

# Cumulus NetQ UI User Guide



# Table of Contents

Cumulus NetQ UI User Guide	10
NetQ User Interface Overview	11
Access the NetQ UI	12
Application Layout	14
Main Menu	14
Recent Actions	15
Search	15
Cumulus Networks Logo	16
Quick Network Health View	16
Workbenches	16
Cards	17
User Settings	17
Format Cues	17
Create and Run Searches	19
Create a Search	19
Run a Recent Search	20
Focus Your Monitoring Using Workbenches	21
Default Workbenches	21
Custom Workbenches	22
Create a Workbench	22
Remove a Workbench	23
Open an Existing Workbench	24
Manage Auto-Refresh for Your Workbenches	24
Disable/Enable Auto-Refresh	24
View Current Settings	25
Change Settings	25
Manage Workbenches	26
Access Data with Cards	27
Card Sizes	27
Small Cards	27
Medium Cards	28
Large Cards	28

Full-Screen Cards	29
Card Size Summary	30
Card Workflows	31
Access a Card Workflow	32
Card Interactions	34
Add Cards to Your Workbench	34
Add Switch Cards to Your Workbench	37
Remove Cards from Your Workbench	38
Change the Time Period for the Card Data	39
Switch to a Different Card Size	40
View a Description of the Card Content	40
Reposition a Card on Your Workbench	41
Data Grid Settings	42
SORT DATA BY COLUMN	42
CHOOSE COLUMNS TO DISPLAY	42
CHANGE ORDER OF COLUMNS	43
TAKE ACTIONS ON ITEMS	43
Export Data	45
Card Decks	46
Set User Preferences	48
Configure Display Settings	48
Change Your Password	52
Manage Your Workbenches	53
NetQ Management	55
Application Management	56
NetQ Management Workbench	56
Manage User Accounts	57
Add New User Account	58
Edit a User Name	59
Change a User's Password	60
Change a User's Access Permissions	61
Correct a Mistyped User ID (Email Address)	62
Export a List of User Accounts	62
Delete a User Account	63
Manage Scheduled Traces	63
Add a Scheduled Trace	63

Delete a Scheduled Trace	64
Export a Scheduled Trace	65
Manage Scheduled Validations	65
View Scheduled Validation Configurations	66
Add a Scheduled Validation	66
Export Scheduled Validation Configurations	67
Lifecycle Management	68
Create a Network Snapshot	68
Compare Network Snapshots	70
Interpreting the Comparison Data	74
<b>VIEW CHANGE DETAILS</b>	74
Manage Network Snapshots	77
Monitor Network Performance	79
Monitor Network Health	80
Network Health Card Workflow Summary	80
View Network Health Summary	88
View Key Metrics of Network Health	89
View System Health	90
View Devices with the Most Issues	90
View Devices with Recent Issues	91
Filter Results by System Service	91
View Network Services Health	92
Filter Results by Network Service	94
View All Network Protocol and Service Validation Results	95
Validate Network Protocol and Service Operations	96
Create Validation Requests	96
Validation Request Card Workflow	96
Create On-demand and Scheduled Validation Requests	102
Run an Existing Scheduled Validation Request On Demand	102
Create a New On-demand Validation Request	103
Create a New Scheduled Validation Request	105
Modify an Existing Scheduled Validation Request	108
View On-demand Validation Results	109
On-Demand Validation Result Card Workflow	109
View Scheduled Validation Results	121
Scheduled Validation Result Card Workflow Summary	121

Granularity of Data Shown Based on Time Period	129
Monitor Network Inventory	134
Devices Inventory Card Workflow Summary	134
View the Number of Each Device Type in Your Network	140
View Which Operating Systems Are Running on Your Network Devices	140
View Switch Components	141
Highlight a Selected Component Type	142
Focus on a Selected Component Type	142
Navigate to the Switch Inventory Workflow	143
View All Switches	144
View All Hosts	144
Monitor Events	146
Monitor Alarms	146
Alarms Card Workflow Summary	146
View Alarm Status Summary	151
View the Distribution of Alarms	152
Monitor System and Interface Alarm Details	152
VIEW ALL SYSTEM AND INTERFACE ALARMS	153
VIEW DEVICES WITH THE MOST ALARMS	153
FILTER ALARMS BY SYSTEM OR INTERFACE	154
COMPARE ALARMS WITH A PRIOR TIME	155
View All Events	156
Monitor Info Events	157
Info Card Workflow Summary	157
View Info Status Summary	162
Compare Timing of Info and Alarm Events	164
View All Info Events Sorted by Time of Occurrence	164
View Devices with the Most Info Events	165
Events Reference	166
Monitor the BGP Service	184
Monitor the BGP Service (All Sessions)	184
BGP Service Card Workflow	184
View Service Status Summary	194
View the Distribution of Sessions and Alarms	195
View Devices with the Most BGP Sessions	195
View Devices with the Most Unestablished BGP Sessions	197

View Devices with the Most BGP-related Alarms	198
View All BGP Events	199
View Details for All Devices Running BGP	200
View Details for All BGP Sessions	201
Take Actions on Data Displayed in Results List	201
Monitor a Single BGP Session	202
BGP Session Card Workflow Summary	204
View Session Status Summary	212
View BGP Session State Changes	213
View Changes to the BGP Service Configuration File	215
View All BGP Session Details	216
Monitor the EVPN Service	218
Monitor the EVPN Service (All Sessions)	218
EVPN Service Card Workflow Summary	218
View the Distribution of Layer 3 VNIs	229
View Devices with the Most EVPN Sessions	230
View Devices with the Most Layer 2 EVPN Sessions	232
View Devices with the Most Layer 3 EVPN Sessions	233
View Devices with the Most EVPN-related Alarms	235
View All EVPN Events	236
View Details for All Devices Running EVPN	237
View Details for All EVPN Sessions	238
Monitor a Single EVPN Session	239
EVPN Session Card Workflow Summary	240
View VTEP Count	247
View All EVPN Session Details	248
Monitor the LLDP Service	250
Monitor the LLDP Service (All Sessions)	250
LLDP Service Card Workflow Summary	250
View the Distribution of Nodes, Alarms, and Sessions	262
View the Distribution of Missing Neighbors	262
View Devices with the Most LLDP Sessions	263
View Devices with the Most Unestablished LLDP Sessions	265
View Switches with the Most LLDP-related Alarms	266
View All LLDP Events	267
View Details About All Switches Running LLDP	268

View Detailed Information About All LLDP Sessions	269
Monitor a Single LLDP Session	270
LLDP Session Card Workflow Summary	272
View LLDP Session Neighbor State Changes	280
View Changes to the LLDP Service Configuration File	282
View All LLDP Session Details	283
Monitor the MLAG Service	285
Monitor the MLAG Service (All Sessions)	285
MLAG Service Card Workflow Summary	285
View Devices with the Most CLAG Sessions	296
View Devices with the Most Unestablished MLAG Sessions	298
View Switches with the Most MLAG-related Alarms	299
View All MLAG Events	300
View Details About All Switches Running MLAG	301
Monitor a Single MLAG Session	303
MLAG Session Card Workflow Summary	304
View MLAG Session Peering State Changes	314
View Changes to the MLAG Service Configuration File	316
All MLAG Session Details	317
View All MLAG Session Events	318
Monitor the OSPF Service	320
Monitor the OSPF Service (All Sessions)	320
OSPF Service Card Workflow	320
View the Distribution of Sessions	330
View Devices with the Most OSPF Sessions	331
View Devices with the Most Unestablished OSPF Sessions	333
View Devices with the Most OSPF-related Alarms	334
View All OSPF Events	336
View Details for All Devices Running OSPF	336
View Details for All OSPF Sessions	337
Monitor a Single OSPF Session	338
OSPF Session Card Workflow Summary	340
View OSPF Session State Changes	349
View Changes to the OSPF Service Configuration File	351
View All OSPF Session Details	352
Monitor Network Connectivity	354

Create a Trace Request	354
Trace Request Card Workflow Summary	354
Create a Layer 3 On-demand Trace Request	359
Create a Layer 3 Trace Through a Given VRF	360
Create a Layer 2 Trace	361
Create a Trace to Run on a Regular Basis (Scheduled Trace)	362
Run a Scheduled Trace on Demand	364
View On-demand Trace Results	366
On-demand Trace Results Card Workflow Summary	366
View Layer 2 Trace Results	372
View Layer 3 Trace Results	375
View Scheduled Trace Results	377
Scheduled Trace Results Card Workflow Summary	377
View Detailed Scheduled Trace Results	384
Monitor Devices	388
Monitor Switches	389
Monitor Switch Performance	389
Switch Card Workflow Summary	389
View the Overall Health of a Switch	399
View Health Performance Metrics	401
View Attributes of a Switch	402
View Current Resource Utilization for a Switch	402
View Interface Statistics for a Switch	403
View All Addresses for a Switch	404
View All Interfaces on a Switch	405
View All Software Packages on a Switch	406
View Disk Storage After BTRFS Allocation	407
View SSD Utilization	408
Monitor Switch Component Inventory	409
Switch Inventory Card Workflow Summary	409
View a Summary of Communication Status for All Switches	415
View the Number of Types of Any Component Deployed	415
View the Distribution of Any Component Deployed	416
View the Number of Switches with Invalid or Missing Licenses	418
View the Most Commonly Deployed ASIC	420
View the Number of Switches with a Particular NetQ Agent	422

View a List of All Data for a Specific Component	424
Monitor Network Elements	425
View All NetQ Agents	425
View All MACs	426
View All VLANs	426
View All IP Routes	427
View All IP Neighbors	427
View All IP Addresses	427
Monitor Using Topology View	429
Access the Topology View	429
Topology Overview	430
Interact with the Topology	431
Move the Topology Focus	431
View Data About the Network	432
Export Your NetQ Topology Data	436

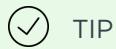
# Cumulus NetQ UI User Guide

This guide is intended for network administrators and operators who are responsible for monitoring and troubleshooting the network in their data center environment. NetQ 2.x offers the ability to easily monitor and manage your data center network infrastructure and operational health. This guide provides instructions and information about monitoring individual components of the network, the network as a whole, and the NetQ software itself using the NetQ graphical user interface (GUI). If you prefer to use a command line interface, refer to the [Cumulus NetQ CLI User Guide](#).

# NetQ User Interface Overview

The NetQ 2.3 graphical user interface (UI) enables you to access NetQ capabilities through a web browser as opposed to through a terminal window using the Command Line Interface (CLI). Visual representations of the health of the network, inventory, and system events make it easy to both find faults and misconfigurations, and to fix them.

The UI is accessible in both on-site and in-cloud deployments. It is supported on Google Chrome. Other popular browsers may be used, but have not been tested and may have some presentation issues.



TIP

Before you get started, you should refer to the [release notes](#) for this version.

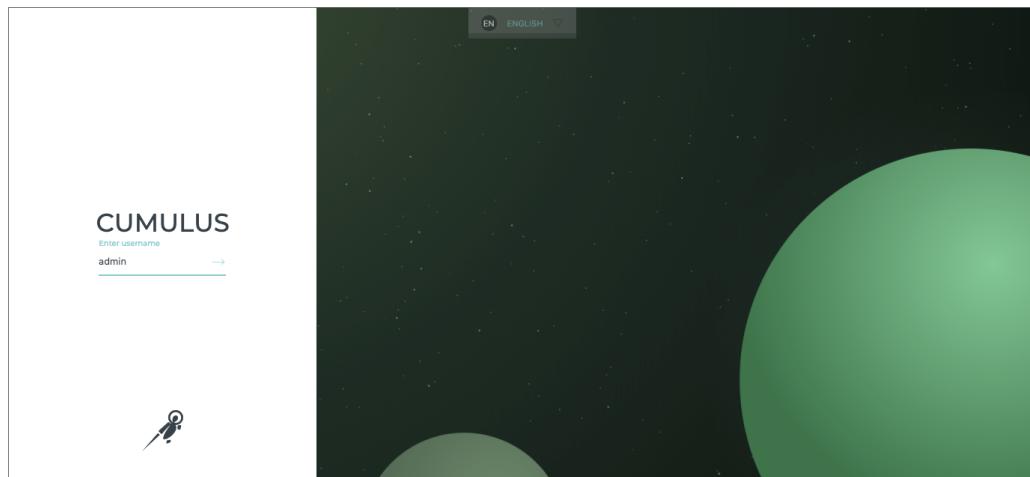
## Access the NetQ UI

# Access the NetQ UI

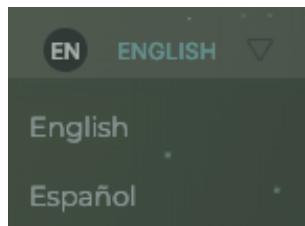
Logging in to the NetQ UI is as easy as opening any web page.

To log in to the UI:

1. Open a new Internet browser window or tab.
2. Enter the following URL into the Address bar for the on-site NetQ Platform/NetQ Appliance or the NetQ Cloud Appliance:
  - On-premises: *https://<netq-platform/appliance-ipaddress>:32666*
  - Cloud: <https://netq.cumulusnetworks.com>



3. Select your language of choice (English or Spanish) from the dropdown at the top of the window.



## Access the NetQ UI

4. Enter your username and then your password:

- NetQ Platform: *admin*, *admin* by default
- NetQ Appliance: *cumulus*, *CumulusLinux!* by default
- NetQ Cloud Appliance: Use credentials provided by Cumulus via email titled *Welcome to Cumulus NetQ!* and accept the terms of use.



On your first login, the default Cumulus Workbench opens, with your username shown in the upper right corner of the application. The NetQ Cloud UI has a **Premises** list in the application header, but is otherwise the same. On future logins, the last workbench that you were viewing is displayed.

