easy access to traffic from physical and virtual networks: Gigamon manages traffic from across the network and delivers it to Riverbed SteelCentral solutions, efficiently and in the correct format. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the Gigamon Visibility Platform for delivery to Riverbed solutions, so that the traffic can be monitored and analyzed together.

An integrated solution of Riverbed SteelCentral and Gigamon Visibility Platform empowers organizations with complete visibility into their infrastructure and application performance with captured data across networks. Some of the key benefits to deploying this joint solution are:

- Access to all network traffic including physical and virtual and delivering this traffic to Riverbed SteelCentral. A mix of GigaVUE H Series, TA Series, and virtual agents acting as TAPs and aggregators will ensure that the SteelCentral applications receive traffic with ease.
- Use of basic and advanced filtering options available in the Gigamon Visibility Platform resulting in less tool overload and sending only specific traffic.
- Header stripping and de-duplication eliminates the need to process unnecessary data and results in higher tool efficiency.
- Data-masking to prevent sensitive information to get exposed and be compliant.
- Load-balancing traffic flows across multiple tools to avoid over-subscription.
- Providing visibility into encrypted traffic with SSL decryption.

Use Case: Delivering relevant OOB traffic to SteelCentral AppResponse

With the advent of digital transformation, businesses are expected to provide faster and robust applications to consumers. This has led to customized experience for different sets of users to maximize revenue and boost customer satisfaction. IT managers and analysts need to get access to the data from various sources in the infrastructure and quickly resolve network and application performance issues. Traffic from all the sources, virtual and physical is sent to a centralized Gigamon Visibility Platform, typically a HC device and then sent to the AppResponse tool as an Out-Of-Band copy.
Based on traffic bandwidth and the type of traffic to be analyzed, the port sizing and filtering options are chosen on the HC device.

Flow maps are configured depending on how many instances or ports (virtual vs physical) of the SteelCentral appliance are deployed.

Deployment Prerequisites

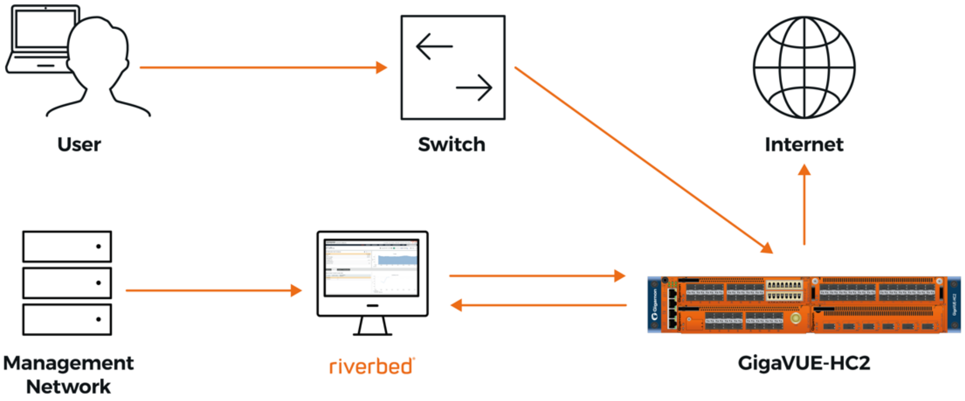
This Gigamon-Riverbed solution comprises of these prerequisites:

- GigaVUE HC2 chassis running GigaVUE-OS 5.7, one PRT-HC0-X24.
- GigaVUE-FM version 5.7 for configuration.
- Riverbed SteelCentral AppResponse 2000 Virtual Edition Version 11.7.0
- Riverbed NetProfiler Virtual Edition 10.17

  NOTE: This guide assumes all appliances are fully licensed for all features used, management network interfaces have been configured, and an account with sufficient admin privileges is used.

Architecture Overview

The logical architecture presents the joint solution comprising of Riverbed tools and Gigamon HC2 appliance. The reference architecture shows each component's position in the overall network infrastructure, where all network components and the out-of-band tools are directly connected to the HC2.



Access Credentials

The default access credentials for Gigamon and Riverbed products are listed below:

- Gigamon GigaVUE-FM access defaults:
  - Username: admin
    Password: admin123A!

No default management IP address

- Riverbed SteelCentral AppResponse Virtual Edition:
    - Username: admin
      Password: admin

NOTE: The GigaVUE-HC2 supports a Graphical User Interface (GUI) named H-VUE and a Command Line Interface (CLI). This document shows only the steps for configuring the GigaVUE-HC2 with Giga-VUE-FM. For the equivalent H-VUE and CLI configuration commands, refer to the *GigaVUE-OS H-VUE User's Guide and GigaVUE-OS CLI User's guide* respectively for the 5.7 release.

2 Configurations

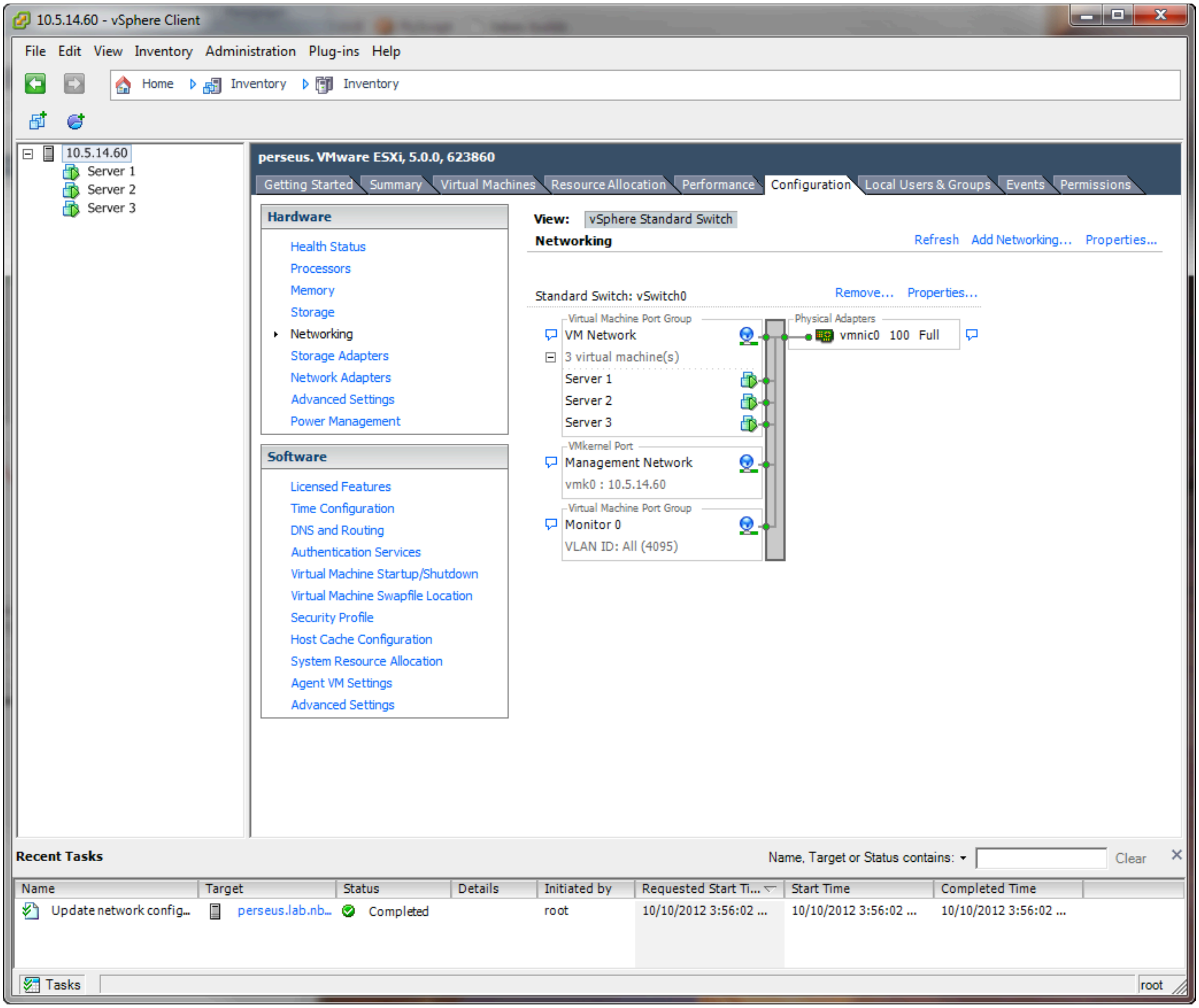
This chapter describes how to setup the Riverbed SteelCentral AppResponse virtual tool to receive traffic from the HC2 device. For simplicity, we will consider one source port and one destination port on the Gigamon HC2 to receive and send traffic. The source port will receive traffic from multiple TAPs and aggregators and by utilizing a Gigamon's flow maps, all the traffic is sent to one port on the HC2. The tool port will be connected to one of the vmnic on the ESXi hypervisor.

Riverbed SteelCentral AppResponse configuration: Monitor port and Virtual Interface Groups

The installation guide for AppResponse from Riverbed describes how to configure the port groups on the VMware ESXi. Follow the procedure provided in the guide if traffic source is same for management and user traffic. If the management traffic and the user traffic is through different vmnics, create another vSwitch and configure the 'Monitor 0' portgroup on this vSwitch.

Shown below are the 2 methods of configuring the portgroups depending on how your source traffic is fed to the AppResponse tool.

Method1 (both management and user traffic on same vmnic):



perseus. VMware ESXi, 5.0.0, 623860

View: vSphere Standard Switch

Networking

Standard Switch: vSwitch0

Virtual Machine Port Group
VM Network
3 virtual machine(s)
Server 1
Server 2
Server 3

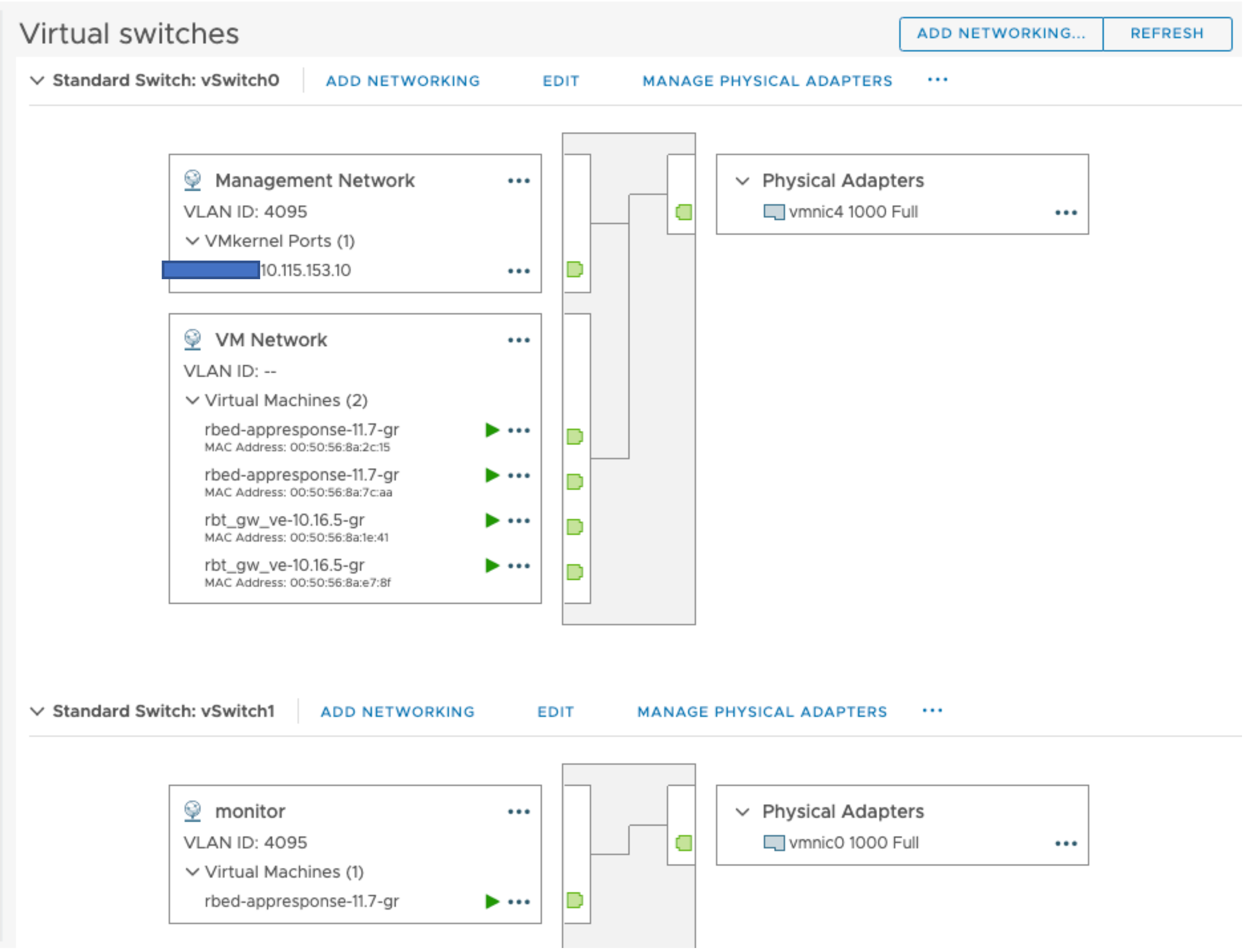
VMkernel Port
Management Network
vmk0 : 10.5.14.60

Virtual Machine Port Group
Monitor 0
VLAN ID: All (4095)

Physical Adapters
vmnic0 100 Full

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Update network config...	perseus.lab.nb...	Completed		root	10/10/2012 3:56:02 ...	10/10/2012 3:56:02 ...	10/10/2012 3:56:02 ...

Method 2 (Separate vmnic for management and user traffic):



Virtual switches

ADD NETWORKING... | REFRESH

Standard Switch: vSwitch0 | ADD NETWORKING | EDIT | MANAGE PHYSICAL ADAPTERS | •••

Management Network •••
VLAN ID: 4095
VMkernel Ports (1)
[redacted]10.115.153.10 •••

VM Network •••
VLAN ID: --
Virtual Machines (2)
rbed-appresponse-11.7-gr
MAC Address: 00:50:56:8a:2c:15
rbed-appresponse-11.7-gr
MAC Address: 00:50:56:8a:7c:aa
rbt_gw_ve-10.16.5-gr
MAC Address: 00:50:56:8a:1e:41
rbt_gw_ve-10.16.5-gr
MAC Address: 00:50:56:8a:e7:8f

Physical Adapters
vmnic4 1000 Full •••

Standard Switch: vSwitch1 | ADD NETWORKING | EDIT | MANAGE PHYSICAL ADAPTERS | •••

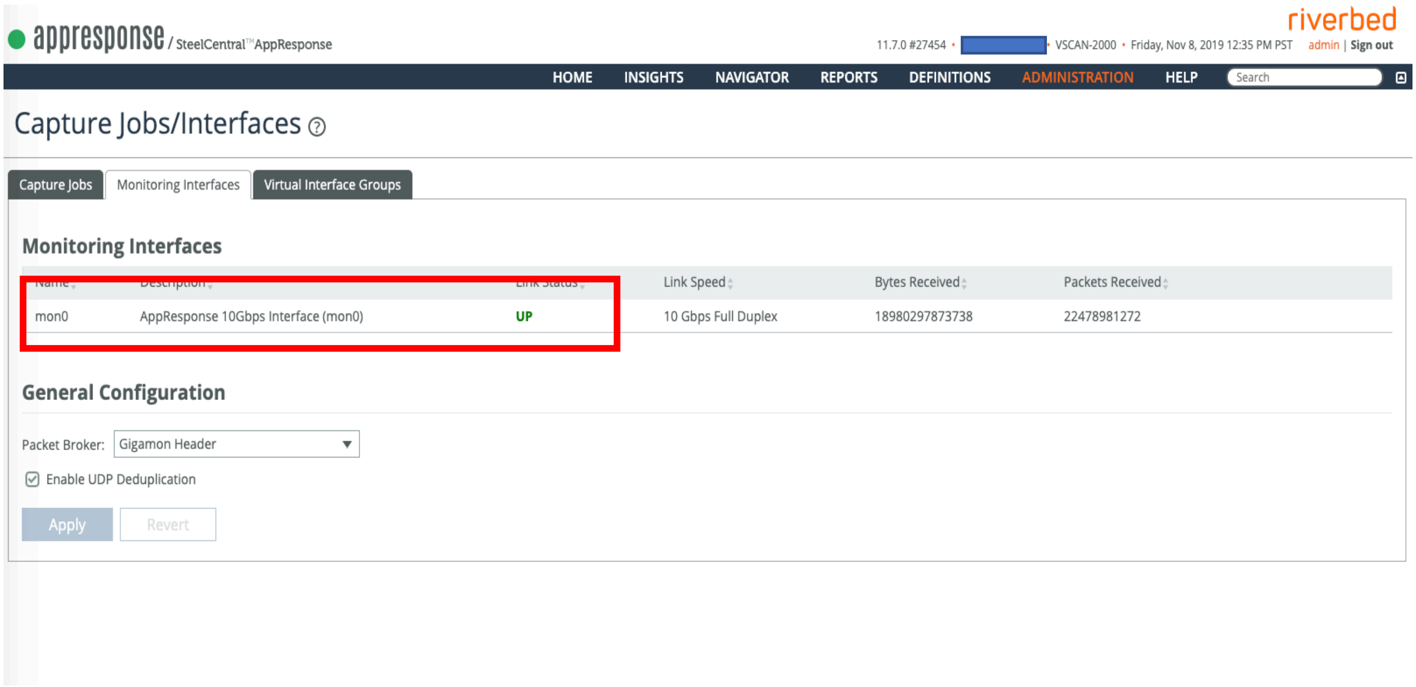
monitor •••
VLAN ID: 4095
Virtual Machines (1)
rbed-appresponse-11.7-gr

Physical Adapters
vmnic0 1000 Full •••

Configuring Virtual Interface Group (VIG) on AppResponse

Before configuring the VIG for the monitor interface, verify if the interface is Link status ‘UP’. Navigate to Administration and click on ‘Capture jobs/Interfaces’ under General traffic settings.

Click on ‘Monitoring Interfaces’.


appresponse / SteelCentral™ AppResponse
riverbed
11.7.0 #27454 • [redacted] • VSCAN-2000 • Friday, Nov 8, 2019 12:35 PM PST admin | Sign out
HOME INSIGHTS NAVIGATOR REPORTS DEFINITIONS ADMINISTRATION HELP Search
Capture Jobs Monitoring Interfaces Virtual Interface Groups

Capture Jobs/Interfaces

Monitoring Interfaces

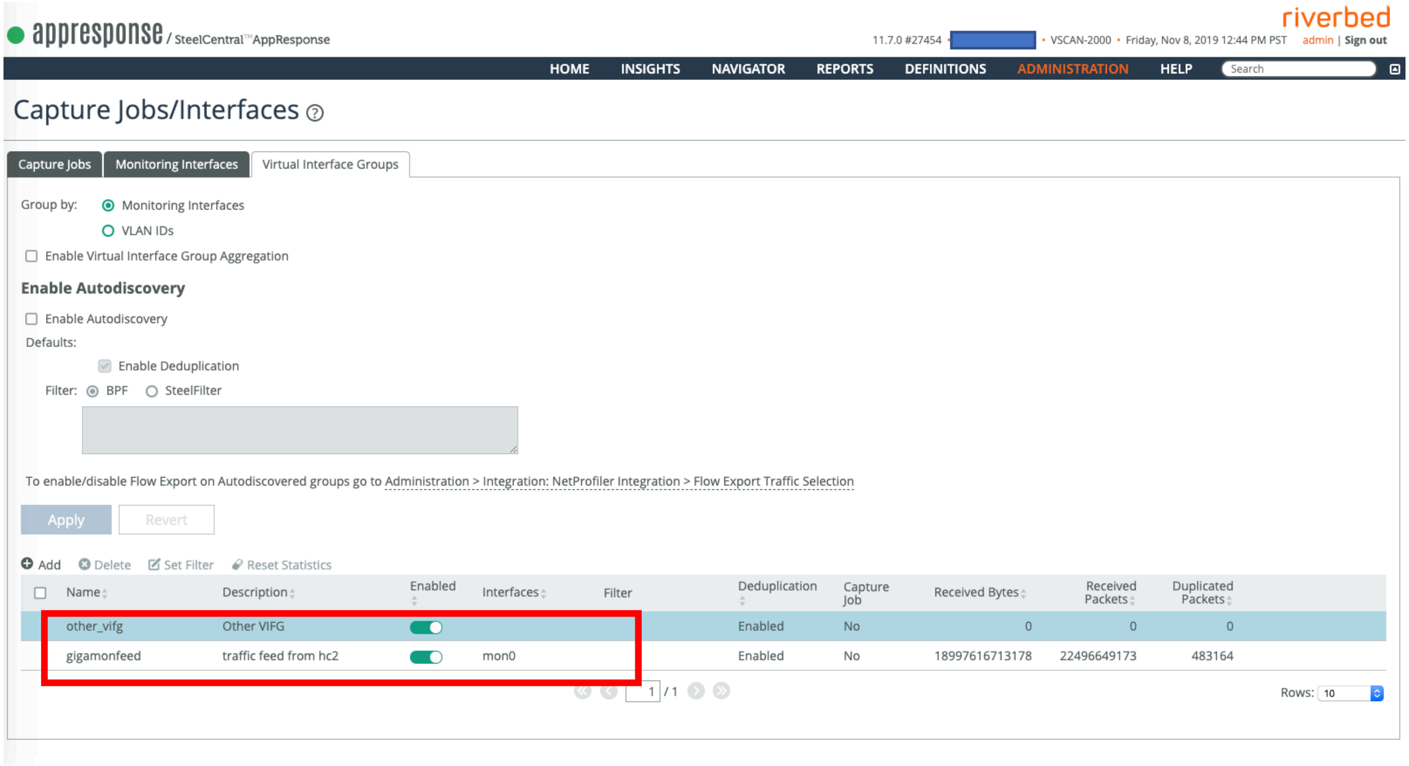
Name	Description	Link Status	Link Speed	Bytes Received	Packets Received
mon0	AppResponse 10Gbps Interface (mon0)	UP	10 Gbps Full Duplex	18980297873738	22478981272

General Configuration

Packet Broker: Gigamon Header

☑ Enable UDP Deduplication

Next, select the Virutal Interface Groups, click Add and configure the new virtual interface group with the mon 0 interface selected.


appresponse / SteelCentral™ AppResponse
riverbed
11.7.0 #27454 • [redacted] • VSCAN-2000 • Friday, Nov 8, 2019 12:44 PM PST admin | Sign out
HOME INSIGHTS NAVIGATOR REPORTS DEFINITIONS ADMINISTRATION HELP Search
Capture Jobs Monitoring Interfaces Virtual Interface Groups

Capture Jobs/Interfaces

Group by: ● Monitoring Interfaces
○ VLAN IDs

□ Enable Virtual Interface Group Aggregation

Enable Autodiscovery

□ Enable Autodiscovery

Defaults:

☑ Enable Deduplication

Filter: ● BPF ○ SteelFilter

To enable/disable Flow Export on Autodiscovered groups go to Administration > Integration: NetProfiler Integration > Flow Export Traffic Selection

Name	Description	Enabled	Interfaces	Filter	Deduplication	Capture Job	Received Bytes	Received Packets	Duplicated Packets
other_vifg	Other VIFG	●			Enabled	No	0	0	0
gigamonfeed	traffic feed from hc2	●	mon0		Enabled	No	18997616713178	22496649173	483164

GigaVUE-HC2 Configuration: Ports and Flow maps

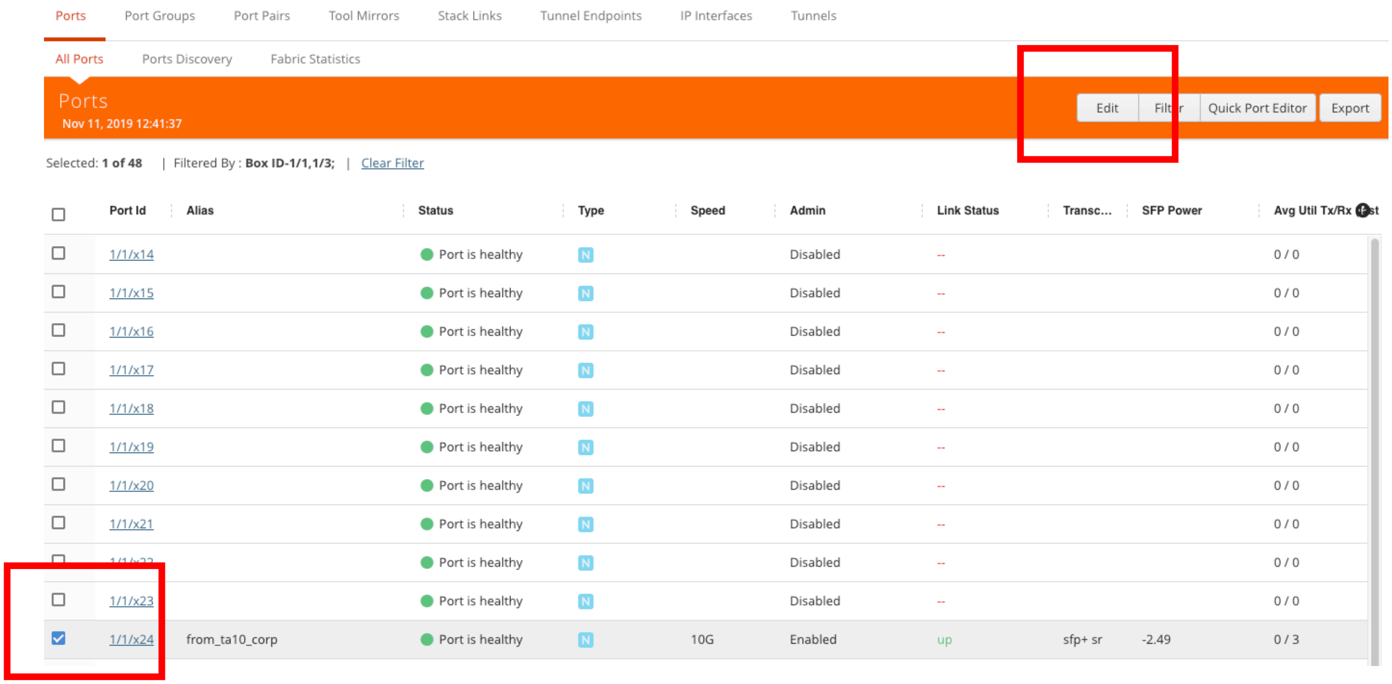
This section covers the HC2 configuration with respect to ports and maps associated with sending traffic to AppResponse. In this deployment, the source traffic is a single port. In a more realistic deployment, there is more than one source port either on the HC2 or on a TA (Traffic Aggregator) device behind this HC2. Based on where traffic is aggregated from multiple TAP points, the map's network port will have one or more ports. In this deployment, 1/1/x24 is the source port and 1/3/x12 is the destination tool port which is the monitor port on the AppResponse.