To log out of the UI:

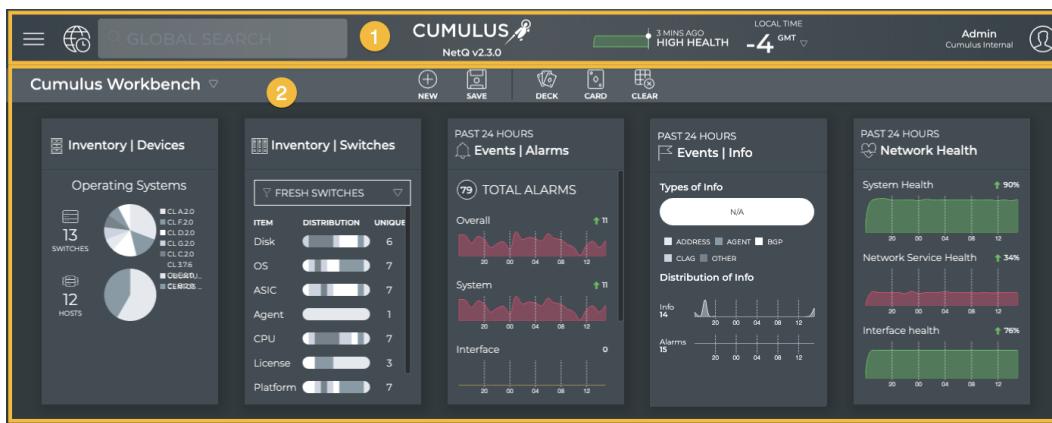
1. Click the user icon at the top right of the application.
2. Select **Log Out**.



# Application Layout

The NetQ UI contains two main areas:

- **Application Header** (1): Contains the main menu, recent actions history, search capabilities, NetQ version, quick health status chart, local time zone, premises list (cloud-only), and user account information.
- **Workbench** (2): Contains a task bar and content cards (with status and configuration information about your network and its various components).



## Main Menu

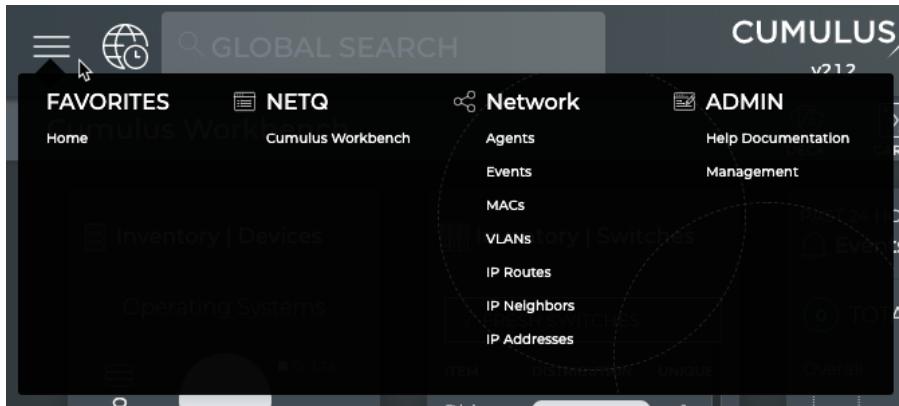
Found in the application header, click



to open the main menu which provides navigation to:

- **Favorites:** contains list of links to workbenches that you have designated as favorites; Home is listed by default and points to the Cumulus Workbench
- **NetQ:** contains list of links to all workbenches in the application
- **Network:** contains list of links to tabular data about various network elements; return to a workbench by selecting it from the NetQ menu

- **Admin:** contains link to user documentation and application management



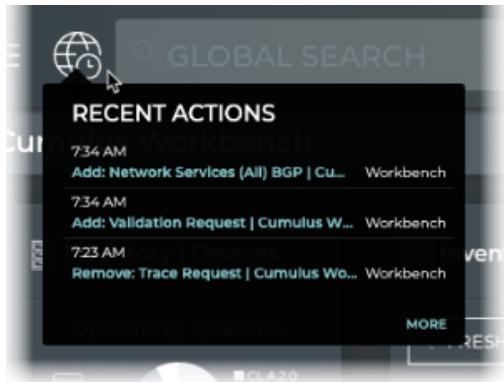
## Recent Actions

Found in the header, Recent Actions keeps track of every action you take on your workbench and then saves each action with a timestamp. This enables you to go back to a previous state or repeat an action.

To open Recent Actions, click



. Click on any of the actions to perform that action again.



## Search

The Global Search field in the UI header enables you to search for devices. It behaves like most searches and can help you quickly find device information. For more detail on creating and running searches, refer to [Create and Run Searches](#).

## Cumulus Networks Logo

Clicking on the Cumulus logo takes you to your favorite workbench. For details about specifying your favorite workbench, refer to [Set User Preferences](#).

## Quick Network Health View

Found in the header, the graph and performance rating provide a view into the health of your network at a glance.



NOTE

On initial start up of the application, it may take up to an hour to reach an accurate health indication as some processes run every 30 minutes.

## Workbenches

A workbench is comprised of a given set of cards. In this release, a pre-configured default workbench, Cumulus Workbench, is available to get you started. It contains Device Inventory, Switch Inventory, Alarm and Info Events, and Network Health cards. On initial login, this workbench is opened. You can create your own workbenches by adding or removing cards available cards to meet your particular needs. For more detail about managing your data using workbenches, refer to [Focus Your Monitoring Using Workbenches](#).

## Cards

Cards present information about your network for monitoring and troubleshooting.

This is where you can expect to spend most of your time. Each card describes a particular aspect of the network. Cards are available in multiple sizes, from small to full screen. The level of the content on a card varies in accordance with the size of the card, with the highest level of information on the smallest card to the most detailed information on the full-screen view. Cards are collected onto a workbench where you see all of the data relevant to a task or set of tasks. You can add and remove cards from a workbench, move between cards and card sizes, and make copies of cards to show different levels of data at the same time. For details about working with cards, refer to [Access Data with Cards](#).

## User Settings

Each user can customize the NetQ application display, change their account password, and manage their workbenches. This is all performed from User Settings



> Profile & Preferences. For details, refer to [Set User Preferences](#).

## Format Cues

Color is used to indicate links, options, and status within the UI.

Item	Color
Hover on item	Blue
Clickable item	Black
Selected item	Green
Highlighted item	Blue

## Application Layout

## Format Cues

Item	Color
Link	Blue
Good/Successful results	Green
Result with critical severity event	Pink
Result with high severity event	Red
Result with medium severity event	Orange
Result with low severity event	Yellow

# Create and Run Searches

The Global Search field in the UI header enables you to search for devices or cards. You can create new searches or run existing searches.

## Create a Search

As with most search fields, simply begin entering the criteria in the search field. As you type, items that match the search criteria are shown in the search history dropdown along with the last time the search was viewed. Wildcards are not allowed, but this predictive matching eliminates the need for them. By default, the most recent searches are shown. If more have been performed, they can be accessed. This may provide a quicker search by reducing entry specifics and suggesting recent searches. Selecting a suggested search from the list provides a preview of the search results to the right.

To create a new search:

1. Click in the **Global Search** field.
2. Enter your search criteria.
3. Click the device hostname or card workflow in the search list to open the associated information.



**(i) NOTE**

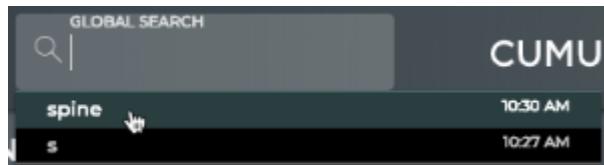
If you have more matches than fit in the window, click the **See All # Results** link to view all found matches. The count represents the number of devices found. It does not include cards found.

## Run a Recent Search

You can re-run a recent search, saving time if you are comparing data from two or more devices.

To re-run a recent search:

1. Click in the **Global Search** field.
2. When the desired search appears in the suggested searches list, select it.

**(i) NOTE**

You may need to click **See All # Results** to find the desired search. If you do not find it in the list, you may still be able to find it in the **Recent Actions** list.

# Focus Your Monitoring Using Workbenches

Workbenches are an integral structure of the Cumulus NetQ application. They are where you collect and view the data that is important to you.

There are two types of workbenches:

- **Default:** Provided by Cumulus Networks for use as they exist; changes made to these workbenches *cannot* be saved
- **Custom:** Created by application users when default workbenches need some adjustments to better meet your needs or a completely different collection of cards is wanted; changes made to these workbenches are saved automatically.

Both types of workbenches display a set of cards. Default workbenches are public (available for viewing by all users), whereas Custom workbenches are private (only viewable by user who created them).

## Default Workbenches

In this release, only one default workbench is available, the *Cumulus Workbench*, to get you started. It contains Device Inventory, Switch Inventory, Alarm and Info Events, and Network Health cards, giving you a high-level view of how your network is operating.



On initial login, the Cumulus Workbench is opened. On subsequent logins, the last workbench you had displayed is opened.

## Custom Workbenches

Users with either administrative or user roles can create and save as many custom workbenches as suits their needs. For example, a user might create a workbench that:

- shows all of the selected cards for the past week and one that shows all of the selected cards for the past 24 hours
- only has data about your virtual overlays; EVPN plus events cards
- has selected switches that you are troubleshooting
- focused on application or user account management
- etc.

### Create a Workbench

To create a workbench:

1. Click



in the workbench header.

ADD A NEW WORKBENCH

NAME \*

CREATE
Cancel

2. Enter a name for the workbench.
3. Click **Create** to open a blank new workbench, or **Cancel** to discard the workbench.
4. Add cards to the workbench using



or



.

Refer to [Access Data with Cards](#) for information about interacting with cards on your workbenches.

### Remove a Workbench

Once you have created a number of custom workbenches, you might find that you no longer need some of them. As an administrative user, you can remove any workbench, except for the default Cumulus Workbench. Users with a user role can only remove workbenches they have created.

To remove a workbench:

1. Click
- in the application header to open the **User Settings** options.



2. Click **Profile & Preferences**.
3. Locate the Workbenches card.
4. Hover over the workbench you want to remove, and click **Delete**.

## Open an Existing Workbench

There are several options for opening workbenches:

- Open through Workbench Header

- Click



next to the current workbench name and locate the workbench

- Under My Home, click the name of your favorite workbench
  - Under My Most Recent, click the workbench if in list
  - Search by workbench name
  - Click **All My WB** to open all workbenches and select it from the list

- Open through Main Menu

- Click



(Main Menu) and select the workbench from the **Favorites** or **NetQ** columns

- Open through Cumulus logo

- Click the logo in the header to open your favorite workbench

## Manage Auto-Refresh for Your Workbenches

With NetQ 2.3.1 and later, you can specify how often to update the data displayed on your workbenches. Three refresh rates are available:

- **Analyze**: updates every 30 seconds
- **Debug**: updates every minute
- **Monitor**: updates every two (2) minutes

By default, auto-refresh is enabled and configured to update every 30 seconds.

### Disable/Enable Auto-Refresh

To disable or pause auto-refresh of your workbenches, simply click the **Refresh** icon.

This toggles between the two states, *Running* and *Paused*, where

## Focus Your Monitoring Using Workbenches

## Manage Auto-Refresh for Your Workbenches



indicates it is currently disabled and

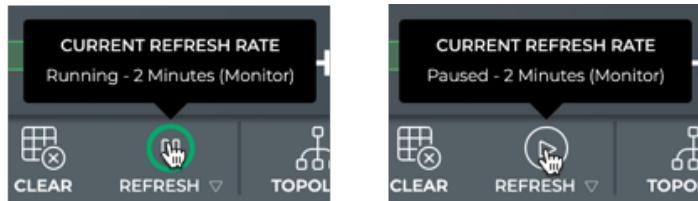


indicates it is currently enabled.

While having the workbenches update regularly is good most of the time, you may find that you want to pause the auto-refresh feature when you are troubleshooting and you do not want the data to change on a given set of cards temporarily. In this case, you can disable the auto-refresh and then enable it again when you are finished.

### View Current Settings

To view the current auto-refresh rate and operational status, hover over the **Refresh** icon on a workbench header, to open the tool tip as follows:



### Change Settings

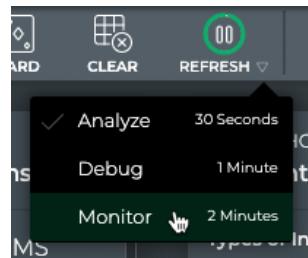
To modify the auto-refresh setting:

1. Click



on the **Refresh** icon.

2. Select the refresh rate you want. The refresh rate is applied immediately. A check mark is shown next to the current selection.



## Manage Workbenches

To manage your workbenches as a group, either:

- Click  next to the current workbench name, then click **Manage My WB**.
- Click , select **Profiles & Preferences** option.

Both of these open the Profiles & Preferences page. Look for the Workbenches card and refer to [Manage Your Workbenches](#) for more information.

# Access Data with Cards

Cards present information about your network for monitoring and troubleshooting. This is where you can expect to spend most of your time. Each card describes a particular aspect of the network. Cards are available in multiple sizes, from small to full screen. The level of the content on a card varies in accordance with the size of the card, with the highest level of information on the smallest card to the most detailed information on the full-screen card. Cards are collected onto a workbench where you see all of the data relevant to a task or set of tasks. You can add and remove cards from a workbench, move between cards and card sizes, change the time period of the data shown on a card, and make copies of cards to show different levels of data at the same time.

## Card Sizes

The various sizes of cards enables you to view your content at just the right level. For each aspect that you are monitoring there is typically a single card, that presents increasing amounts of data over its four sizes. For example, a snapshot of your total inventory may be sufficient, but to monitor the distribution of hardware vendors may requires a bit more space.

### Small Cards

Small cards are most effective at providing a quick view of the performance or statistical value of a given aspect of your network. They are commonly comprised of an icon to identify the aspect being monitored, summary performance or statistics in the form of a graph and/or counts, and often an indication of any related events. Other content items may be present. Some examples include a Devices Inventory card, a Switch Inventory

card, an Alarm Events card, an Info Events card, and a Network Health card, as shown here:



### Medium Cards

Medium cards are most effective at providing the key measurements for a given aspect of your network. They are commonly comprised of an icon to identify the aspect being monitored, one or more key measurements that make up the overall performance. Often additional information is also included, such as related events or components. Some examples include a Devices Inventory card, a Switch Inventory card, an Alarm Events card, an Info Events card, and a Network Health card, as shown here. Compare these with their related small- and large-sized cards.



### Large Cards

Large cards are most effective at providing the detailed information for monitoring specific components or functions of a given aspect of your network. These can aid in isolating and resolving existing issues or preventing potential issues. They are commonly comprised of detailed statistics and graphics. Some large cards also have tabs for additional detail about a given statistic or other related information. Some examples include a Devices Inventory card, an Alarm Events card, and a Network Health card, as shown here. Compare these with their related small- and medium-sized cards.

## Access Data with Cards

## Card Sizes



## Full-Screen Cards

Full-screen cards are most effective for viewing all available data about an aspect of your network all in one place. When you cannot find what you need in the small,

## Access Data with Cards

## Card Sizes

medium, or large cards, it is likely on the full-screen card. Most full-screen cards display data in a grid, or table; however, some contain visualizations. Some examples include All Events card and All Switches card, as shown here.

The screenshot shows the 'Events | Alarms' card with a title bar indicating '284 RESULTS'. A search bar at the top left says 'DEFAULT TIME Past 24 Hours'. Below the search bar is a button labeled 'Export'. The main area is titled 'All Events' and contains a table with columns: SOURCE, MESSAGE, TYPE, SEVERITY, and TIME. The table lists several entries from different servers (server02, server01, server03, server04, exit02, leaf04) with various log messages, types (ntp, services), severities (critical, warning), and times (e.g., 8/6/19 4:03 PM, 8/6/19 4:02 PM).

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
server02	Sync state changed from yes to no for server02	ntp	critical	8/6/19 4:03 PM
server01	Sync state changed from yes to no for server01	ntp	critical	8/6/19 4:03 PM
server03	Sync state changed from yes to no for server03	ntp	critical	8/6/19 4:03 PM
server04	Sync state changed from yes to no for server04	ntp	critical	8/6/19 4:03 PM
exit02	Service zebra status changed from active to inactive	services	critical	8/6/19 4:02 PM
exit02	Service bgpd status changed from active to inactive	services	critical	8/6/19 4:02 PM
leaf04	Service zebra status changed from active to inactive	services	critical	8/6/19 4:02 PM
leaf04	Service bgpd status changed from active to inactive	services	critical	8/6/19 4:02 PM

The screenshot shows the 'Inventory | Devices | Switches' card with a title bar indicating '8 RESULTS'. A search bar at the top left says 'DEFAULT TIME'. Below the search bar is a button labeled 'Export'. The main area is titled 'All Switches' and contains a table with columns: HOSTNAME, TIME, ASIC MOD..., AGENT VE..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., PLATFOR..., and MEMORY. The table lists four devices (exit01, exit02, leaf01, leaf02) with their respective details. The table has a header row with colspans for 'HOSTNAME' and 'TIME'.

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	MEMORY
exit01	9/27/19 4:17 ...	VX	2.3.0-c13u2l...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
exit02	9/27/19 4:18 ...	VX	2.3.0-c13u2l...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
leaf01	9/27/19 4:17 ...	VX	2.3.0-c13u2l...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
leaf02	9/27/19 4:18 ...	VX	2.3.0-c13u2l...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi

## Card Size Summary

Card Size	Small	Medium	Large	Full Screen

Primary Purpose	<ul style="list-style-type: none"> <li>Quick view of status, typically at the level of good or bad</li> <li>Enable quick actions, run a validation or trace for example</li> </ul>	<ul style="list-style-type: none"> <li>View key performance parameters or statistics</li> <li>Perform an action</li> <li>Look for potential issues</li> </ul>	<ul style="list-style-type: none"> <li>View detailed performance and statistics</li> <li>Perform actions</li> <li>Compare and review related information</li> </ul>	<ul style="list-style-type: none"> <li>View all attributes for given network aspect</li> <li>Free-form data analysis and visualization</li> <li>Export data to third-party tools</li> </ul>
-----------------	--	---	---	---

## Card Workflows

The UI provides a number of card workflows. Card workflows focus on a particular aspect of your network and are a linked set of each size card—a small card, a medium card, one or more large cards, and one or more full screen cards. The following card workflows are available:

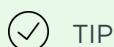
- **Network Health:** network-wide view of network health
- **Devices|Switches:** health of a given switch
- **Inventory|Devices:** information about all switches and hosts in the network
- **Inventory|Switches:** information about the components on a given switch
- **Events|Alarms:** information about all critical severity events in the system
- **Events|Info:** information about all warning, info, and debug events in the system
- **Network Services:** information about the network services and sessions
- **Validation Request (and Results):** network-wide validation of network protocols and services

- **Trace Request** (and Results): find available paths between two devices in the network fabric

### Access a Card Workflow

You can access a card workflow in multiple ways:

- For workbenches available from the main menu, open the workbench that contains the card flow
- Open a prior search
- Add it to a workbench
- Search for it



TIP

If you have multiple cards open on your workbench already, you might need to scroll down to see the card you have just added.

To open the card workflow through an existing workbench:

1. Click in the workbench task bar.
2. Select the relevant workbench.



The workbench opens, hiding your previous workbench.

To open the card workflow from Recent Actions:

1. Click



in the application header.

2. Look for an “Add: <card name>” item.
3. If it is still available, click the item.

The card appears on the current workbench, at the bottom.

To access the card workflow by adding the card:

1. Click



in the workbench task bar.

2. Follow the instructions in [Add Cards to Your Workbench](#) or [Add Switch Cards to Your Workbench](#).

The card appears on the current workbench, at the bottom.

To access the card workflow by searching for the card:

1. Click in the **Global Search** field.
2. Begin typing the name of the card.
3. Select it from the list.



The card appears on a current workbench, at the bottom.

## Card Interactions

Every card contains a standard set of interactions, including the ability to switch between card sizes, and change the time period of the presented data. Most cards also have additional actions that can be taken, in the form of links to other cards, scrolling, and so forth. The four sizes of cards for a particular aspect of the network are connected into a flow; however, you can have duplicate cards displayed at the different sizes. Cards with tabular data provide filtering, sorting, and export of data. The medium and large cards have descriptive text on the back of the cards.

To access the time period, card size, and additional actions, hover over the card. These options appear, covering the card header, enabling you to select the desired option.

### Add Cards to Your Workbench

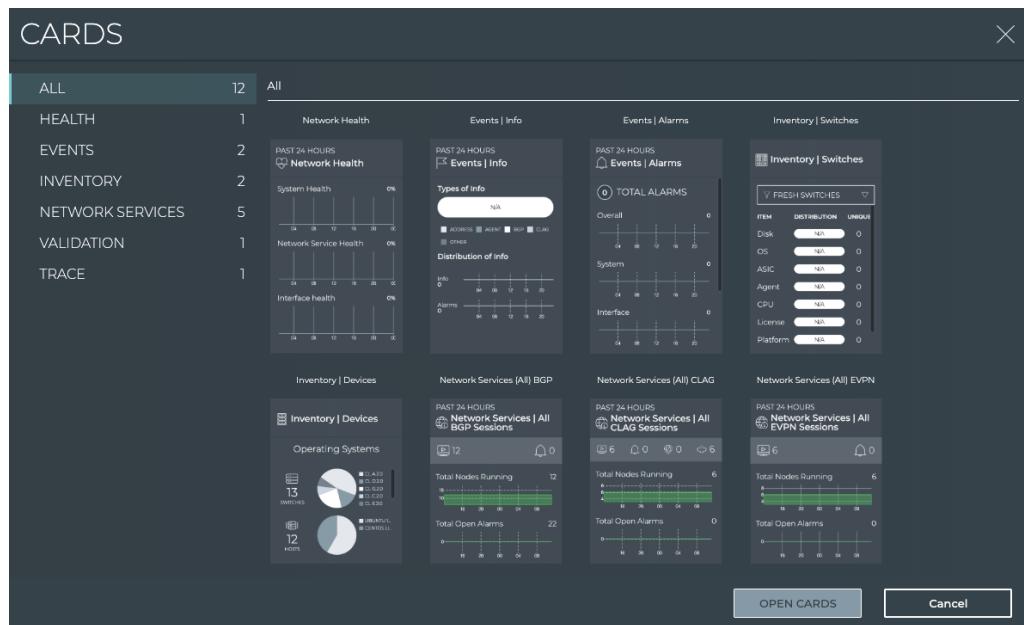
You can add one or more cards to a workbench at any time. To add Devices | Switches cards, refer to [Add Switch Cards to Your Workbench](#). For all other cards, follow the steps in this section.

To add one or more cards:

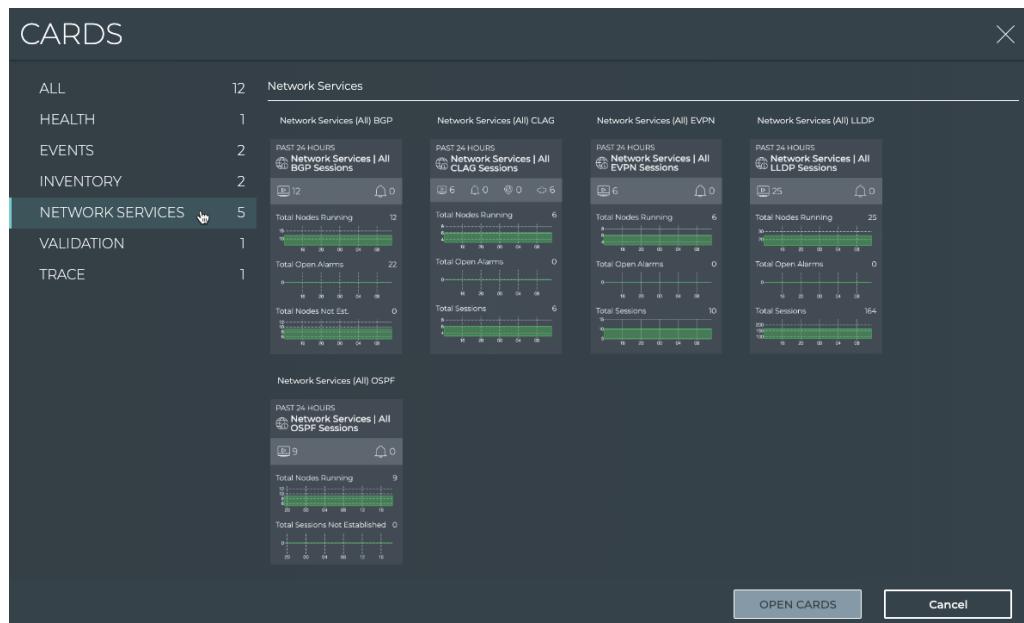
1. Click



to open the **Cards** modal.



2. Scroll down until you find the card you want to add, or select the category of cards to find the card you want to add.



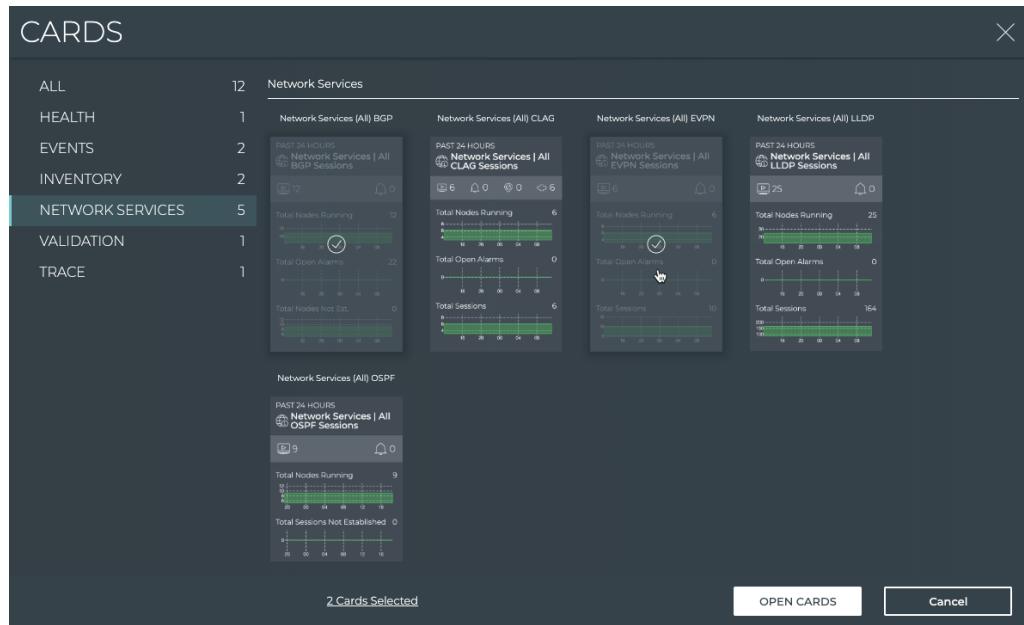
3. Click on each card you want to add.

As you select each card, it is grayed out and a



appears on top of it. If you have selected one or more cards using the category option, you can select another category without losing your current selection. Note

that the total number of cards selected for addition to your workbench is noted at the bottom.