The configuration will have 3 basic steps:

- Configure the network port
- Configure the tool port
- Configure a flow map

Step 1: Configure the network port

1. Login to the GigaVUE-FM, select Physical Nodes (Under Physical)
2. Select the HC2 from the list of physical nodes.
3. Choose the port that needs to be configured as network port and click 'Edit'.

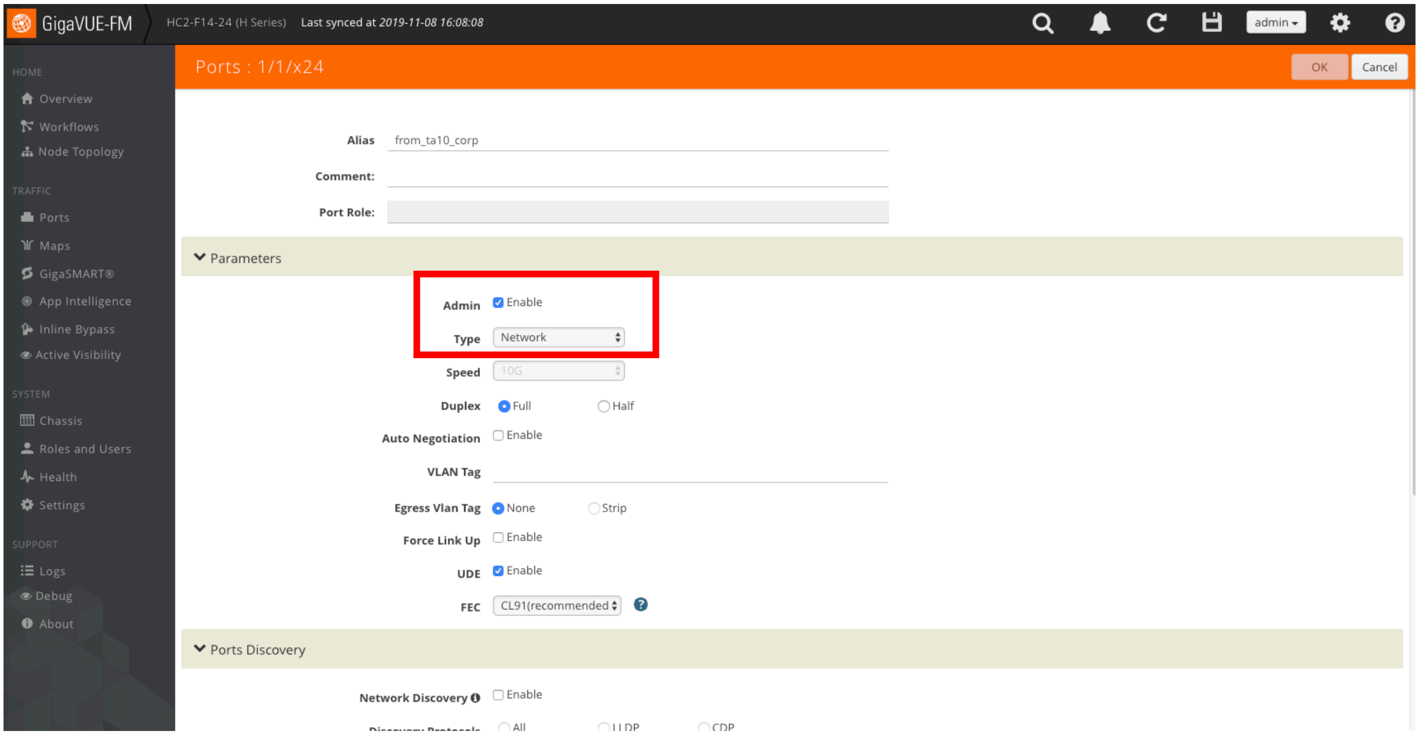


Ports
Nov 11, 2019 12:41:37

Selected: **1 of 48** | Filtered By : **Box ID-1/1,1/3;** | Clear Filter

☐	Port Id	Alias	Status	Type	Speed	Admin	Link Status	Transc...	SFP Power	Avg Util Tx/Rx
☐	1/1/x14		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x15		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x16		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x17		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x18		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x19		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x20		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x21		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x22		● Port is healthy	N		Disabled	--			0 / 0
☐	1/1/x23		● Port is healthy	N		Disabled	--			0 / 0
☑	1/1/x24	from_ta10_corp	● Port is healthy	N	10G	Enabled	up	sfp+ sr	-2.49	0 / 3

4. Provide a suitable alias to label the port. Select 'Network' for the type of port.
5. Click 'OK'.



Last synced at 2019-11-08 16:08:08

Ports : 1/1/x24

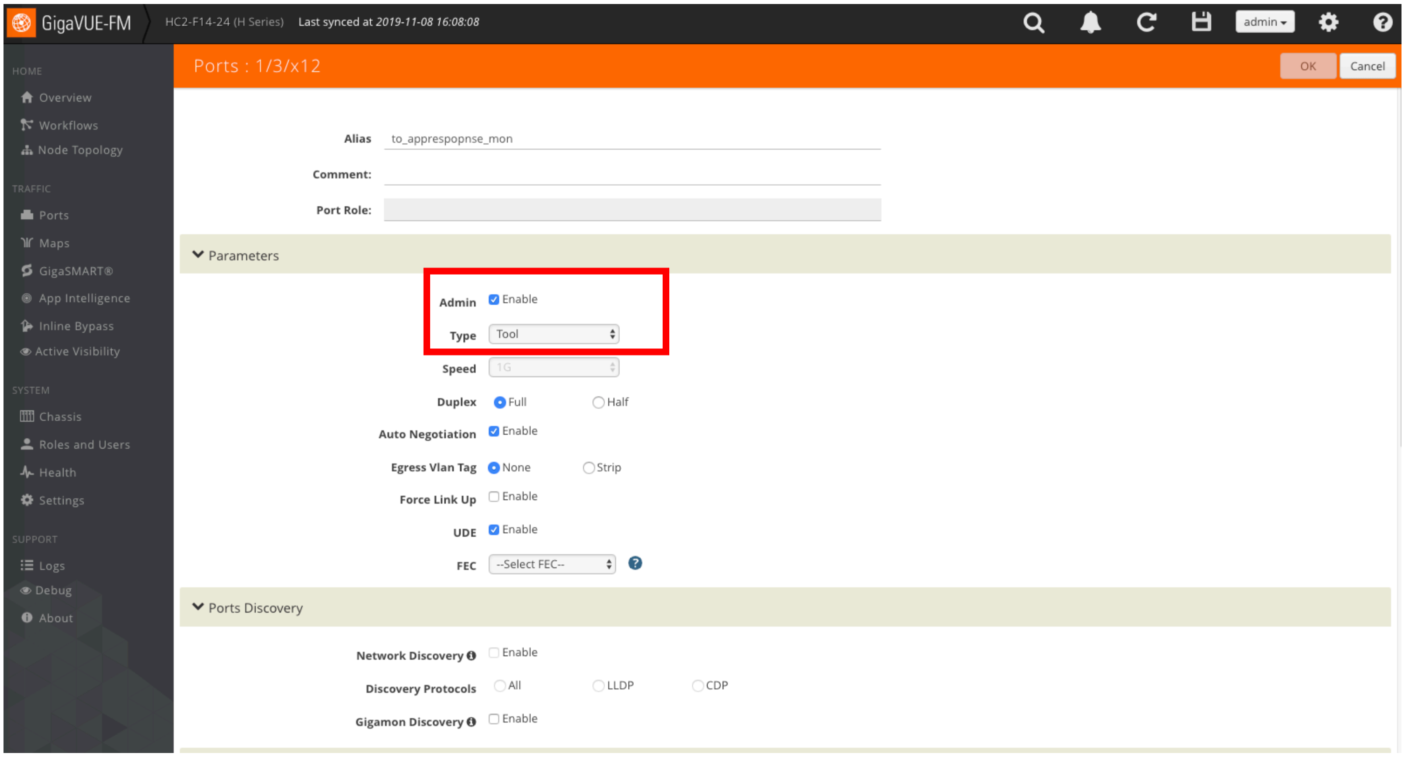
Alias: from_ta10_corp
Comment:
Port Role:

Admin: ☑ Enable
Type: Network
Speed: 10G
Duplex: ● Full ○ Half
Auto Negotiation: □ Enable
VLAN Tag:
Egress Vlan Tag: ● None ○ Strip
Force Link Up: □ Enable
UDE: ☑ Enable
FEC: CL91(recommended)

Network Discovery: □ Enable
Discovery Protocols: ○ All ○ LLDP ○ CDP

Step 2:

1. Choose the port that needs to be configured as tool port and click 'Edit'.
2. Provide a suitable alias to label the port. Select 'Tool' for the type of port.
3. Click 'OK'.



Last synced at 2019-11-08 16:08:08

Ports : 1/3/x12

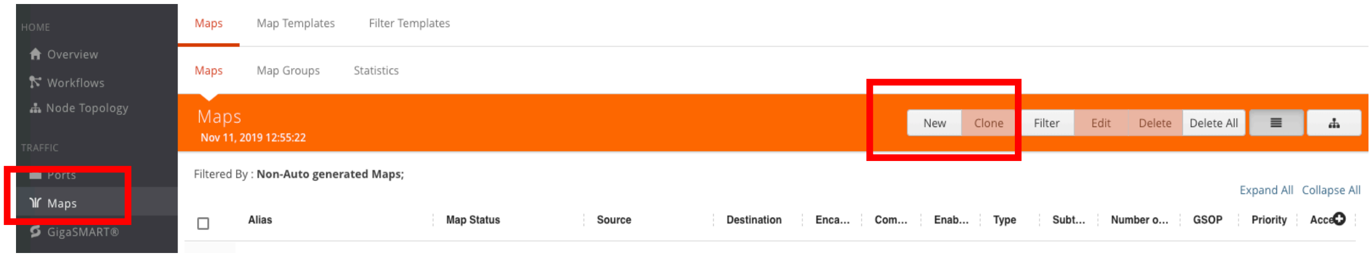
Alias: to_apprespopnse_mon
Comment:
Port Role:

Admin: ☑ Enable
Type: Tool
Speed: 1G
Duplex: ● Full ○ Half
Auto Negotiation: ☑ Enable
Egress Vlan Tag: ● None ○ Strip
Force Link Up: □ Enable
UDE: ☑ Enable
FEC: --Select FEC--

Network Discovery: □ Enable
Discovery Protocols: ○ All ○ LLDP ○ CDP
Gigamon Discovery: □ Enable

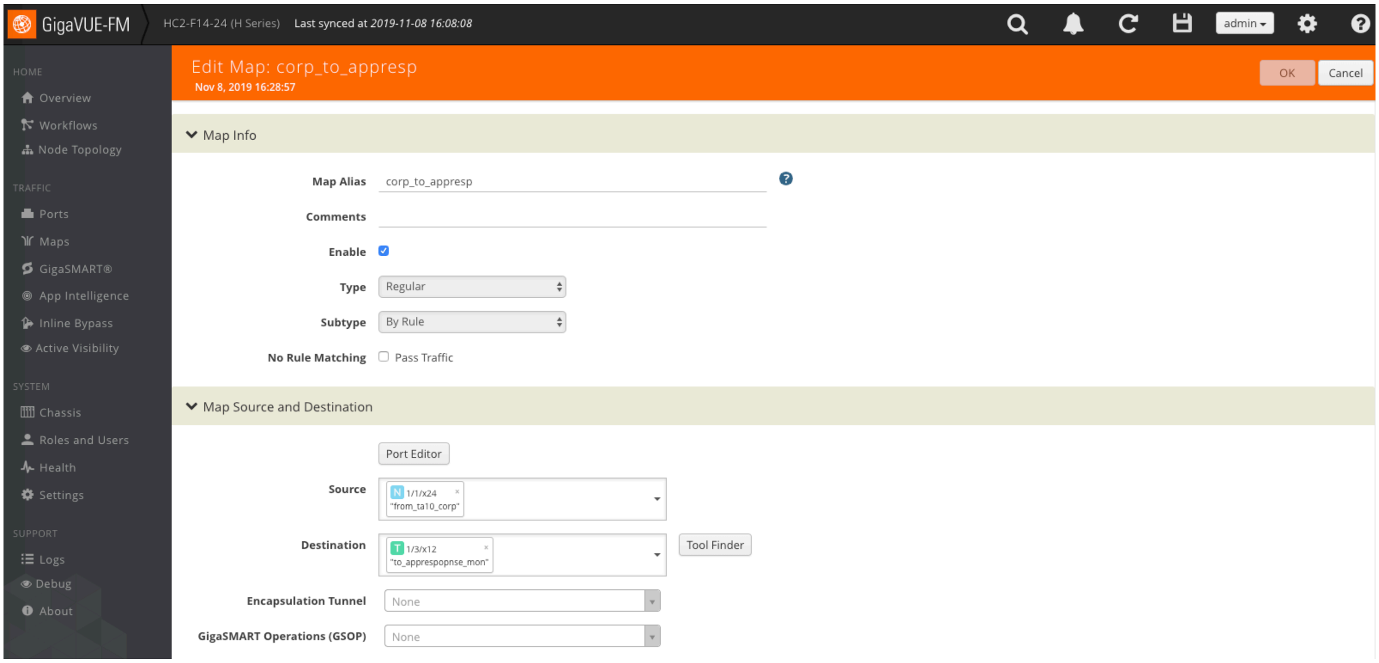
Step 3:

1. From the GigaVUE-FM, click on Maps from the menu on the left.
2. Click New to enter the map details.



Filtered By : **Non-Auto generated Maps;**

3. Provide a map alias, Click on ‘Enable’ on Map Info.
4. Select Regular under type and ‘By Rule’ under Subtype.
5. Select the appropriate source and Destination ports based on the configuration in Step 1 and 2.