Also note that if you change your mind and do not want to add a particular card you have selected, simply click on it again to remove it from the cards to be added. Note the total number of cards selected decreases with each card you remove.

4. When you have selected all of the cards you want to add to your workbench, you can confirm which cards have been selected by clicking the **Cards Selected** link. Modify your selection as needed.

The screenshot shows the 'CARDS' modal with a dark background. On the left, a sidebar lists categories: ALL (12), HEALTH (1), EVENTS (2), INVENTORY (2), NETWORK SERVICES (5), VALIDATION (1), and TRACE (1). To the right, three cards are displayed under the heading 'Selected Cards': 'Network Services (All) EVPN' (6 nodes running, 0 open alarms), 'Network Services (All) BGP' (12 nodes running, 22 open alarms), and 'Inventory | Devices' (13 services, 12 nodes, 0 not ed.). At the bottom left is a button labeled '3 Cards Selected'. At the bottom right are 'OPEN CARDS' and 'Cancel' buttons.

5. Click **Open Cards** to add the selected cards, or **Cancel** to return to your workbench without adding any cards.

The cards are placed at the end of the set of cards currently on the workbench. You might need to scroll down to see them. By default, the medium size of the card is added to your workbench for all except the Validation and Trace cards. These are added in the large size by default. You can rearrange the cards as described in [Reposition a Card on Your Workbench](#).

#### Add Switch Cards to Your Workbench

You can add switch cards to a workbench at any time. For all other cards, follow the steps in [Add Cards to Your Workbench](#).

To add a switch card:

1. Click  to open the Add Switch Card modal.

WHAT DEVICE

DEVICE NAME

Choose card size

MEDIUM

ADD Cancel

2. Begin entering the hostname of the switch you want to monitor.
3. Select the device from the suggestions that appear.

WHAT DEVICE

DEVICE NAME

lea

leaf01	switch
leaf02	switch
leaf03	switch
leaf04	switch

ADD Cancel



TIP

If you attempt to enter a hostname that is unknown to NetQ, a pink border appears around the entry field and you are unable to select **Add**. Try checking for spelling errors. If you feel your entry is valid, but not an available choice, consult with your network administrator.

4. Optionally select the small or large size to display instead of the medium size.
5. Click **Add** to add the switch card to your workbench, or **Cancel** to return to your workbench without adding the switch card.

### Remove Cards from Your Workbench

Removing cards is handled one card at a time.

To remove a card:

1. Hover over the card you want to remove.
2. Click  (More Actions menu).
3. Click **Remove**.



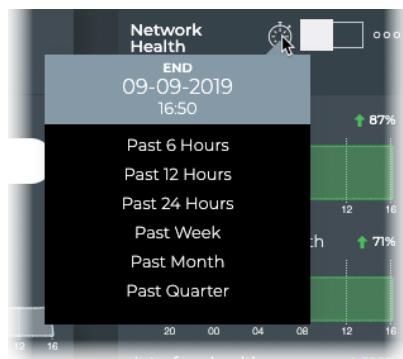
The card is removed from the workbench, but not from the application.

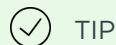
### Change the Time Period for the Card Data

All cards have a default time period for the data shown on the card, typically the last 24 hours. You can change the time period to view the data during a different time range to aid analysis of previous or existing issues.

To change the time period for a card:

1. Hover over any card.
2. Click  in the header.
3. Select a time period from the dropdown list.





Changing the time period in this manner only changes the time period for the given card.

### Switch to a Different Card Size

You can switch between the different card sizes at any time. Only one size is visible at a time. To view the same card in different sizes, open a second copy of the card.

To change the card size:

1. Hover over the card.
2. Hover over the Card Size Picker and move the cursor to the right or left until the desired size option is highlighted.



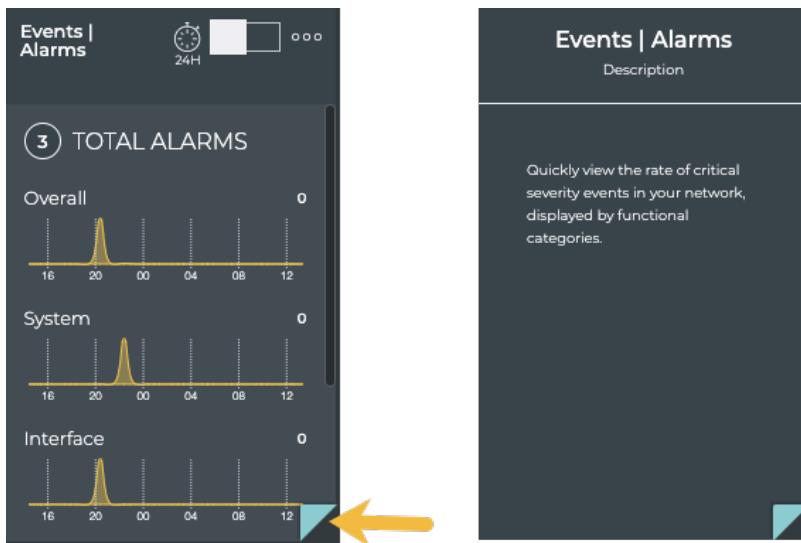
Single width opens a small card. Double width opens a medium card. Triple width opens large cards. Full width opens full-screen cards.

3. Click the Picker.

The card changes to the selected size, and may move its location on the workbench.

### View a Description of the Card Content

When you hover over a medium or large card, the bottom right corner turns up and is highlighted. Clicking the corner turns the card over where a description of the card and any relevant tabs are described. Hover and click again to turn it back to the front side.

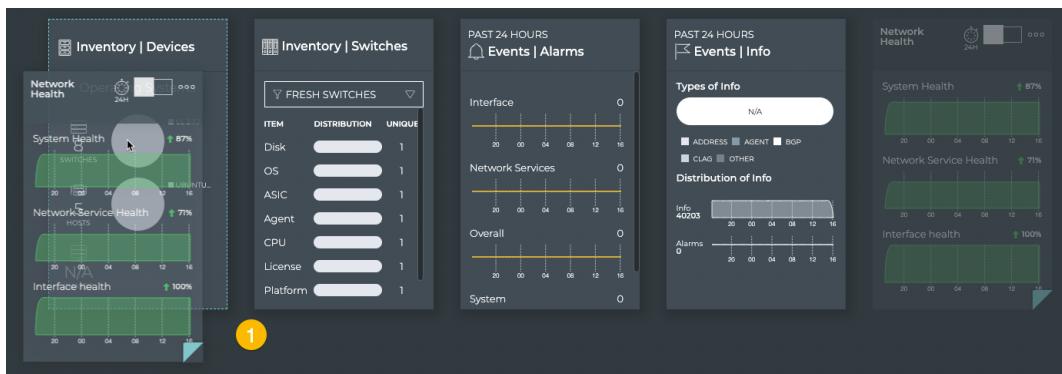


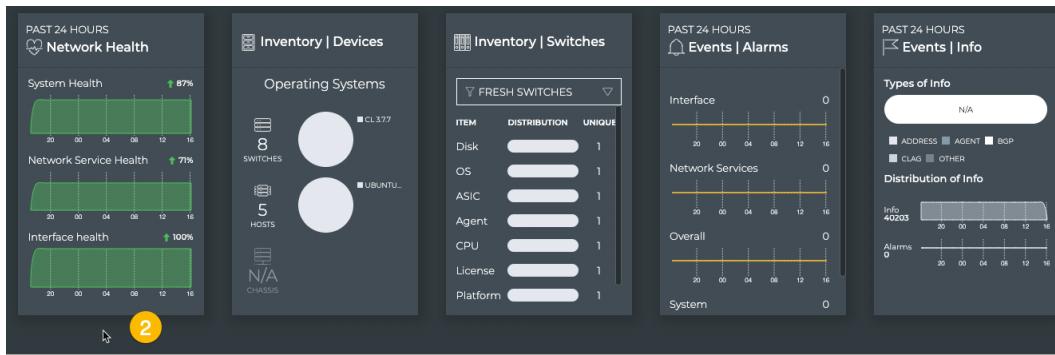
### Reposition a Card on Your Workbench

You can also move cards around on the workbench, using a simple drag and drop method.

To move a card:

1. Simply click and drag the card to left or right of another card, next to where you want to place the card.
2. Release your hold on the card when the other card becomes highlighted with a dotted line. In this example, we are moving the medium Network Health card to the left of the medium Devices Inventory card.





## Data Grid Settings

You can manipulate the data in a data grid in a full-screen card in several ways.

### SORT DATA BY COLUMN

Hover over a column header and click



.

### CHOOSE COLUMNS TO DISPLAY

1. Click



at the top right of the card.

2. Click **Change Columns** from the **Display Settings**.
3. Click the checkbox next to each column name to toggle on/off the columns you would like displayed. Columns listed under **Active** are displayed. Columns listed under **Inactive** are not displayed.



#### TIP

When you have a large number of possible columns for display, you can search for the column name using the **Quick Filter** to find and select or deselect the column more quickly.

4. Click



to close the selection box and view the updated data grid.

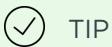
#### CHANGE ORDER OF COLUMNS

1. Click



and then click **Change Columns**.

2. Hover over a column name.

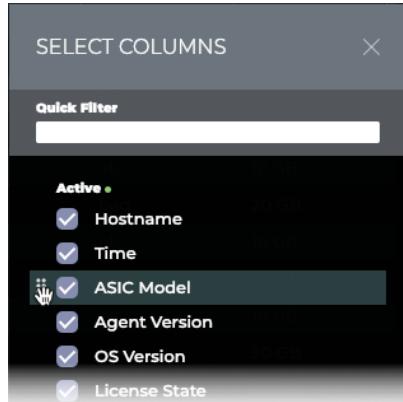


TIP

You use the **Quick Filter** to find the column when you have a large number of columns.

3. Point to the six dots to the left of the checkbox.

4. Click and drag the selected column up or down in the list.



5. Click



to close the selection box and view the updated data grid.

#### TAKE ACTIONS ON ITEMS

In the full screen cards, you can determine which results are displayed in the results list, and which are exported.

To take actions on the data, click in the blank column at the very left of a row. A checkbox appears, selecting that item, and an edit menu is shown at the bottom of the card (shown enlarged here).

HOSTNAME	TIME	ASIC MOD.	AGENT V.E..	OS VERSI..	LICENSE S..	DISK TOTA..	OS.VERSI..	PLATFOR..	M
exit01	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76
exit02	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76
<input checked="" type="checkbox"/> leaf01	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76
<input checked="" type="checkbox"/> leaf02	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76
leaf03	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76
leaf04	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76

2 ITEMS SELECTED    Select All    Clear All    Hide Selected    Show Only Selected    Export Selected

You can perform the following actions on the results list. **Note:** The actions vary based on the card displayed.

Option	Action or Behavior on Click
Select All	Selects all items in the results list
Clear All	Clears all existing selections of items in the results list. This also hides the edit menu.
Edit	Edit the selected items
Delete	Remove the selected items
Generate/Delete AuthKeys	Create or remove NetQ Cloud authorization keys
Open Cards	Open the corresponding validation or trace result card
Hide Selected	Hide selected items (switches, sessions, alarms, and so forth) from the results list
Show Only Selected	Hide unselected items (switches, sessions, alarms, and so forth) from the results list

Option	Action or Behavior on Click
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the <b>Export</b> button.

To return to original display of results, click the associated tab.

## Export Data

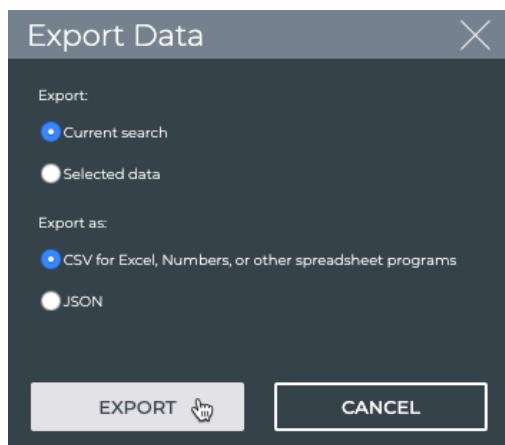
You can export tabular data from a full screen card to a CSV- or JSON-formatted file.

To export the data:

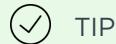
1. If you want to export only a subset of the data listed, select those items first.
2. Click **EXPORT**.

HOSTNAME	TIME
exit01	8/28/19 2:20 ...
exit02	8/28/19 2:20

3. Select all data or selected data for export in the dialog box:



4. Select the export format.
5. Click **EXPORT** to save the file to your downloads directory.



You can quickly export all data to a .csv file in one of two ways:

- Click **Export** at top of list, and click **Export** in the dialog, or
- Select one item, click **Select All**, click **Export Selected**.

## Card Decks



This option only applies to NetQ 2.1.0 through 2.2.1. It has been removed from NetQ 2.2.2 and later.

A card deck is a collection of related cards that can be added and removed from a workbench all at once. They are distinct from card workflows, which focus on a particular aspect of your network. A card deck pulls multiple cards with related information to aid the user in performing a broader task. It also simplifies the creation of new workbenches when a card deck is available. The following card decks are provided by default:

- **Inventory:** includes the medium Inventory | Switches and Inventory | Devices cards
- **Events:** includes the medium Events | Alarms and Events | Info cards

To add a card deck:

1. Click



in the workbench task bar.

2. Select the deck you want to add to your workbench.

# Set User Preferences

Each user can customize the NetQ application display, change his account password, and manage his workbenches.

## Configure Display Settings

The Display card contains the options for setting the application theme, language, time zone, and date formats. There are two themes available: a Light theme and a Dark theme (default). The screen captures in this document are all displayed with the Dark theme. English is the only language available for this release. You can choose to view data in the time zone where you or your data center resides. You can also select the date and time format, choosing words or number format and a 12- or 24-hour clock. All changes take effect immediately.

To configure the display settings:

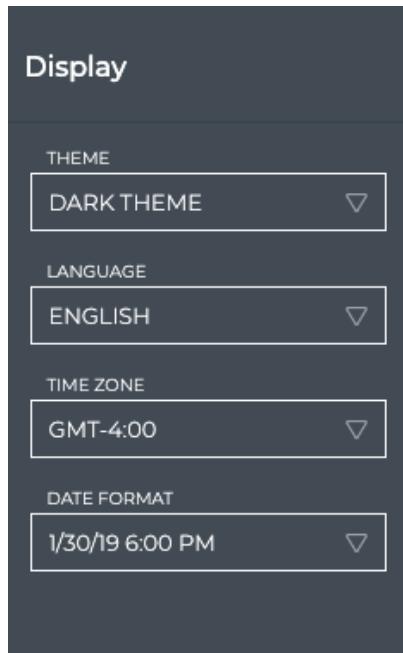
1. Click  in the application header to open the **User Settings** options.



2. Click **Profile & Preferences**.
3. Locate the Display card.

## Set User Preferences

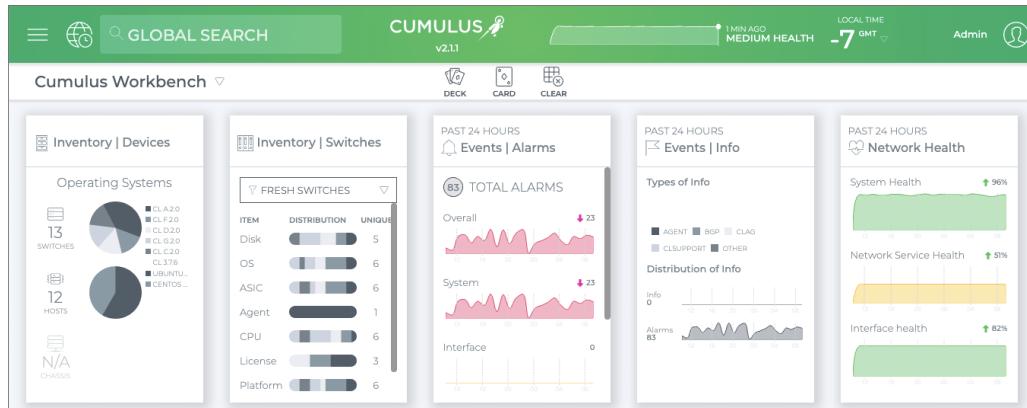
## Configure Display Settings



4. In the **Theme** field, click



to select your choice of theme. This figure shows the light theme. Switch back and forth as desired.



5. In the **Time Zone** field, click



to change the time zone from the default.

By default, the time zone is set to the user's local time zone. If a time zone has not been selected, NetQ defaults to the current local time zone where NetQ is installed. All time values are based on this setting. This is displayed in the application header, and is based on Greenwich Mean Time (GMT).

**Tip:** You can also change the time zone from the header display.

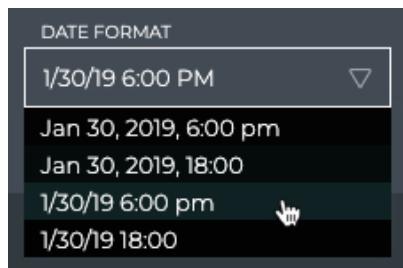


If your deployment is not local to you (for example, you want to view the data from the perspective of a data center in another time zone) you can change the display to another time zone. The following table presents a sample of time zones:

Time Zone	Description	Abbreviation
GMT +12	New Zealand Standard Time	NST
GMT +11	Solomon Standard Time	SST
GMT +10	Australian Eastern Time	AET
GMT +9:30	Australia Central Time	ACT
GMT +9	Japan Standard Time	JST
GMT +8	China Taiwan Time	CTT
GMT +7	Vietnam Standard Time	VST
GMT +6	Bangladesh Standard Time	BST
GMT +5:30	India Standard Time	IST
GMT+5	Pakistan Lahore Time	PLT
GMT +4	Near East Time	NET
GMT +3:30	Middle East Time	MET
GMT +3	Eastern African Time/Arab Standard Time	EAT/AST
GMT +2	Eastern European Time	EET
GMT +1	European Central Time	ECT

Time Zone	Description	Abbreviation
GMT	Greenwich Mean Time	GMT
GMT -1	Central African Time	CAT
GMT -2	Uruguay Summer Time	UYST
GMT -3	Argentina Standard/Brazil Eastern Time	AGT/BET
GMT -4	Atlantic Standard Time/Puerto Rico Time	AST/PRT
GMT -5	Eastern Standard Time	EST
GMT -6	Central Standard Time	CST
GMT -7	Mountain Standard Time	MST
GMT -8	Pacific Standard Time	PST
GMT -9	Alaskan Standard Time	AST
GMT -10	Hawaiian Standard Time	HST
GMT -11	Samoa Standard Time	SST
GMT -12	New Zealand Standard Time	NST

6. In the **Date Format** field, select the data and time format you want displayed on the cards.



The four options include the date displayed in words or abbreviated with numbers, and either a 12- or 24-hour time representation. The default is the third option.

7. Return to your workbench by clicking



and selecting a workbench from the NetQ list.

## Change Your Password

You can change your account password at any time should you suspect someone has hacked your account or your administrator requests you to do so.

To change your password:

1. Click

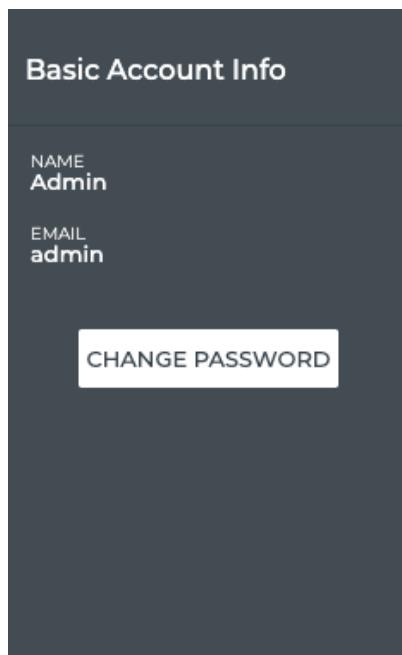


in the application header to open the **User Settings** options.



2. Click **Profile & Preferences**.

3. Locate the Basic Account Info card.



4. Click **Change Password**.

5. Enter your current password.
6. Enter and confirm a new password.

A screenshot of a 'CHANGE PASSWORD' dialog box. The box has a dark background with white text and borders. It contains three input fields: 'CURRENT PASSWORD' with '\*\*\*\*\*', 'NEW PASSWORD' with '\*\*\*\*\*', and 'CONFIRM NEW PASSWORD' with '\*\*\*\*\*'. At the bottom are two buttons: 'SAVE' on the left and 'CANCEL' on the right.

7. Click **Save** to change to the new password, or click **Cancel** to discard your changes.
8. Return to your workbench by clicking  
≡  
and selecting a workbench from the NetQ list.

## Manage Your Workbenches

You can view all of your workbenches in a list form, making it possible to manage various aspects of them. There are public and private workbenches. Public workbenches are visible by all users. Private workbenches are visible only by the user who created the workbench. From the Workbenches card, you can:

- **Specify a favorite workbench:** This tells NetQ to open with that workbench when you log in instead of the default Cumulus Workbench.
- **Search for a workbench:** If you have a large number of workbenches, you can search for a particular workbench by name, or sort workbenches by their access type or cards that reside on them.
- **Delete a workbench:** Perhaps there is one that you no longer use. You can remove workbenches that you have created (private workbenches). An administrative role is required to remove workbenches that are common to all users (public workbenches).

To manage your workbenches:

1. Click



in the application header to open the **User Settings** options.



2. Click **Profile & Preferences**.
3. Locate the Workbenches card.

Workbenches		
WORKBENCH NAME	ACCESS	CARDS
Cumulus Workbench	Public	Inventory   Devices, Inventory   Switches, ...

4. To specify a favorite workbench, click to the left of the desired workbench name.



is placed there to indicate its status as your favorite workbench.

5. To search the workbench list by name, access type, and cards present on the workbench, click the relevant header and begin typing your search criteria.
6. To sort the workbench list, click the relevant header and click



.

7. To delete a workbench, hover over the workbench name to view the **Delete** button.  
As an administrator, you can delete both private and public workbenches.
8. Return to your workbench by clicking



and selecting a workbench from the NetQ list.

# NetQ Management

As an administrator, you have two major tasks related to managing Cumulus NetQ:

- **Application Management:** manage access to and various application-wide settings for the Cumulus NetQ UI from a single location
- **Lifecycle Management:** manage the software deployment onto your network devices

The NetQ UI makes both of these tasks easier than ever.

# Application Management

As an administrator, you can manage access to and various application-wide settings for the Cumulus NetQ UI from a single location.

Individual users have the ability to set preferences specific to their workspaces. This information is covered separately. Refer to [Set User Preferences](#).

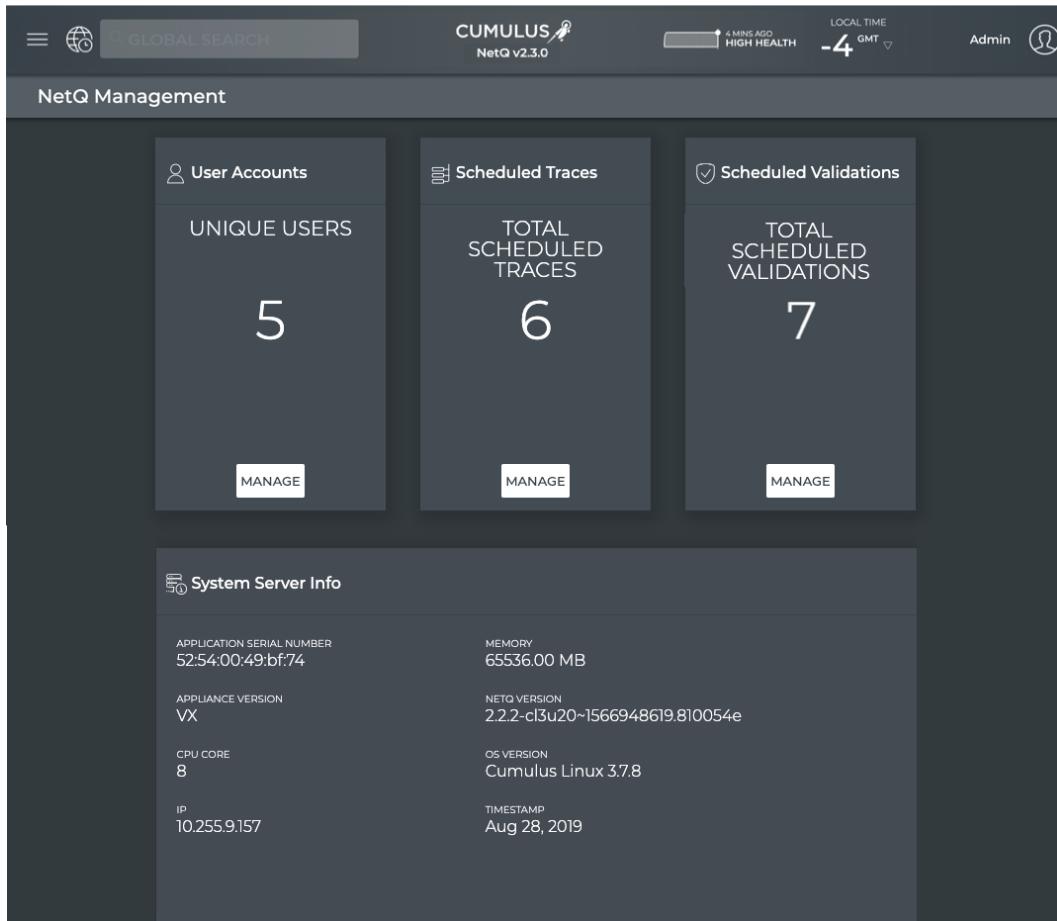
## NetQ Management Workbench

The NetQ Management workbench is accessed from the main menu. For the user(s) responsible for maintaining the application, this is a good place to start each day.

To open the workbench, click



, and select **Management** under the **Admin** column.



#### NOTE

For on-premises deployments, an additional LDAP Server Info card is available. Refer to [Integrate NetQ with Your LDAP server](#) for details.

## Manage User Accounts

From the NetQ Management workbench, you can view the number of users with accounts in the system. As an administrator, you can also add, modify, and delete user accounts using the User Accounts card.

## Add New User Account

For each user that monitors at least one aspect of your data center network, a user account is needed. Adding a local user is described here. Refer to [Integrate NetQ with Your LDAP server](#) for instructions for adding LDAP users.

To add a new user account:

1. Click **Manage** on the User Accounts card, to open the **User Accounts** tab.
2. Click **Add User**.

The screenshot shows a dark-themed 'ADD NEW USER' dialog box. It includes fields for 'EMAIL ADDRESS', 'FIRST NAME' (highlighted in red), 'LAST NAME', 'RE-ENTER ADMIN PASSWORD', 'USER TYPE: ADMIN' (selected), 'CREATE PASSWORD', 'USER PASSWORD', and 'CONFIRM USER PASSWORD'. At the bottom are 'SAVE' and 'Cancel' buttons.

3. Enter the user's email address, along with their first and last name.

**NOTE**

Be especially careful entering the email address as you *cannot* change it once you save the account. If you save a mistyped email address, you must delete the account and create a new one.

4. Select the user type: *Admin* or *User*.
5. Enter your password in the **Admin Password** field (only users with administrative permissions can add users).