Last synced at *2019-11-08 16:08:08*

Edit Map: corp_to_appresp
Nov 8, 2019 16:28:57

Map Alias: corp_to_appresp

Comments:

Enable: ☑

Type: Regular

Subtype: By Rule

No Rule Matching: ☐ Pass Traffic

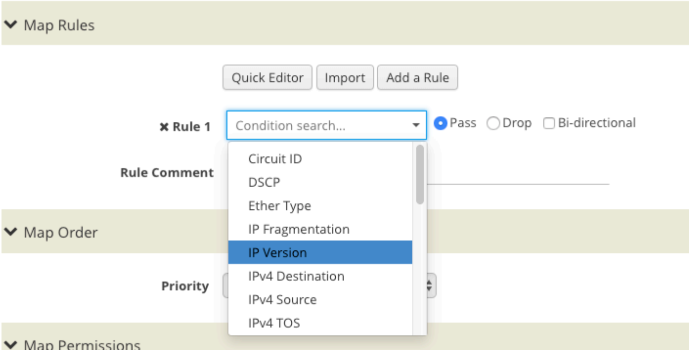
Source: N 1/1/x24 "from_ta10_corp"

Destination: T 1/3/x12 "to_apprespopnse_mon"

Encapsulation Tunnel: None

GigaSMART Operations (GSOP): None

6. Under Map Rules, click ‘Add Rule’, click Condition Search and choose IP Version from drop-down. Select ‘Pass’.


⌄ Map Rules

Quick Editor | Import | Add a Rule

✖ Rule 1 Condition search... ● Pass ○ Drop □ Bi-directional

Rule Comment

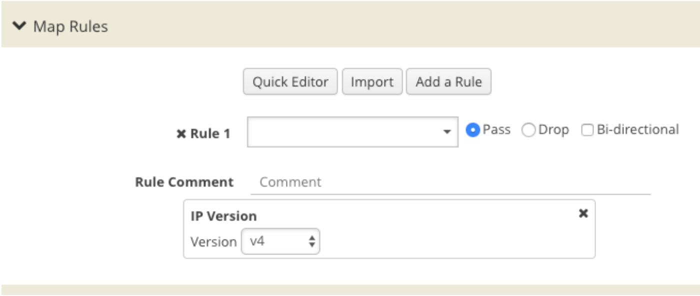
- Circuit ID
- DSCP
- Ether Type
- IP Fragmentation
- IP Version
- IPv4 Destination
- IPv4 Source
- IPv4 TOS

⌄ Map Order

Priority

⌄ Map Permissions

7. Select Version v4. Click OK to create the map.


⌄ Map Rules

Quick Editor | Import | Add a Rule

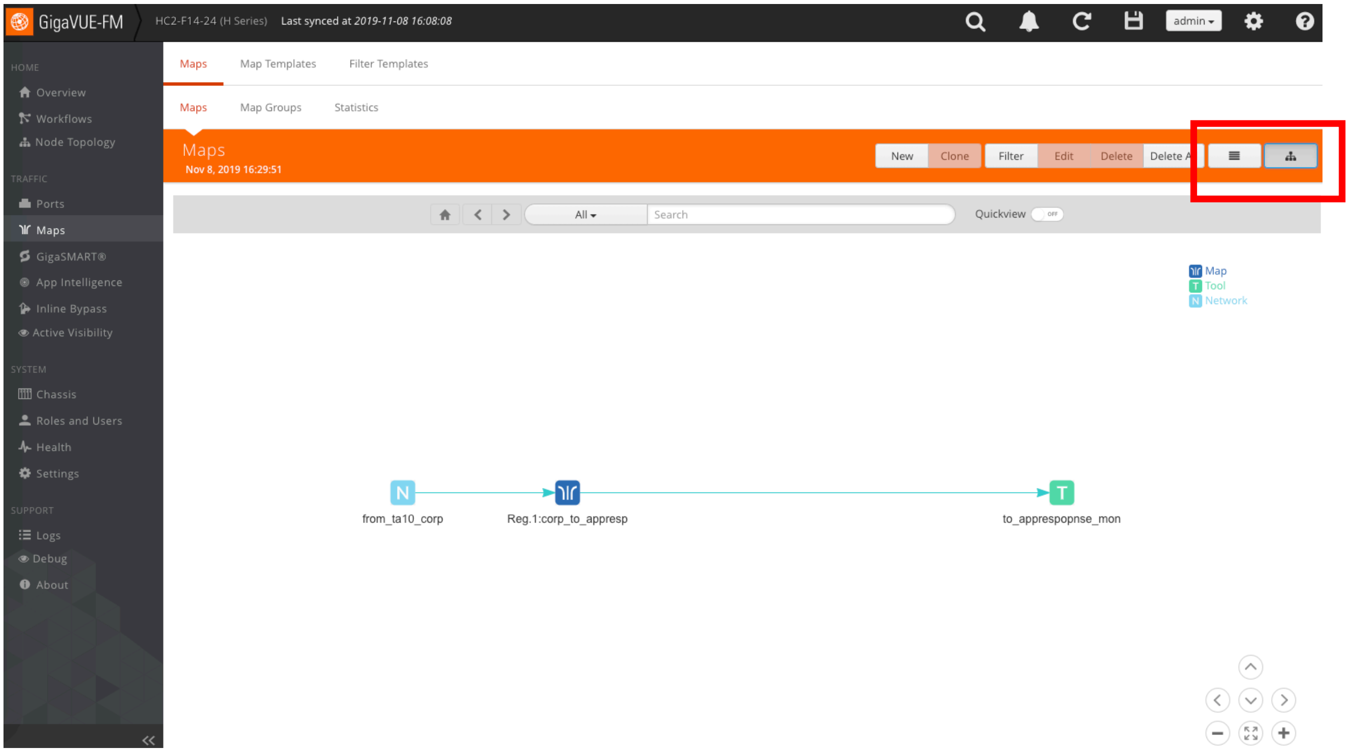
✖ Rule 1 ● Pass ○ Drop □ Bi-directional

Rule Comment Comment

IP Version ✖

Version v4

8. Verify map topology view by clicking on topology view.



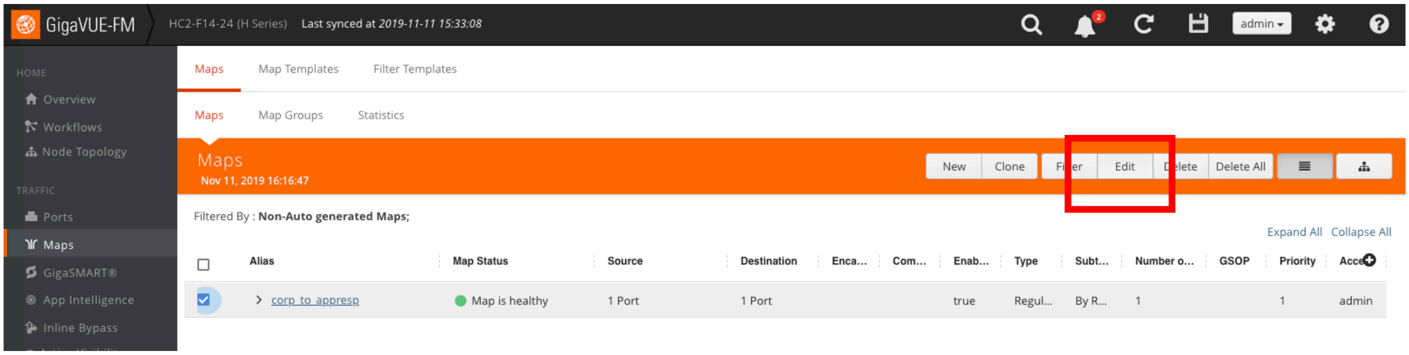
GigaVUE-HC2 Configuration: Basic filtering

This section provides the necessary steps to configure basic filtering (L2-L4) on the Gigamon HC2 device. These filters can be configured either on the tool port or the flow map itself and the best use-case of the filters is that it vastly reduces the amount of traffic sent to the Riverbed tool.

Filtering on fabric maps

To add filters on the fabric maps, follow the steps below:

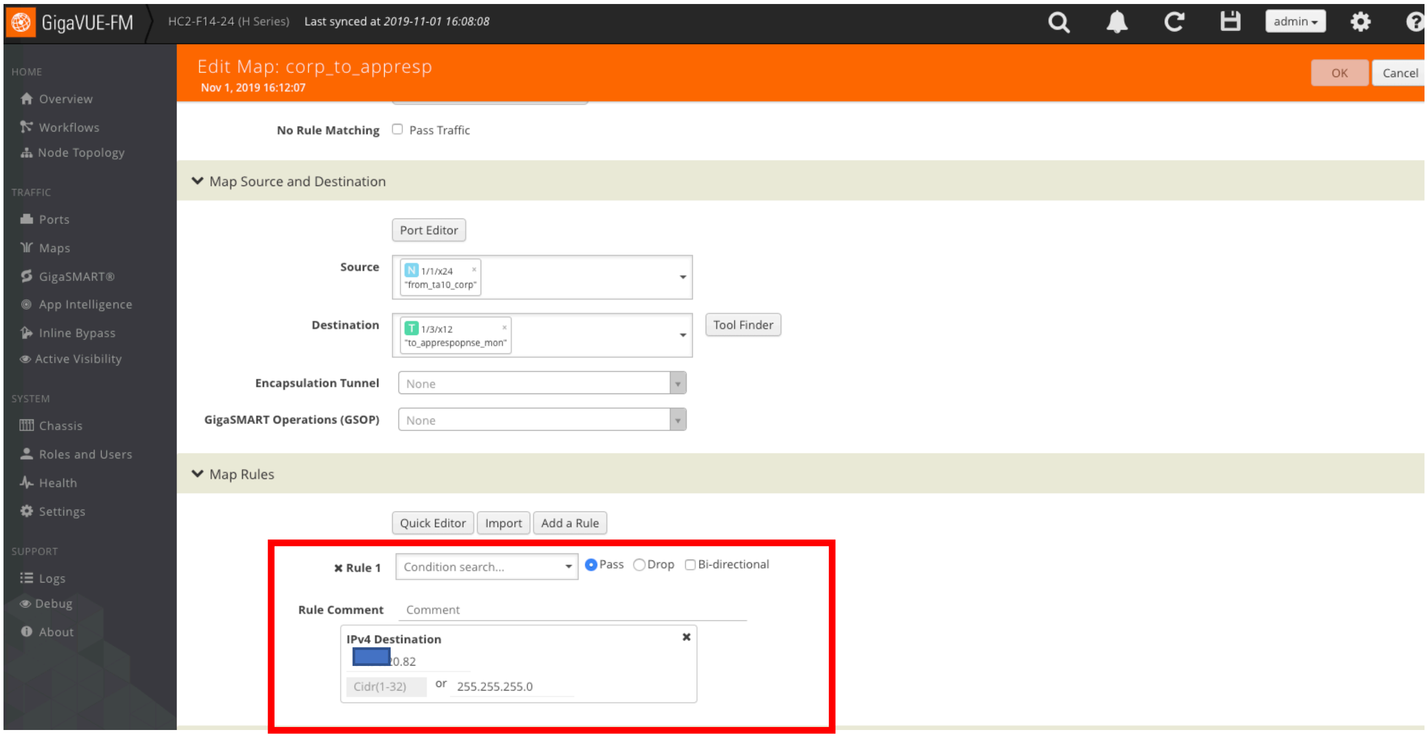
1. Select the map that was created and click Edit



Filtered By : **Non-Auto generated Maps;**

□	Alias	Map Status	Source	Destination	Enca...	Com...	Enab...	Type	Subt...	Number o...	GSOP	Priority	Acce...
☑	corp_to_appresp	● Map is healthy	1 Port	1 Port			true	Regul...	By R...	1		1	admin

2. Under Map Rules, where Rule 1 is created, click on Condition search and choose IPv4 Destination. A rule comment can be added and the IPv4 destination address can be configured with the netmask. Click OK.