6. Create a password for the user.
  - a. Enter a password for the user.
  - b. Re-enter the user password. If you do not enter a matching password, it will be underlined in red.
7. Click **Save** to create the user account, or **Cancel** to discard the user account.

USER ID	FIRST NAME	LAST NAME	ROLE	LAST LOGIN	DATE CREATED	ACCESS KEY
admin	Admin	Admin	admin	09/09/2019	08/28/2019	
user1@com...	user1	Admin	admin	never	09/10/2019	
user2@com...	user2	User	user	never	09/10/2019	

By default the User Accounts table is sorted by *Role*. Change the sort by clicking in any of the headers, then click



8. Repeat these steps to add all of your users.

#### Edit a User Name

If a user's first or last name was incorrectly entered, you can fix them easily.

To change a user name:

1. Click **Manage** on the User Accounts card to open the **User Accounts** tab.
2. Hover over the account you want to change, and click the checkbox next to it.
3. In the Edit menu that appears at the bottom of the window, click
4. Modify the first and/or last name as needed.
5. Enter your admin password.

EDIT USER

EMAIL ADDRESS admin.user@company.com	
FIRST NAME Admin	LAST NAME User
RE-ENTER ADMIN PASSWORD	
USER TYPE: ADMIN ▾	
RESET PASSWORD	
SAVE	Cancel

6. Click **Save** to commit the changes or **Cancel** to discard them.

#### Change a User's Password

Should a user forget his password or for security reasons, you can change a password for a particular user account.

To change a password:

1. Click **Manage** on the User Accounts card to open the **User Accounts** tab.
2. Hover over the account you want to change, and click the checkbox next to it.
3. In the Edit menu that appears at the bottom of the window, click .  
.
4. Click **Reset Password**.
5. Enter your admin password.

EDIT USER

EMAIL ADDRESS admin.user@company.com	
FIRST NAME Admin	LAST NAME User
RE-ENTER ADMIN PASSWORD	
USER TYPE: ADMIN ▾	
CREATE PASSWORD	
USER PASSWORD	
CONFIRM USER PASSWORD	
SAVE	Cancel

6. Enter a new password for the user.
7. Re-enter the user password. *Tip: If the password you enter does not match, Save is gray (not activated).*
8. Click **Save** to commit the change, or **Cancel** to discard the change.

#### Change a User's Access Permissions

If a particular user has only standard user permissions and they need administrator permissions to perform their job (or the opposite, they have administrator permissions, but only need user permissions), you can modify their access rights.

To change access permissions:

1. Click **Manage** on the User Accounts card.
2. Click the **User Accounts** tab.
3. Hover over the account you want to change, and click the checkbox next to it.
4. In the Edit menu that appears at the bottom of the window, click 
5. Select the appropriate user type from the dropdown list.

The screenshot shows the 'Edit User' dialog box. It contains fields for 'EMAIL ADDRESS' (user1.user@company.com), 'FIRST NAME' (User1), 'LAST NAME' (User), and 'RE-ENTER ADMIN PASSWORD'. A dropdown menu for 'USER TYPE' is open, showing 'User Type: Admin' and 'User Type: User', with 'User Type: User' being the selected option. At the bottom are 'SAVE' and 'Cancel' buttons.

6. Enter your admin password.
7. Click **Save** to commit the change, or **Cancel** to discard the change.

#### Correct a Mistyped User ID (Email Address)

You cannot edit a user's email address, because this is the identifier the system uses for authentication. If you need to change an email address, you must create a new one for this user. Refer to [Add a New User Account](#). You should delete the incorrect user account. Select the user account, and click **Delete** in the Edit menu.

#### Export a List of User Accounts

You can export user account information at any time using the User Accounts tab.

To export information for one or more user accounts:

1. Click **Manage** on the User Accounts card to open the **User Accounts** tab.
2. Select one or more accounts that you want to export by clicking the checkbox next to them.
3. To export all user accounts, click **Select All** in the Edit menu and then click **Export Selected**.



4. To export specific user accounts, select only those accounts you want to export, and click **Export Selected** in the Edit menu.

### Delete a User Account

NetQ application administrators should remove user accounts associated with users that are no longer using the application.

To delete one or more user accounts:

1. Click **Manage** on the User Accounts card to open the **User Accounts** tab.
2. Select one or more accounts that you want to remove by clicking the checkbox next to them.
3. Click  
 in the Edit menu to remove the accounts.

## Manage Scheduled Traces

From the NetQ Management workbench, you can view the number of traces scheduled to run in the system. A set of default traces are provided with the NetQ GUI. As an administrator, you can run one or more scheduled traces, add new scheduled traces, and edit or delete existing traces.

### Add a Scheduled Trace

You can create a scheduled trace to provide regular status about a particularly important connection between a pair of devices in your network or for temporary troubleshooting.

To add a trace:

1. Click **Manage** on the Scheduled Traces card to open the **Scheduled Traces** tab.
2. Click **Add Trace** to open the large New Trace Request card.

The screenshot shows the 'New Trace Request' form. At the top, there's a dropdown menu labeled 'NEW TRACE REQUEST'. Below it are two input fields: 'SOURCE' (set to 'IP / HOST') and 'VRF'. To the right of 'VRF' is another input field for 'VLAN ID'. Underneath these are two more input fields: 'DESTINATION' (set to 'IP / MAC') and 'VLAN ID'. A 'SCHEDULE:' section follows, with 'Run every' set to 'HOUR' and 'Starting' set to 'DATE / TIME: 9/10/19 15:42'. To the right of the schedule are two status indicators: 'Scheduled Traces Remaining' (13) and '(Limit: 15)'. At the bottom are three buttons: 'RUN NOW', 'UPDATE', and 'SAVE AS NEW'.

3. Enter source and destination addresses.

NOTE

For layer 2 traces, the source must be a hostname and the destination must be a MAC address. For layer 3 traces, the source can be a hostname or IP address, and the destination must be an IP address.

4. Specify a VLAN for a layer 2 trace or (optionally) a VRF for a layer 3 trace.
5. Set the schedule for the trace, by selecting how often to run the trace and when to start it the first time.
6. Click **Save As New** to add the trace. You are prompted to enter a name for the trace in the **Name** field.

If you want to run the new trace right away for a baseline, select the trace you just added from the dropdown list, and click **Run Now**.

#### Delete a Scheduled Trace

If you do not want to run a given scheduled trace any longer, you can remove it.

To delete a scheduled trace:

1. Click **Manage** on the Scheduled Trace card to open the **Scheduled Traces** tab.
2. Hover over and select at least one trace.
3. Click



Export a Scheduled Trace

You can export a scheduled trace configuration at any time using the Scheduled Traces tab.

To export one or more scheduled trace configurations:

1. Click **Manage** on the Scheduled Trace card to open the **Scheduled Traces** tab.
2. Hover over and select at least one trace.
3. To export all traces, click **Select All** and then **Export Selected**.



4. To export specific traces, select only those traces you want to export, and click **Export Selected**.

## Manage Scheduled Validations

From the NetQ Management workbench, you can view the total number of validations scheduled to run in the system. A set of default scheduled validations are provided and pre-configured with the NetQ UI. These are not included in the total count. As an administrator, you can view and export the configurations for all scheduled validations, or add a new validation.

## View Scheduled Validation Configurations

You can view the configuration of a scheduled validation at any time. This can be useful when you are trying to determine if the validation request needs to be modified to produce a slightly different set of results (editing or cloning) or if it would be best to create a new one.

To view the configurations:

1. Click **Manage** on the Scheduled Validations card to open the **Scheduled Validations** tab.

2. Click



in the top right to return to your NetQ Management cards.

## Add a Scheduled Validation

You can add a scheduled validation at any time using the Scheduled Validations tab.

To add a scheduled validation:

1. Click **Manage** on the Scheduled Validations card.
2. Click the **Scheduled Validations** tab.
3. Click **Add Validation** to open the large Validation Request card.

The screenshot shows the 'Validation Request' card interface. At the top left is the title 'Validation Request'. Below it is a dropdown menu set to 'VALIDATION'. To the right is a section titled 'Network protocols and services' containing buttons for AGENTS, BGP, CLAG, EVPN, INTERFACES, LICENSE, NTP, OSPF, VXLAN, VLAN, MTU, and SENSORS. Underneath this is a 'SCHEDULE:' section. It includes a 'Run every' dropdown set to 'HOUR' and a 'Starting' dropdown set to 'DATE/TIME 9/10/19 15:47'. To the right of these dropdowns is the text 'Scheduled Validations Remaining 13 (Limit : 15)'. At the bottom of the card are three buttons: 'RUN NOW', 'UPDATE', and 'SAVE AS NEW'.

4. Configure the request. Refer to [Validate Network Protocol and Service Operations](#) for details.

#### Export Scheduled Validation Configurations

You can export one or more scheduled validation configurations at any time using the Scheduled Validations tab.

To export a scheduled validation:

1. Click **Manage** on the Scheduled Validations card.
2. Click the **Scheduled Validations** tab.
3. Hover over and select at least one validation.
4. To export all validations, click **Select All** and then **Export Selected**.



5. To export specific validations, select only those validations you want to export, and click **Export Selected**.

# Lifecycle Management

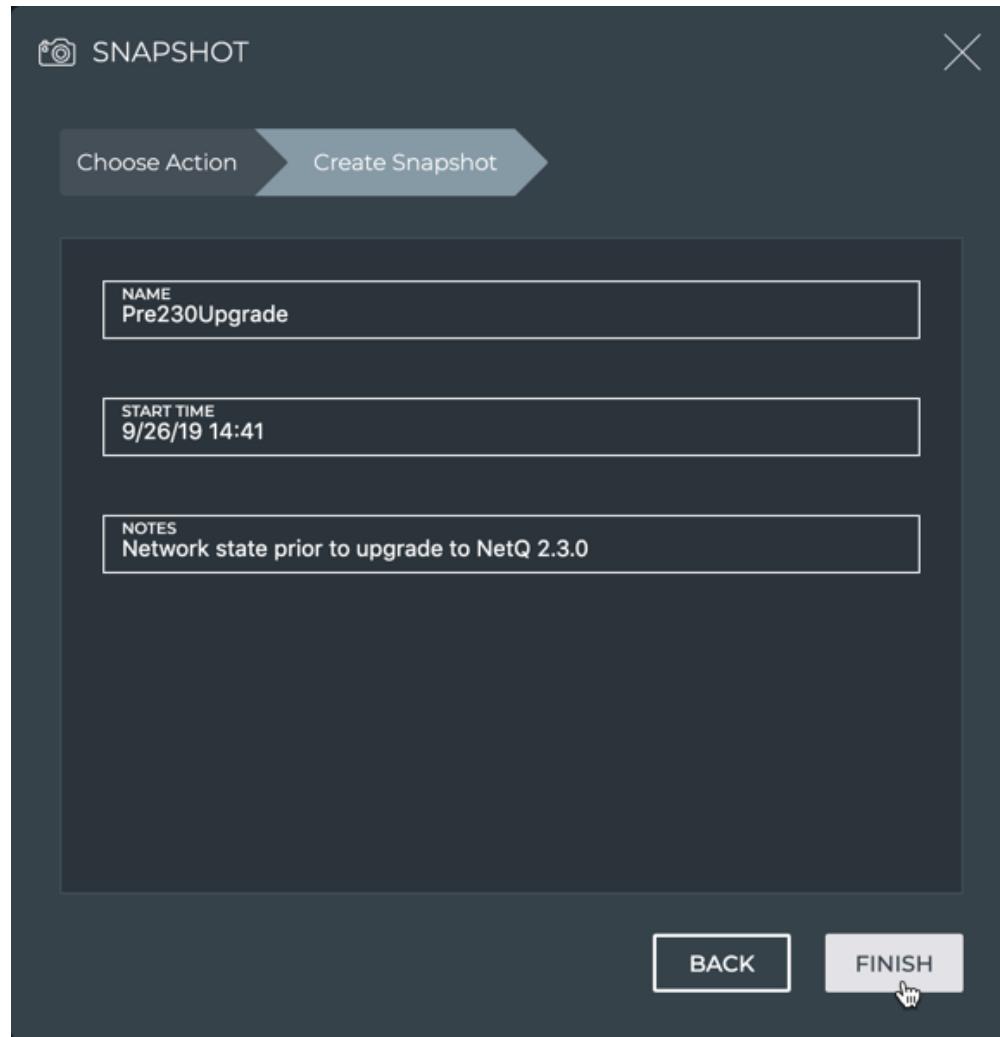
As an administrator, you want to manage the deployment of Cumulus NetQ software onto your network devices (servers, appliances, switches, and hosts) in the most efficient way and with the most information about the process as possible. With this release, NetQ provides the first of many features to enable you to do just that. It includes the ability to take a snapshot of the live network state and configuration before you make changes to your network, take a snapshot after you make those changes, and then compare them.

## Create a Network Snapshot

It is simple to capture the state of your network using the snapshot feature.

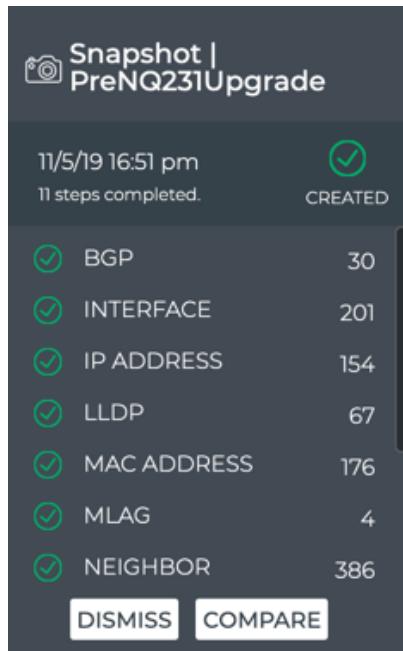
To create a snapshot:

1. From any workbench, click  in the workbench header.
2. Click **Create Snapshot**.
3. Enter a name and, optionally, a descriptive note for the snapshot.



4. Click **Finish**.

A medium Snapshot card appears on your desktop. Spinning arrows are visible while it works. When it finishes you can see the number of items that have been captured, and if any failed. This example shows a successful result.



NOTE

If you change your mind and do not want to create the snapshot, click **Back** or **Choose Action**. Do not click **Done** until you are ready to close the card. Done saves the snapshot automatically.

## Compare Network Snapshots

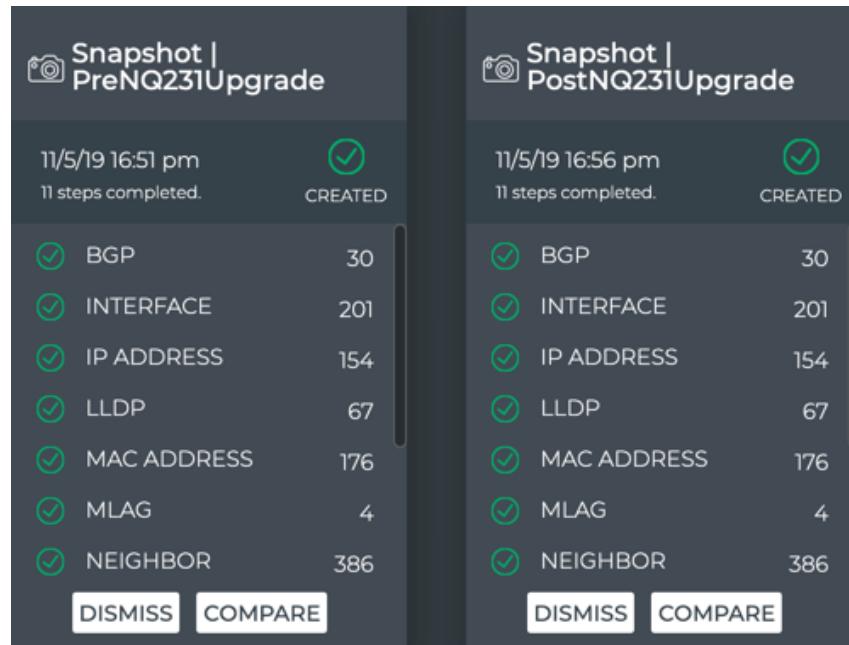
You can compare the state of your network before and after an upgrade or other configuration change to validate the changes.

To compare network snapshots:

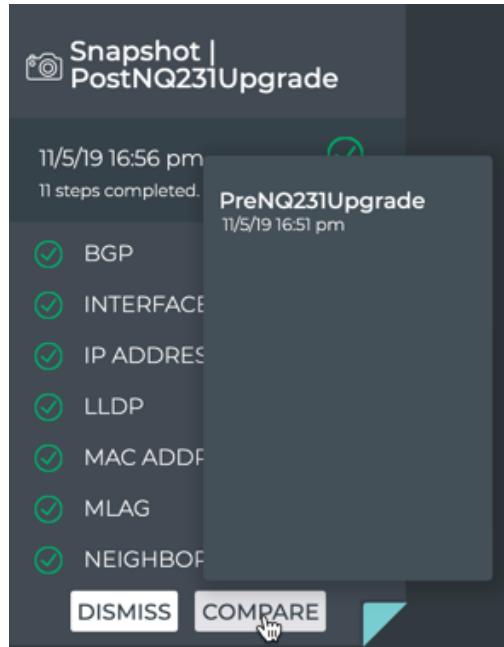
1. Create a snapshot (as described in previous section) *before* you make any changes.
2. Make your changes.
3. Create a second snapshot.

4. Compare the results of the two snapshots:

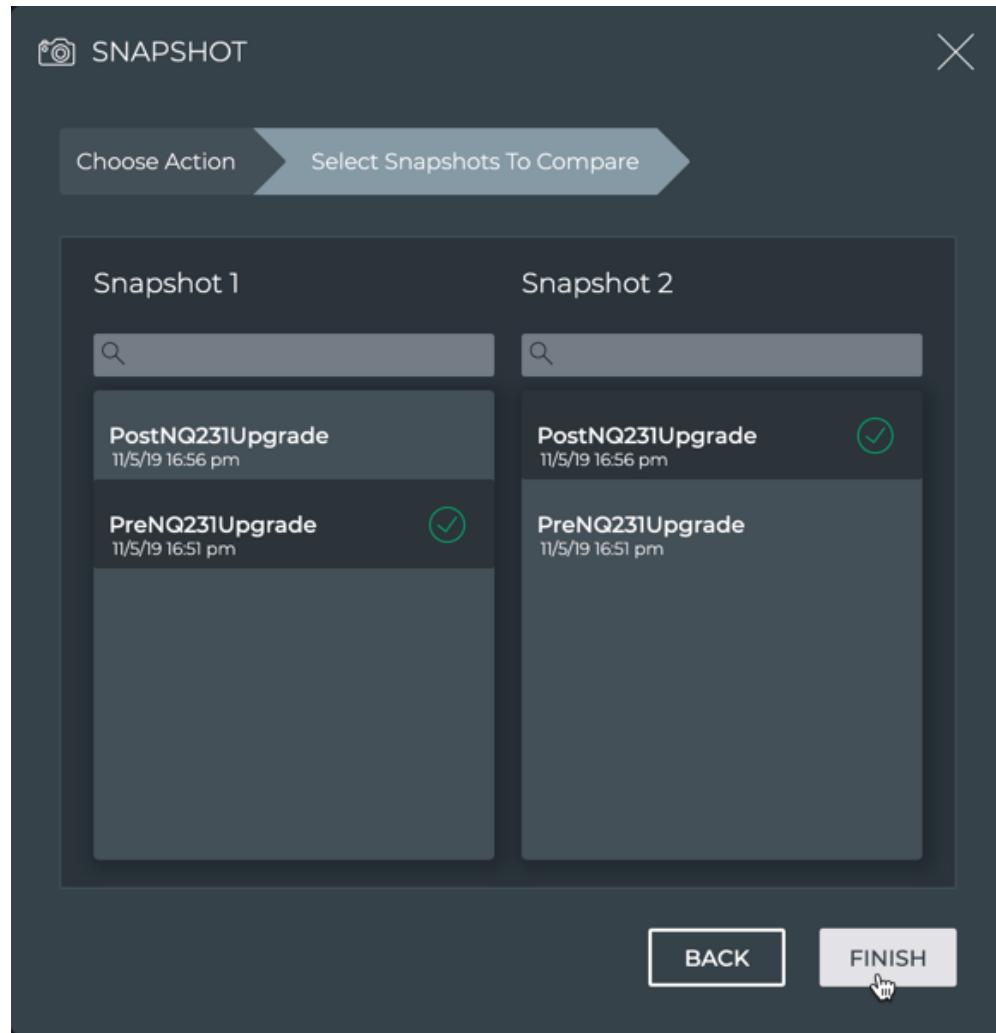
- If you have the two desired snapshot cards open:
  - Simply put them next to each other to view an overview.
  - Scroll down to see all of the items.



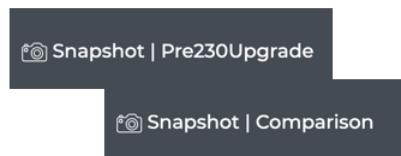
- If you have only one of the cards open:
  - Click **Compare** on the open card.
  - Select the snapshot to compare with. Note that only snapshots taken before this snapshot appear in the selection list.

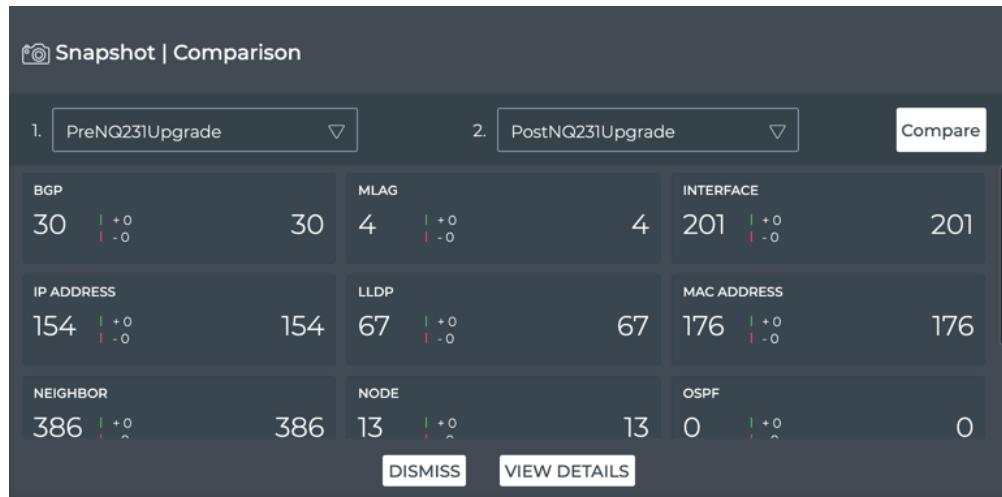


- If you have closed one or both of the cards (you may have created them some time before):
  - Click 
  - .
  - Click **Compare Snapshots**.
  - Click on the two snapshots you want to compare.
  - Click **Finish**. Note that two snapshots must be selected before **Finish** is active.



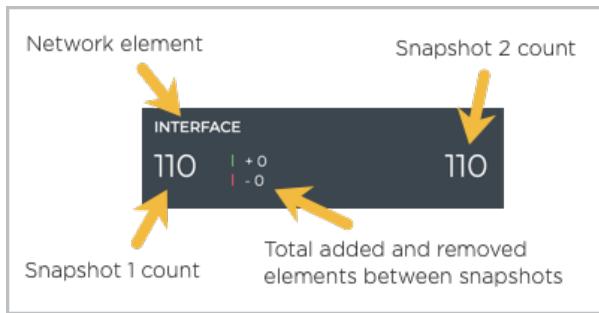
In the latter two cases, the large Snapshot card opens. The only difference is in the card title. If you opened the comparison card from a snapshot on your workbench, the title includes the name of that card. If you open the comparison card through the Snapshot menu, the title is generic, indicating a comparison only. Functionally, you have reached the same point.





### Interpreting the Comparison Data

For each network element that is compared, count values and changes are shown:



For example, if the snapshot taken first had a total count of 110 interfaces, changes were made that added 40 interfaces and removed 32 interfaces before the second snapshot was taken, the second snapshot total count of interfaces would be eight more than in the first snapshot, or 118.

From this card, you can also change which snapshots to compare. Select an alternate snapshot from one of the two snapshot dropdowns and then click **Compare**.

[VIEW CHANGE DETAILS](#)

You can view additional details about the changes that have occurred between the two snapshots by clicking **View Details**. This opens the full screen Detailed Snapshot Comparison card.

From this card you can:

- see each of the elements that was added and removed, and various information about each
- export the results per element

Detailed Snapshot Comparison					
BGP	PRE230UPGRADE ← POST230UPGRADE			REMOVED	ADDED
CLAG					14 RESULTS
INTERFACE	EXPORT				
IP ADDRESS	HOST NAME	PREFIX	MASK	IF NAME	
LINKS	oob-mgmt-server	fe80:f852:3cff:fe...	64	veth160fa814	
LLDP	oob-mgmt-server	fe80:f098:bffff...	64	flannel.1	
MAC ADDRESS	oob-mgmt-server	fe80:d8bc:38fff...	64	cni0	
NEIGHBOR	oob-mgmt-server	fe80:cc0a:31fff:fe...	64	vethcb9f215c	
NODE	oob-mgmt-server	fe80:c4fc:8bffff...	64	veth5d413b20	
OSPF	oob-mgmt-server	fe80:9025f7ff:fe...	64	veth05b5d569	
ROUTE	oob-mgmt-server	fe80:6cd8:ffff:fe...	64	veth4a1ca00e	
SENSORS	oob-mgmt-server	fe80:5054:ffff:fe...	64	eth0	
SERVICES	exit02	10.255.8.233	24	eth0	
	exit02	fe80:fcce:61ffff...	64	vlan4001	
	exit01	fe80:3429:65ffff...	64	bridge	
				vlan4001	

Element	Data Descriptions
BGP	<ul style="list-style-type: none"> <li>• <b>Hostname:</b> Name of the host running the BGP session</li> <li>• <b>VRF:</b> Virtual route forwarding interface if used</li> <li>• <b>BGP Session:</b> Session that was removed or added</li> <li>• <b>ASN:</b> Autonomous system number</li> </ul>
CLAG	<ul style="list-style-type: none"> <li>• <b>Hostname:</b> Name of the host running the CLAG session</li> <li>• <b>CLAG Sysmac:</b> MAC address for a bond interface pair that was removed or added</li> </ul>
Interface	<ul style="list-style-type: none"> <li>• <b>Hostname:</b> Name of the host where the interface resides</li> <li>• <b>IF Name:</b> Name of the interface that was removed or added</li> </ul>

Element	Data Descriptions
IP Address	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host where address was removed or added</li> <li><b>Prefix:</b> IP address prefix</li> <li><b>Mask:</b> IP address mask</li> <li><b>IF Name:</b> Name of the interface that owns the address</li> </ul>
Links	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host where the link was removed or added</li> <li><b>IF Name:</b> Name of the link</li> <li><b>Kind:</b> Bond, bridge, eth, loopback, macvlan, swp, vlan, vrf, or vxlan</li> </ul>
LLDP	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the discovered host that was removed or added</li> <li><b>IF Name:</b> Name of the interface</li> </ul>
MAC Address	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host where MAC address resides</li> <li><b>MAC address:</b> MAC address that was removed or added</li> <li><b>VLAN:</b> VLAN associated with the MAC address</li> </ul>
Neighbor	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the neighbor peer that was removed or added</li> <li><b>VRF:</b> Virtual route forwarding interface if used</li> <li><b>IF Name:</b> Name of the neighbor interface</li> <li><b>IP address:</b> Neighbor IP address</li> </ul>
Node	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the network node that was removed or added</li> </ul>

Element	Data Descriptions
OSPF	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host running the OSPF session</li> <li><b>IF Name:</b> Name of the associated interface that was removed or added</li> <li><b>Area:</b> Routing domain for this host device</li> <li><b>Peer ID:</b> Network subnet address of router with access to the peer device</li> </ul>
Route	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host running the route that was removed or added</li> <li><b>VRF:</b> Virtual route forwarding interface associated with route</li> <li><b>Prefix:</b> IP address prefix</li> </ul>
Sensors	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host where sensor resides</li> <li><b>Kind:</b> Power supply unit, fan, or temperature</li> <li><b>Name:</b> Name of the sensor that was removed or added</li> </ul>
Services	<ul style="list-style-type: none"> <li><b>Hostname:</b> Name of the host where service is running</li> <li><b>Name:</b> Name of the service that was removed or added</li> <li><b>VRF:</b> Virtual route forwarding interface associated with service</li> </ul>

## Manage Network Snapshots

You can create as many snapshots as you like and view them at any time. When a snapshot becomes old and no longer useful, you can remove it.