Edit Map: corp_to_appresp

Nov 1, 2019 16:12:07

No Rule Matching □ Pass Traffic

Source: N 1/1/x24 "from_ta10_corp"

Destination: T 1/3/x12 "to_apprespopnse_mon"

Encapsulation Tunnel: None

GigaSMART Operations (GSOP): None

× Rule 1 Condition search... ● Pass ○ Drop □ Bi-directional

Rule Comment: Comment

IPv4 Destination ×

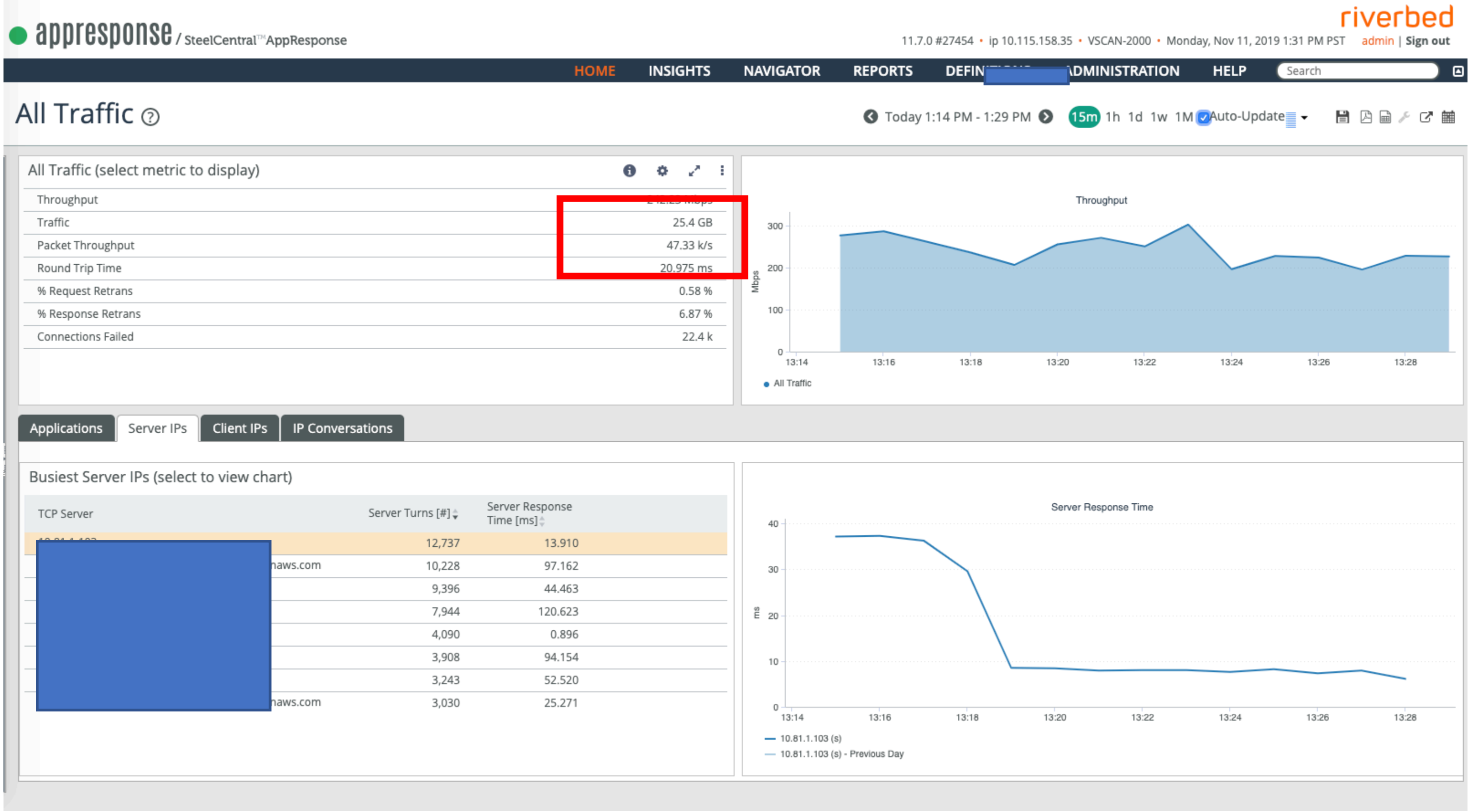
[redacted]0.82

Cidr(1-32) or 255.255.255.0

Verifying traffic on Riverbed AppResponse

The next few screenshots will show the effect of basic filtering applied on Gigamon's HC2 device so that the AppResponse tool is not overwhelmed by all the traffic that is being tapped and fed to the packet broker.

Without filtering



11.7.0 #27454 • ip 10.115.158.35 • VSCAN-2000 • Monday, Nov 11, 2019 1:31 PM PST admin | Sign out

All Traffic ?

Today 1:14 PM - 1:29 PM ☑ Auto-Update

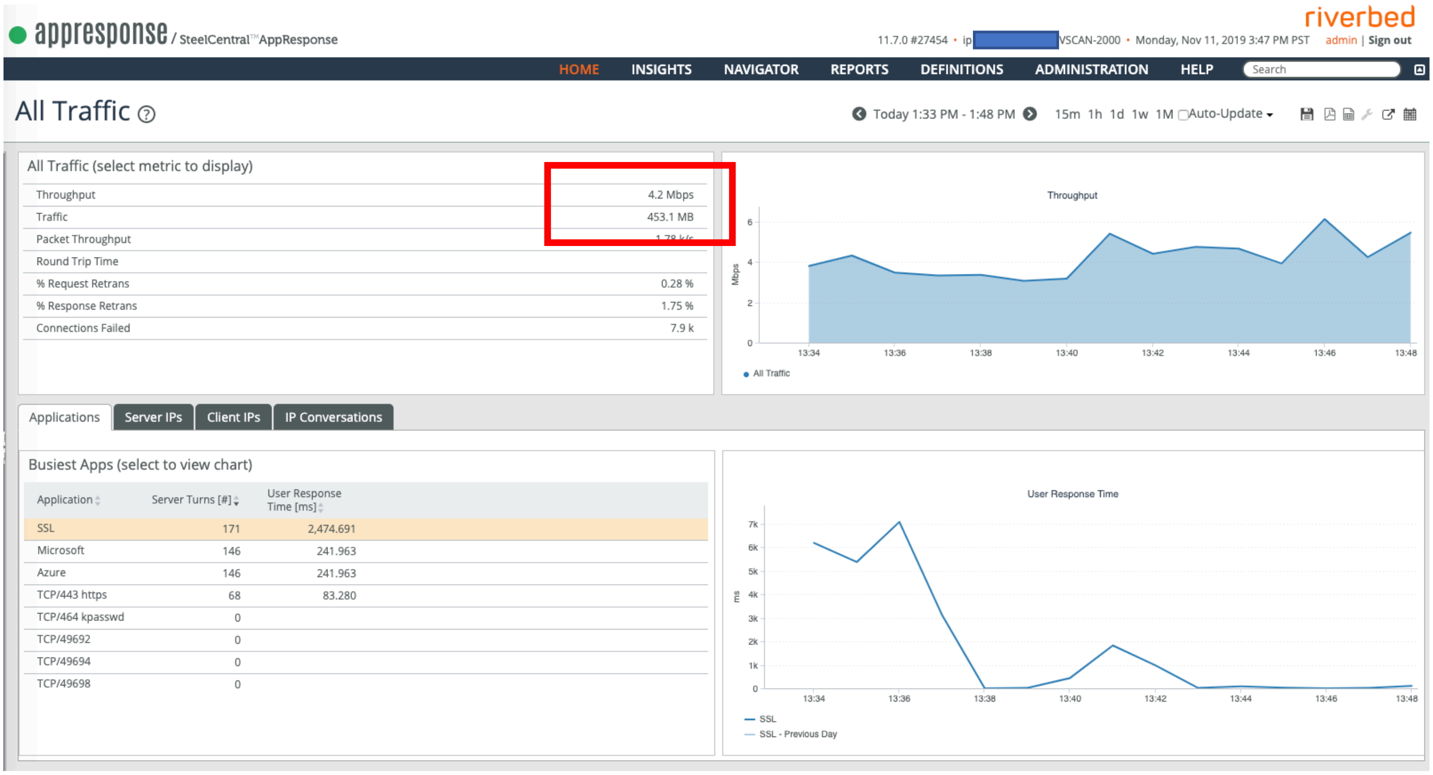
All Traffic (select metric to display)

Throughput	242.25 Mbps
Traffic	25.4 GB
Packet Throughput	47.33 k/s
Round Trip Time	20.975 ms
% Request Retrans	0.58 %
% Response Retrans	6.87 %
Connections Failed	22.4 k

Busiest Server IPs (select to view chart)

TCP Server	Server Turns [#]	Server Response Time [ms]
[redacted]	12,737	13.910
[redacted]aws.com	10,228	97.162
[redacted]	9,396	44.463
[redacted]	7,944	120.623
[redacted]	4,090	0.896
[redacted]	3,908	94.154
[redacted]	3,243	52.520
[redacted]aws.com	3,030	25.271

With filtering


appresponse / SteelCentral™ AppResponse
riverbed
11.7.0 #27454 • ip[redacted]VSCAN-2000 • Monday, Nov 11, 2019 3:47 PM PST admin | Sign out
HOME INSIGHTS NAVIGATOR REPORTS DEFINITIONS ADMINISTRATION HELP Search
All Traffic
Today 1:33 PM - 1:48 PM 15m 1h 1d 1w 1M Auto-Update
Throughput
Mbps
All Traffic
Applications
Server IPs
Client IPs
IP Conversations
User Response Time
ms
SSL
SSL - Previous Day

All Traffic (select metric to display)

Throughput	4.2 Mbps
Traffic	453.1 MB
Packet Throughput	1.78 k/s
Round Trip Time	
% Request Retrans	0.28 %
% Response Retrans	1.75 %
Connections Failed	7.9 k

Busiest Apps (select to view chart)

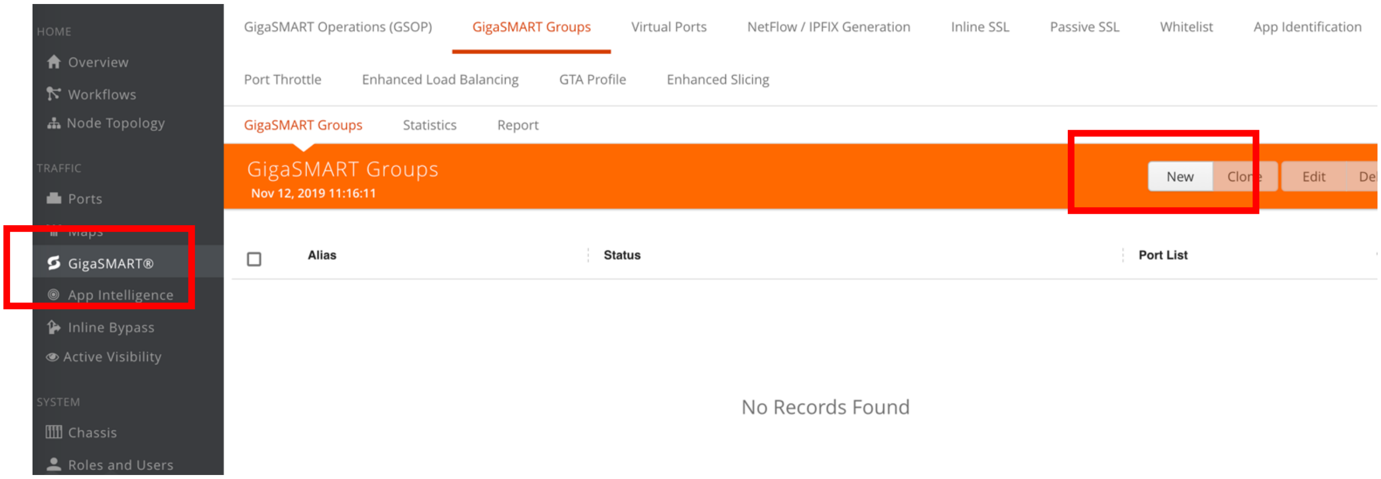
Application	Server Turns [#]	User Response Time [ms]
SSL	171	2,474.691
Microsoft	146	241.963
Azure	146	241.963
TCP/443 https	68	83.280
TCP/464 kpasswd	0	
TCP/49692	0	
TCP/49694	0	
TCP/49698	0	

GigaVUE-HC2 Configuration: GigaSMART functionalities

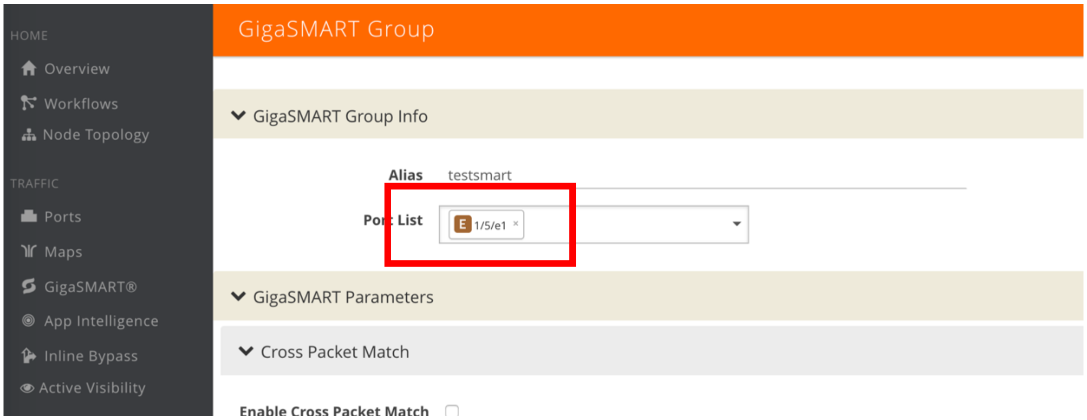
The GigaSMART features are beneficial to perform other manipulations such as packet deduplication, header stripping, masking and load-balancing. In the below example we can see how GigaSMART is configured and how it is applied to a map.

Step 1: Configure a GigaSMART Group

1. Click GigaSMART on the menu options and click GigaSMART Groups tab. Click New.



2. Select the engine port and scroll down to the various default configurations. You can change any parameter on the desired operation.



GigaSMART Group

GigaSMART Group Info

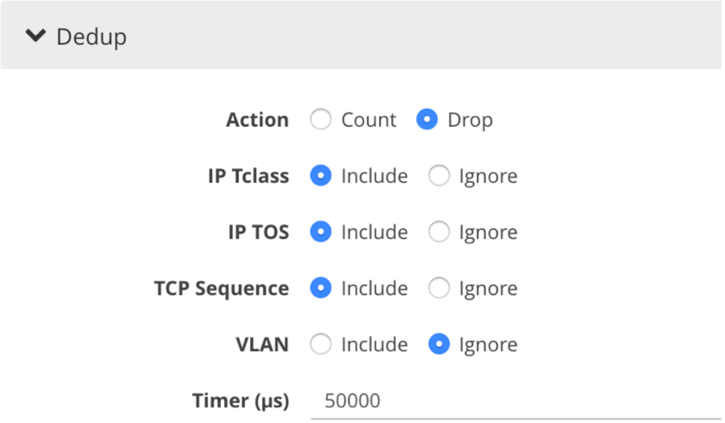
Alias: testsmart

Port List: E 1/5/e1 ×

GigaSMART Parameters

Cross Packet Match

Enable Cross Packet Match □

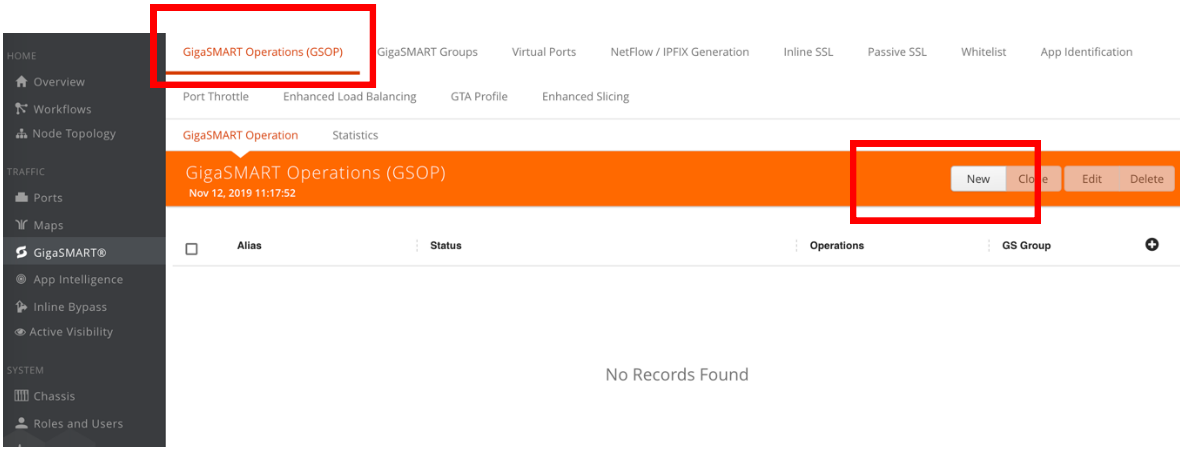


Dedup

Action	○ Count	● Drop
IP Tclass	● Include	○ Ignore
IP TOS	● Include	○ Ignore
TCP Sequence	● Include	○ Ignore
VLAN	○ Include	● Ignore
Timer (µs)	50000	

Step 2: Configure a GigaSMART Operation

1. Click GigaSMART Operations tab and click New.

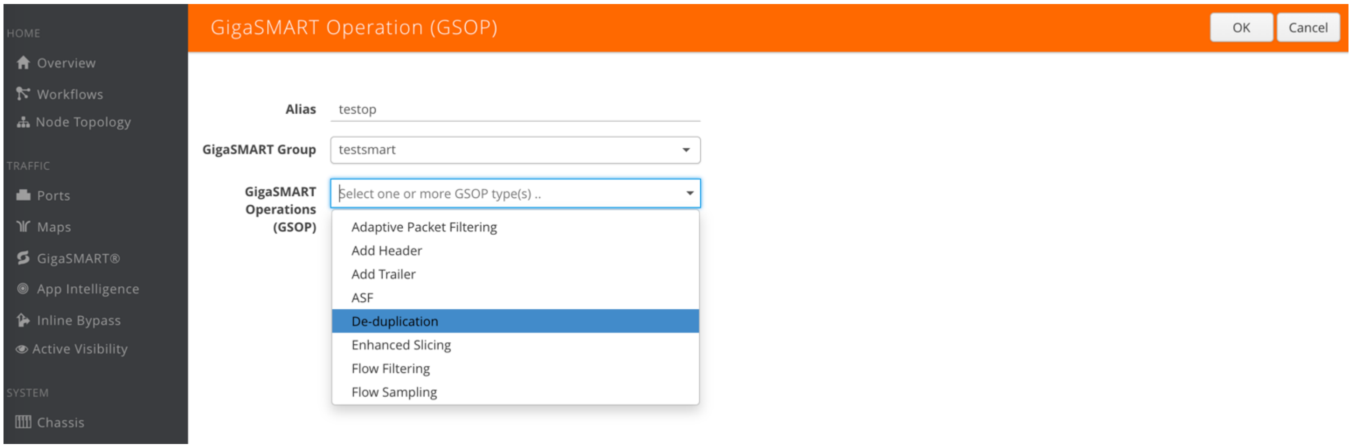


GigaSMART Operations (GSOP)
Nov 12, 2019 11:17:52

□	Alias	Status	Operations	GS Group

No Records Found

2. Provide an alias for the GSOP and select the Group from the dropdown. Select the GSOP from the list. Configure additional parameters based on the operation selected.



GigaSMART Operation (GSOP)

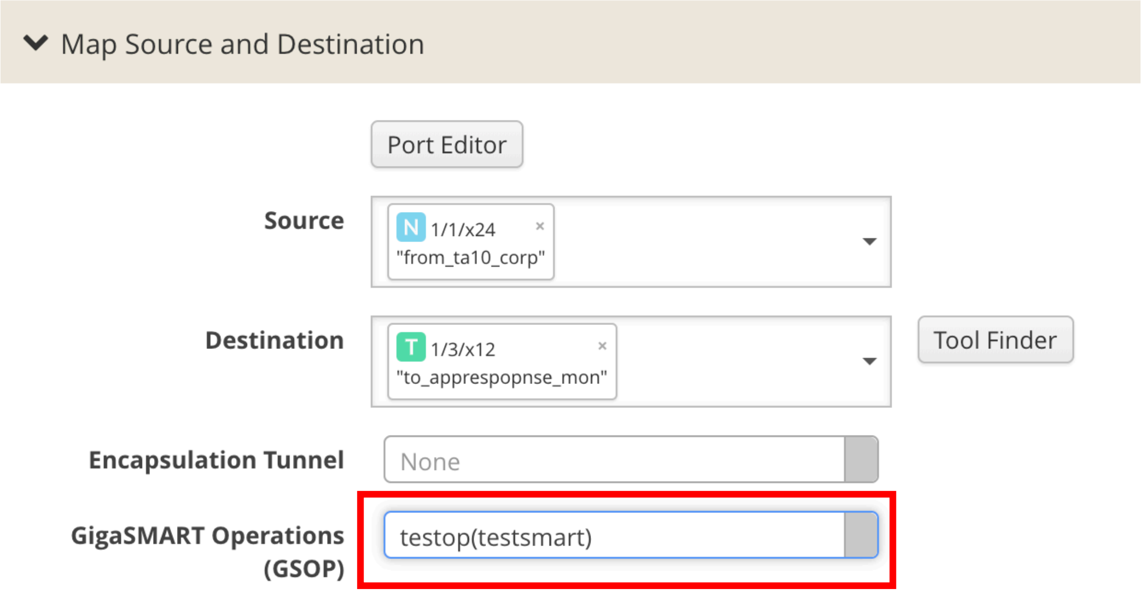
Alias: testop

GigaSMART Group: testsmart

GigaSMART Operations (GSOP): Select one or more GSOP type(s) ..

Step 3: Configure map with the GSOP

1. Click on Maps and select the map to be configure with the GSOP and click Edit.
2. Scroll down to Map source and destination and select the GSOP drop down with the GSOP created in Step 2.



Map Source and Destination

Source: N 1/1/x24 "from_ta10_corp"

Destination: T 1/3/x12 "to_aprespopnse_mon"

Encapsulation Tunnel: None

GigaSMART Operations (GSOP): testop(testsmart)

Use Case: Sending flow data to NetProfiler

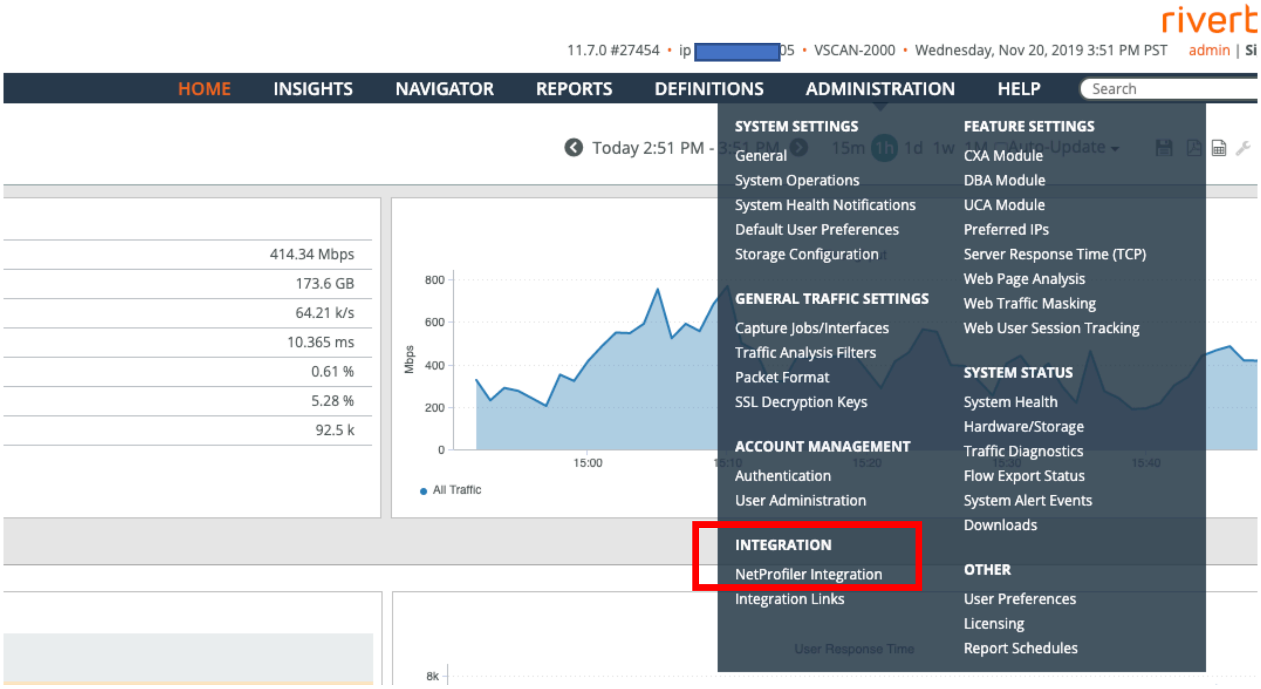
Riverbed's NetProfiler can be integrated with the SteelCentral AppResponse for additional analysis based on the flow data from AppResponse. SteelCentral NetProfiler gives an end-to-end monitoring and reporting capability when integrated with Gigamon Visibility Platform and SteelCentral AppResponse.

To integrate the NetProfiler tool with AppResponse, install the Virtual Edition preferably in the same ESXi environment as the AppResponse and provide a management IP address. The IP address must be able to reach the AppResponse tool for the flows to be forwarded.

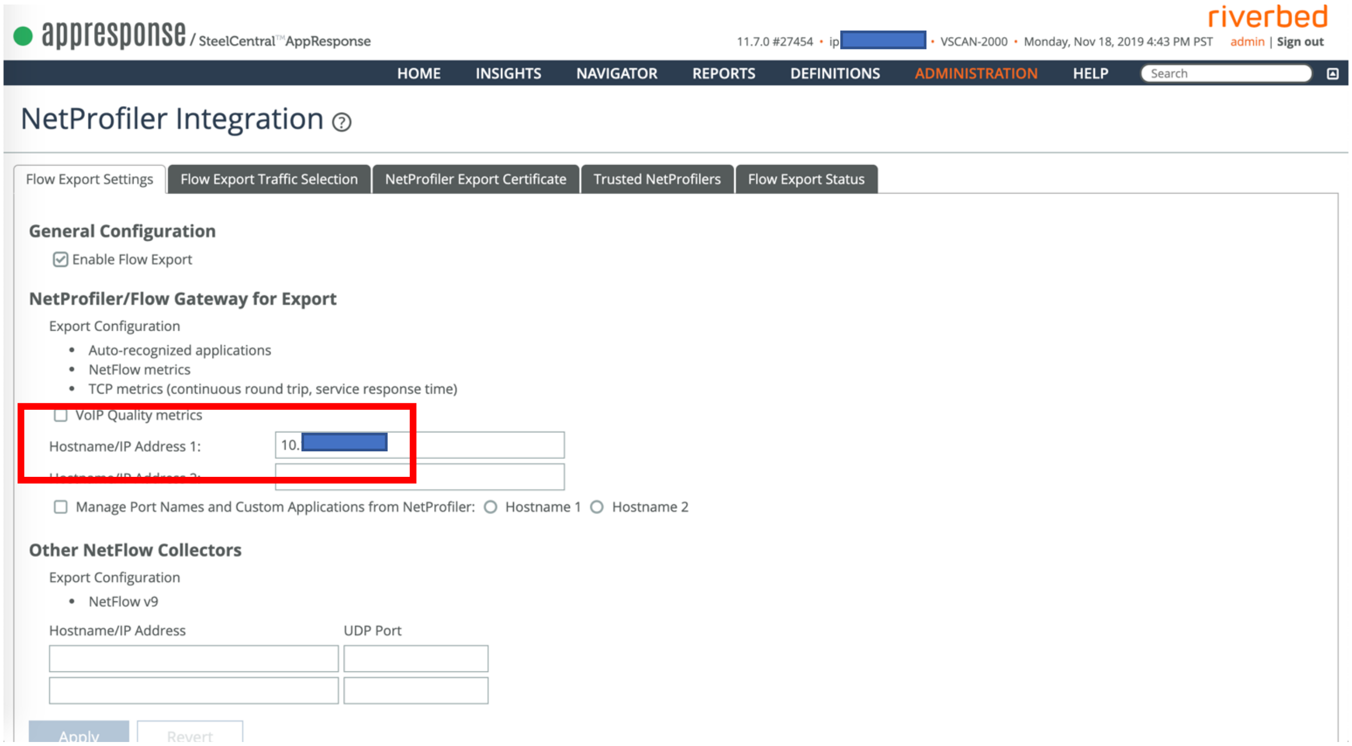
Configure NetProfiler Integration on AppResponse

Step 1: Add Netprofiler details on AppResponse

1. Under Administration, look for Integration and select NetProfiler Integration.



2. On ‘Flow Export Settings’, the ‘Enable Flow Export’ box must be checked. Provide the IP address/Hostname for the NetProfiler and click Apply.



11.7.0 #27454 • ip [redacted] • VSCAN-2000 • Monday, Nov 18, 2019 4:43 PM PST

NetProfiler Integration

General Configuration

☑ Enable Flow Export

NetProfiler/Flow Gateway for Export

Export Configuration

- Auto-recognized applications
- NetFlow metrics
- TCP metrics (continuous round trip, service response time)

□ VoIP Quality metrics

Hostname/IP Address 1: 10.[redacted]

Hostname/IP Address 2:

□ Manage Port Names and Custom Applications from NetProfiler: ○ Hostname 1 ○ Hostname 2

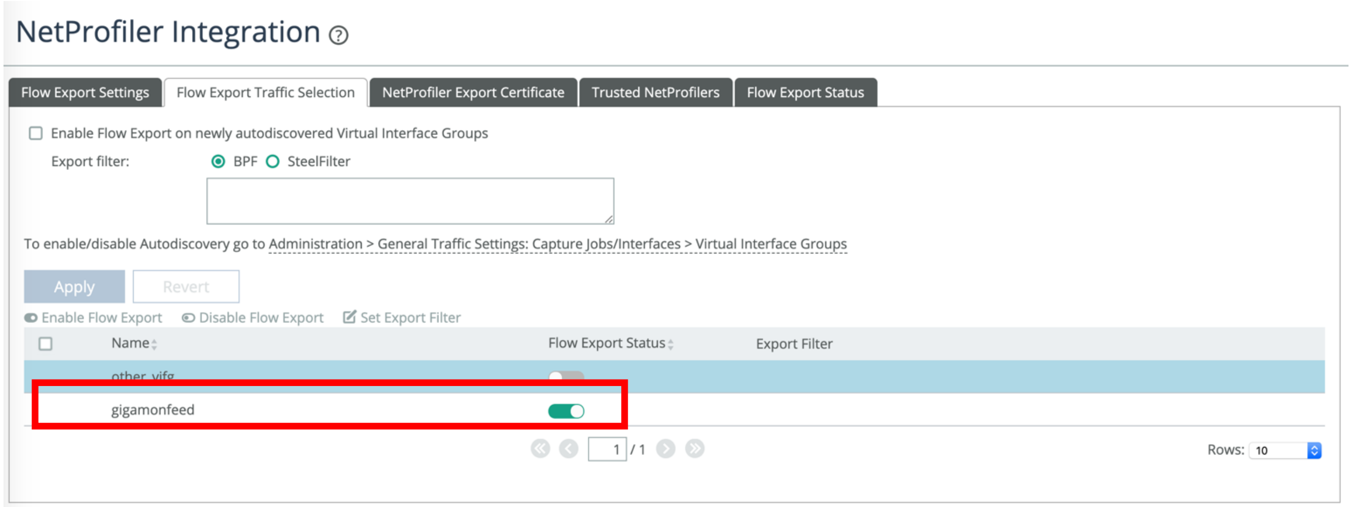
Other NetFlow Collectors

Export Configuration

- NetFlow v9

Hostname/IP Address UDP Port

3. Navigate to Flow Export Traffic Selection, enable the appropriate interface which needs to forward the flows to the NetProfiler.



NetProfiler Integration

□ Enable Flow Export on newly autodiscovered Virtual Interface Groups

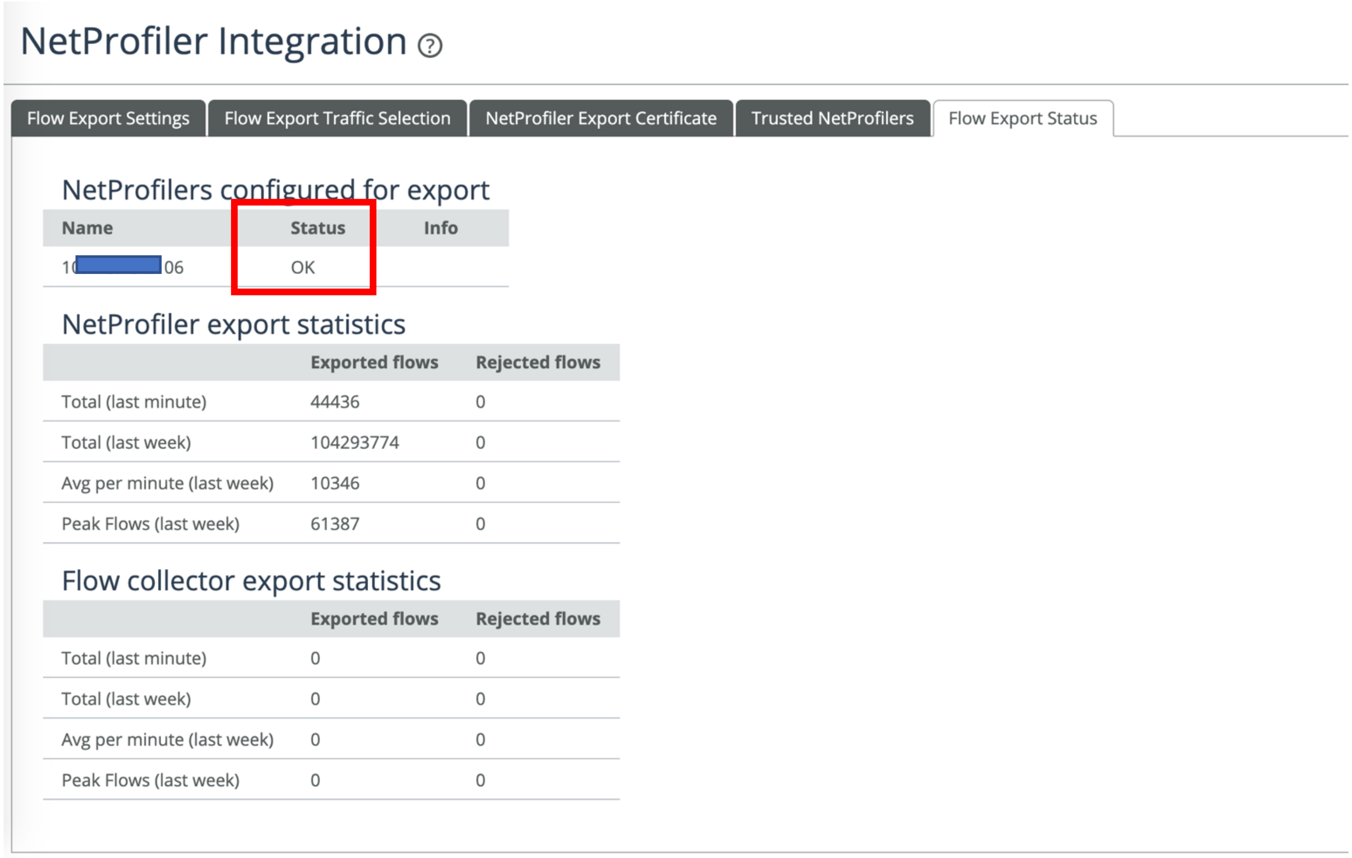
Export filter: ● BPF ○ SteelFilter

To enable/disable Autodiscovery go to Administration > General Traffic Settings: Capture Jobs/Interfaces > Virtual Interface Groups

□	Name	Flow Export Status	Export Filter
	other_vifg	○	
	gigamonfeed	●	

1 / 1 Rows: 10

4. If necessary, configure the Export Certificates as mentioned in the User Guide for AppResponse. Click on Flow Export Status to verify that the flows are forwarded to the NetProfiler.



NetProfiler Integration ?

Flow Export Settings | Flow Export Traffic Selection | NetProfiler Export Certificate | Trusted NetProfilers | Flow Export Status

NetProfilers configured for export

Name	Status	Info
1[redacted]06	OK	

NetProfiler export statistics

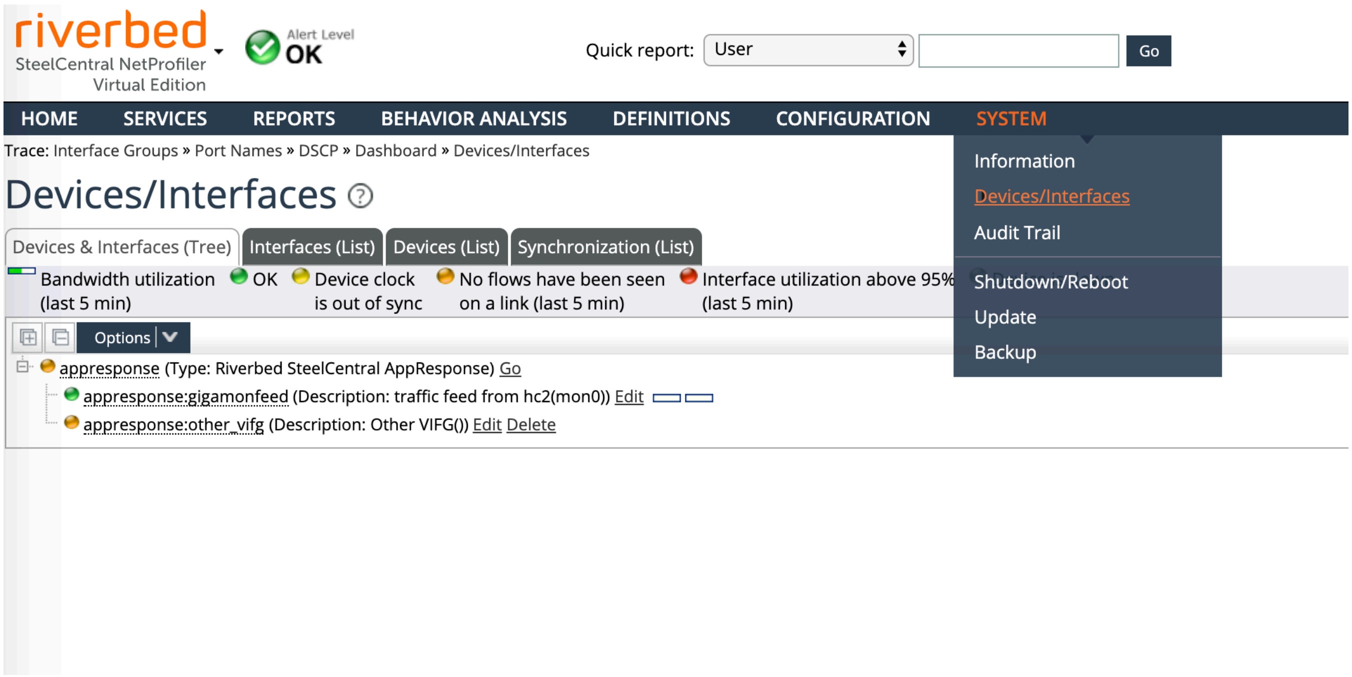
	Exported flows	Rejected flows
Total (last minute)	44436	0
Total (last week)	104293774	0
Avg per minute (last week)	10346	0
Peak Flows (last week)	61387	0

Flow collector export statistics

	Exported flows	Rejected flows
Total (last minute)	0	0
Total (last week)	0	0
Avg per minute (last week)	0	0
Peak Flows (last week)	0	0

Step 2: Verify reports and dashboards on NetProfiler

1. Login to the NetProfiler with the IP address. Under System, click Devices/Interfaces.



Trace: Interface Groups » Port Names » DSCP » Dashboard » Devices/Interfaces

Devices/Interfaces ?

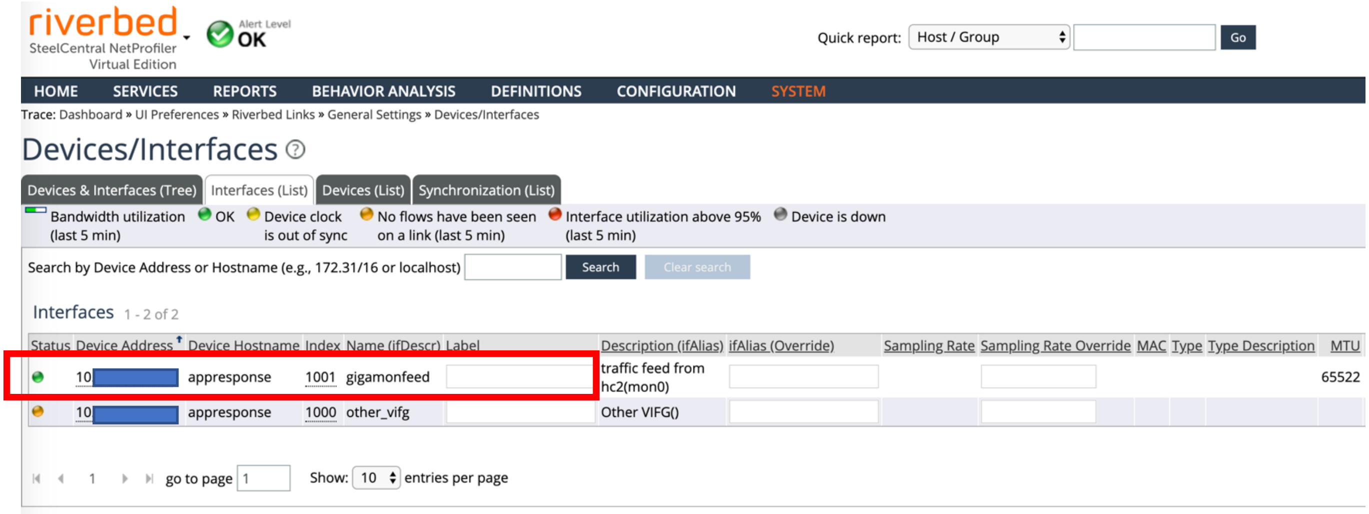
Devices & Interfaces (Tree) | Interfaces (List) | Devices (List) | Synchronization (List)

Bandwidth utilization (last 5 min) ● OK ● Device clock is out of sync ● No flows have been seen on a link (last 5 min) ● Interface utilization above 95% (last 5 min)

Options

- ● appresponse (Type: Riverbed SteelCentral AppResponse) Go
  - ● appresponse:gigamonfeed (Description: traffic feed from hc2(mon0)) Edit
  - ● appresponse:other_vifg (Description: Other VIFG()) Edit Delete

2. Click on Interfaces tab and verify if the required interface from the AppResponse tool is OK(Green).



Trace: Dashboard » UI Preferences » Riverbed Links » General Settings » Devices/Interfaces

Devices/Interfaces

Bandwidth utilization (last 5 min) ● OK ● Device clock is out of sync ● No flows have been seen on a link (last 5 min) ● Interface utilization above 95% (last 5 min) ● Device is down

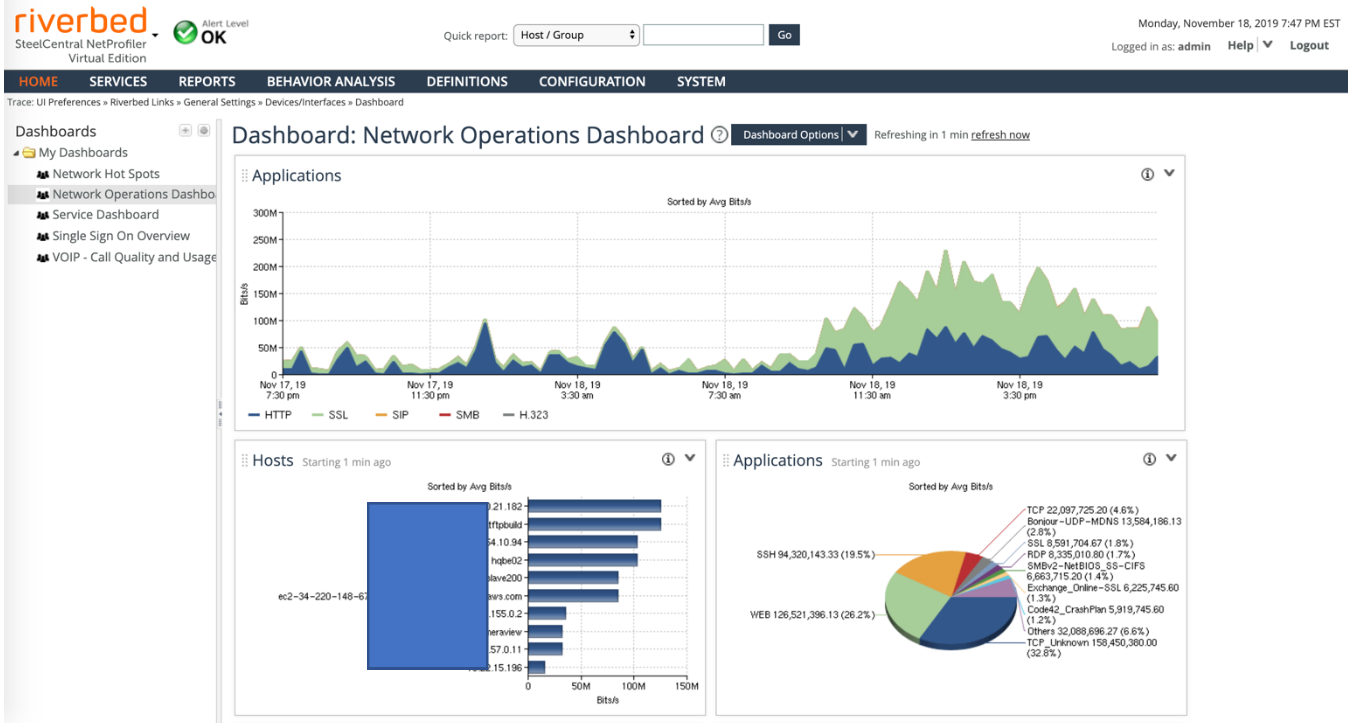
Search by Device Address or Hostname (e.g., 172.31/16 or localhost) Search Clear search

Interfaces 1 - 2 of 2

Status	Device Address	Device Hostname	Index	Name (ifDescr)	Label	Description (ifAlias)	ifAlias (Override)	Sampling Rate	Sampling Rate Override	MAC	Type	Type Description	MTU
●	10[redacted]	appresponse	1001	gigamonfeed		traffic feed from hc2(mon0)							65522
●	10[redacted]	appresponse	1000	other_vifg		Other VIFG()							

1 go to page 1 Show: 10 entries per page

3. Navigate through the different dashboards and reports for the required analysis.



[redacted]

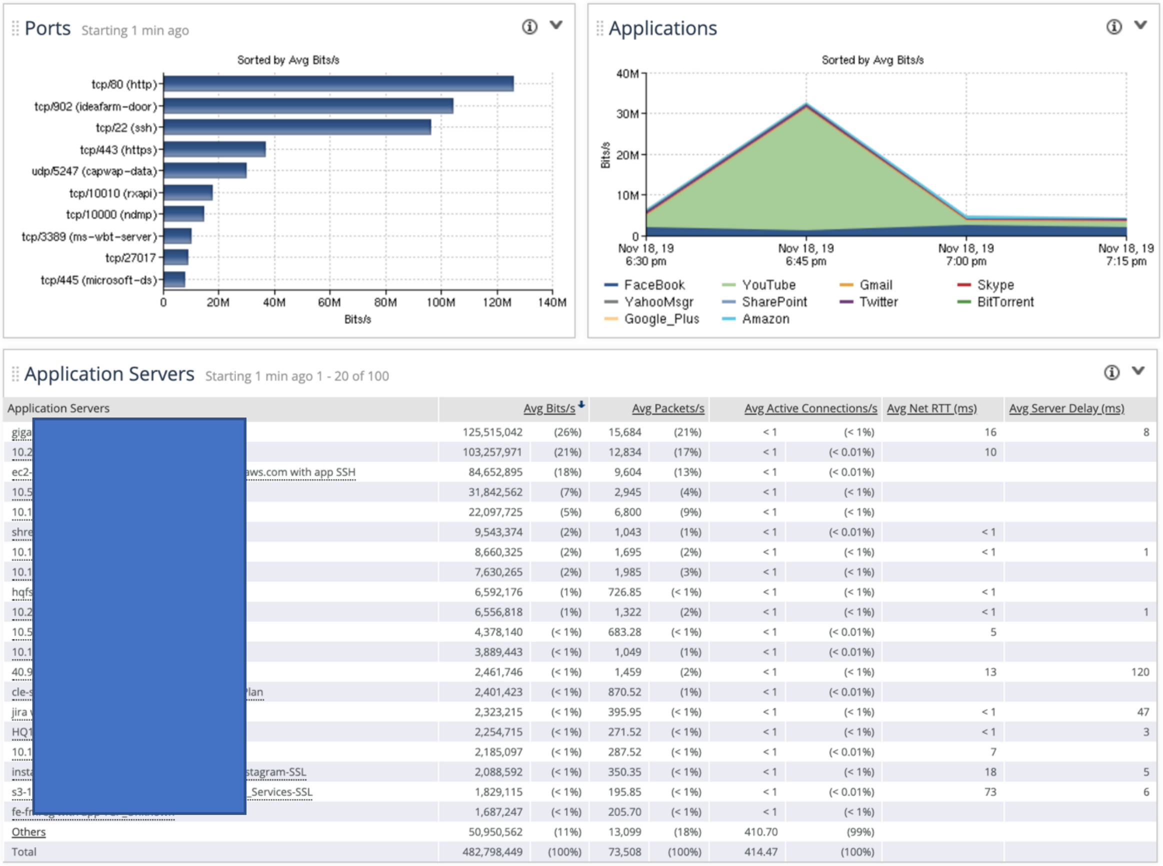
Monday, November 18, 2019 7:47 PM EST

Logged in as: admin Help Logout

Trace: UI Preferences » Riverbed Links » General Settings » Devices/Interfaces » Dashboard

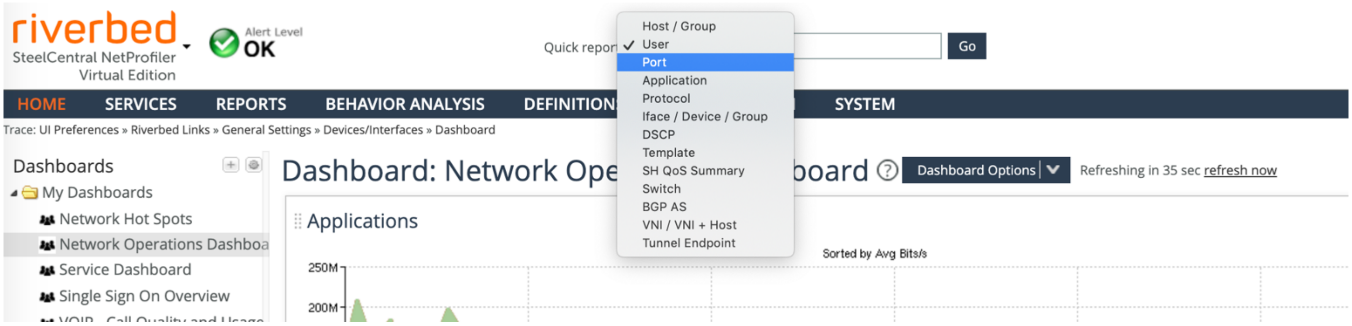
Dashboard: Network Operations Dashboard

Refreshing in 1 min refresh now



Application Servers Starting 1 min ago 1 - 20 of 100

Application Servers	Avg Bits/s		Avg Packets/s		Avg Active Connections/s		Avg Net RTT (ms)	Avg Server Delay (ms)
giga[redacted]	125,515,042	(26%)	15,684	(21%)	< 1	(< 1%)	16	8
10.2[redacted]	103,257,971	(21%)	12,834	(17%)	< 1	(< 0.01%)	10	
ec2-[redacted]aws.com with app SSH	84,652,895	(18%)	9,604	(13%)	< 1	(< 0.01%)		
10.5[redacted]	31,842,562	(7%)	2,945	(4%)	< 1	(< 1%)		
10.1[redacted]	22,097,725	(5%)	6,800	(9%)	< 1	(< 1%)		
shre[redacted]	9,543,374	(2%)	1,043	(1%)	< 1	(< 0.01%)	< 1	
10.1[redacted]	8,660,325	(2%)	1,695	(2%)	< 1	(< 1%)	< 1	1
10.1[redacted]	7,630,265	(2%)	1,985	(3%)	< 1	(< 1%)		
hqfs[redacted]	6,592,176	(1%)	726.85	(< 1%)	< 1	(< 1%)	< 1	
10.2[redacted]	6,556,818	(1%)	1,322	(2%)	< 1	(< 1%)	< 1	1
10.5[redacted]	4,378,140	(< 1%)	683.28	(< 1%)	< 1	(< 0.01%)	5	
10.1[redacted]	3,889,443	(< 1%)	1,049	(1%)	< 1	(< 0.01%)		
40.9[redacted]	2,461,746	(< 1%)	1,459	(2%)	< 1	(< 1%)	13	120
cle-[redacted]lan	2,401,423	(< 1%)	870.52	(1%)	< 1	(< 0.01%)		
jira [redacted]	2,323,215	(< 1%)	395.95	(< 1%)	< 1	(< 1%)	< 1	47
HQ1[redacted]	2,254,715	(< 1%)	271.52	(< 1%)	< 1	(< 1%)	< 1	3
10.1[redacted]	2,185,097	(< 1%)	287.52	(< 1%)	< 1	(< 0.01%)	7	
insta[redacted]stagram-SSL	2,088,592	(< 1%)	350.35	(< 1%)	< 1	(< 1%)	18	5
s3-1[redacted]_Services-SSL	1,829,115	(< 1%)	195.85	(< 1%)	< 1	(< 0.01%)	73	6
fe-f[redacted]	1,687,247	(< 1%)	205.70	(< 1%)	< 1	(< 1%)		
Others	50,950,562	(11%)	13,099	(18%)	410.70	(99%)		
Total	482,798,449	(100%)	73,508	(100%)	414.47	(100%)		



3 Summary

The deployment guide was a description of how to combine Gigamon's visibility platform and Riverbed's SteelCentral AppResponse for application and network performance management. The joint solution offers some of the following benefits:

- Minimize tool sprawl by tapping and aggregating all the traffic points with the Gigamon TAPs and sending all the traffic to a HC device to perform further filtering and advanced functions.
- Reduce the load on Riverbed's AppResponse and NetProfiler tools thereby saving considerable cost and overhead for the tool end user.

For more information on the GigaVUE-HC2 and other Gigamon Visibility Platforms, go to *www.Gigamon.com.*

How to get Help

For issues with Gigamon products, refer to https://www.Gigamon.com/support/support-and-services/contact-support.html and your Support Agreement with Gigamon. You can also email Technical Support at support@Gigamon.com.

For issues related to Riverbed products, refer to your Support Agreement with Riverbed and follow the directions on how to open a Support Case.