To view an existing snapshot:

- From any workbench, click  in the workbench header.
- Click **View/Delete Snapshots**.

3. Click **View**.
4. Click the snapshot you want to view, then click **Finish**.

Click **Back** or **Choose Action** to cancel viewing of your selected snapshot.

To remove an existing snapshot:

1. From any workbench, click  in the workbench header.
2. Click **View/Delete Snapshots**.
3. Click **Delete**.
4. Click the snapshot you want to remove, then click **Finish**.

Click **Back** or **Choose Action** to cancel the deletion of your selected snapshot.

# Monitor Network Performance

The core capabilities of Cumulus NetQ enable you to monitor your network by viewing performance and configuration data about your individual network devices and the entire fabric network-wide. The topics contained in this section describe monitoring tasks that apply across the entire network. For device-specific monitoring refer to [Monitor Switches](#).

# Monitor Network Health

As with any network, one of the challenges is keeping track of all of the moving parts.

With the NetQ GUI, you can view the overall health of your network at a glance and then delve deeper for periodic checks or as conditions arise that require attention. For a general understanding of how well your network is operating, the Network Health card workflow is the best place to start as it contains the highest view and performance rollups.

## Network Health Card Workflow Summary

The small Network Health card displays:



Item	Description
⌚	Indicates data is for overall Network Health

Item	Description
Health trend	<p>Trend of overall network health, represented by an arrow:</p> <ul style="list-style-type: none"> <li>• <b>Pointing upward and green:</b> Health score in the most recent window is higher than in the last two data collection windows, an increasing trend</li> <li>• <b>Pointing downward and bright pink:</b> Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend</li> <li>• <b>No arrow:</b> Health score is unchanged over the last two data collection windows, trend is steady</li> </ul> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Health score	<p>Average of health scores for system health, network services health, and interface health during the last data collection window. The health score for each category is calculated as the percentage of items which passed validations versus the number of items checked.</p> <p>The collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Health rating	<p>Performance rating based on the health score during the time window:</p> <ul style="list-style-type: none"> <li>• <b>Low:</b> Health score is less than 40%</li> <li>• <b>Med:</b> Health score is between 40% and 70%</li> <li>• <b>High:</b> Health score is greater than 70%</li> </ul>
Chart	<p>Distribution of overall health status during the designated time period</p>

The medium Network Health card displays the distribution, score, and trend of the:

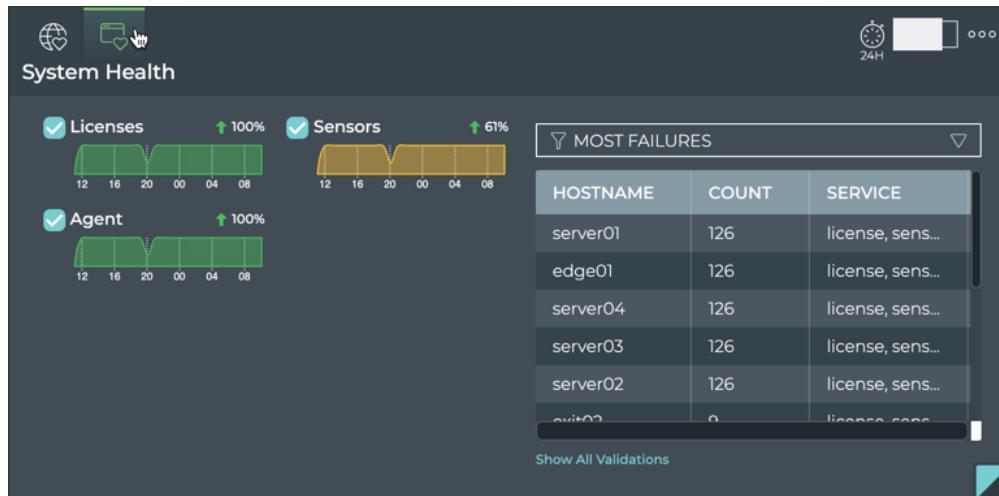


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for overall Network Health
Health trend	<p>Trend of system, network service, and interface health, represented by an arrow:</p> <ul style="list-style-type: none"> <li><b>Pointing upward and green:</b> Health score in the most recent window is higher than in the last two data collection windows, an increasing trend</li> <li><b>Pointing downward and bright pink:</b> Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend</li> <li><b>No arrow:</b> Health score is unchanged over the last two data collection windows, trend is steady</li> </ul> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>

Item	Description
Health score	<p>Percentage of devices which passed validation versus the number of devices checked during the time window for:</p> <ul style="list-style-type: none"> <li><b>System health:</b> NetQ Agent health, Cumulus Linux license status, and sensors</li> <li><b>Network services health:</b> BGP, CLAG, EVPN, LNV, NTP, OSPF, and VXLAN health</li> <li><b>Interface health:</b> interfaces MTU, VLAN health</li> </ul> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Chart	Distribution of overall health status during the designated time period

The large Network Health card contains two tabs.

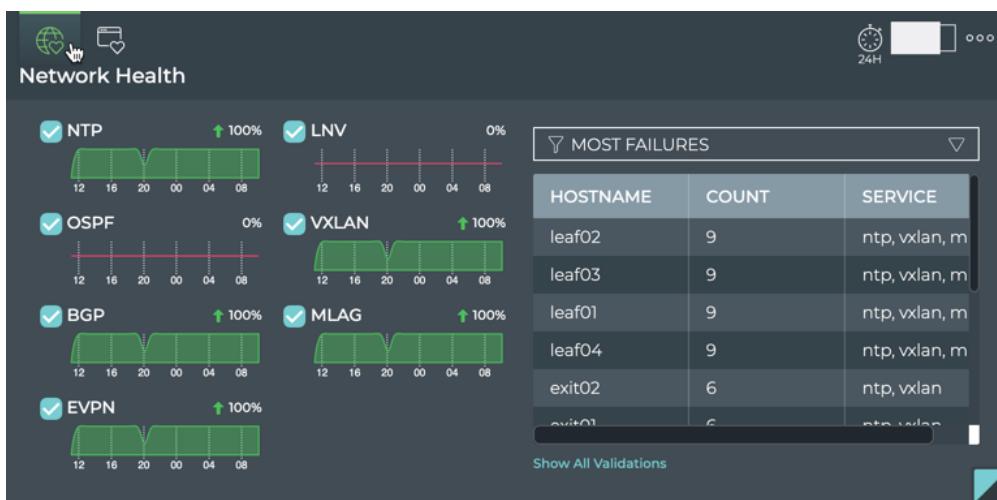
The *System Health* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for System Health
Health trend	<p>Trend of NetQ Agents, Cumulus Linux licenses, and sensor health, represented by an arrow:</p> <ul style="list-style-type: none"> <li><b>Pointing upward and green:</b> Health score in the most recent window is higher than in the last two data collection windows, an increasing trend</li> <li><b>Pointing downward and bright pink:</b> Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend</li> <li><b>No arrow:</b> Health score is unchanged over the last two data collection windows, trend is steady</li> </ul> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Health score	<p>Percentage of devices which passed validation versus the number of devices checked during the time window for NetQ Agents, Cumulus Linux license status, and platform sensors.</p> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Charts	Distribution of health score for NetQ Agents, Cumulus Linux license status, and platform sensors during the designated time period

Item	Description
Table	<p>Listing of items that match the filter selection:</p> <ul style="list-style-type: none"> <li>• <b>Most Failures:</b> Devices with the most validation failures are listed at the top</li> <li>• <b>Recent Failures:</b> Most recent validation failures are listed at the top</li> </ul>
Show All Validations	Opens full screen Network Health card with a listing of validations performed by network service and protocol

The *Network Health* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for Network Protocols and Services Health

Item	Description
Health trend	<p>Trend of BGP, CLAG, EVPN, LNV, NTP, OSPF, and VXLAN services health, represented by an arrow:</p> <ul style="list-style-type: none"> <li>• <b>Pointing upward and green:</b> Health score in the most recent window is higher than in the last two data collection windows, an increasing trend</li> <li>• <b>Pointing downward and bright pink:</b> Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend</li> <li>• <b>No arrow:</b> Health score is unchanged over the last two data collection windows, trend is steady</li> </ul> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Health score	<p>Percentage of devices which passed validation versus the number of devices checked during the time window for BGP, CLAG, EVPN, LNV, NTP, and VXLAN protocols and services.</p> <p>The data collection window varies based on the time period of the card. For a 24 hour time period (default), the window is one hour. This gives you current, hourly, updates about your network health.</p>
Charts	<p>Distribution of passing validations for BGP, CLAG, EVPN, LNV, NTP, and VXLAN services during the designated time period</p>
Table	<p>Listing of devices that match the filter selection:</p> <ul style="list-style-type: none"> <li>• <b>Most Failures:</b> Devices with the most validation failures are listed at the top</li> <li>• <b>Recent Failures:</b> Most recent validation failures are listed at the top</li> </ul>

Item	Description
Show All Validations	Opens full screen Network Health card with a listing of validations performed by network service and protocol

The full screen Network Health card displays all events in the network.

The screenshot shows a full-screen Network Health card. On the left is a sidebar with a tree view of network services: BGP, OSPF, NTP, LNV, VXLAN, MLAG, EVPN, Interfaces, VLAN, MTU, Agents, Sensors, and License. The BGP node is expanded. At the top center, there's a search bar with a magnifying glass icon and a dropdown menu labeled "DEFAULT TIME Past 24 Hours". To the right of the search bar is a button labeled "Export" and a gear icon. The main area contains a table titled "72 RESULTS". The table has columns: VALIDATION LABEL, TIME, CHECKED NODE COUNT, FAILED NODE COUNT, FAILED SESSION COUNT, and TOTAL SESSION COUNT. The data in the table is as follows:

VALIDATION LABEL	TIME	CHECKED NODE COUNT	FAILED NODE COUNT	FAILED SESSION COUNT	TOTAL SESSION COUNT
BgpEvpn	10/3/19 12:27 PM	8	0	0	30
BgpEvpn (old)	10/3/19 12:27 PM	8	0	0	30
Default validation	10/3/19 12:16 PM	8	0	0	30
BgpEvpn	10/3/19 11:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 11:27 AM	8	0	0	30
Default validation	10/3/19 11:16 AM	8	0	0	30
BgpEvpn	10/3/19 10:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 10:27 AM	8	0	0	30
Default validation	10/3/19 10:16 AM	8	0	0	30
BgpEvpn	10/3/19 9:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 9:27 AM	8	0	0	30
Default validation	10/3/19 9:16 AM	8	0	0	30
BgpEvpn	10/3/19 8:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 8:27 AM	8	0	0	30
Default validation	10/3/19 8:16 AM	8	0	0	30
BgpEvpn	10/3/19 7:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 7:27 AM	8	0	0	30
Default validation	10/3/19 7:16 AM	8	0	0	30

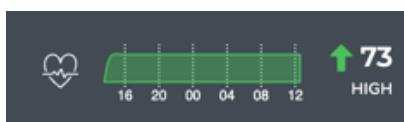
Item	Description
Title	Network Health
×	Closes full screen card and returns to workbench
Default Time	Range of time in which the displayed data was collected
Results	Number of results found for the selected tab

Item	Description
Each network protocol or service	<p>Displays results of that network protocol or service validations that occurred during the designated time period. By default, the requests list is sorted by the date and time that the validation was completed (<b>Time</b>). This tab provides the following additional data about each protocol and service:</p> <ul style="list-style-type: none"> <li>• <b>Validation Label:</b> User-defined name of a validation or Default validation</li> <li>• <b>Checked Node Count:</b> Number of nodes running the service included in the validation</li> <li>• <b>Failed Node Count:</b> Number of nodes that failed the validation</li> <li>• <b>Failed Session Count:</b> Number of sessions that failed the validation. Only applies to BGP, CLAG, EVPN, and OSPF.</li> <li>• <b>Total Session Count:</b> Number of sessions running the protocol or service included in the validation. Only applies to BGP, CLAG, EVPN, and OSPF.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

## View Network Health Summary

Overall network health is based on successful validation results. The summary includes the percentage of successful results, a trend indicator, and a distribution of the validation results.

To view a summary of your network health, open the small Network Health card.



## Monitor Network Health

## View Key Metrics of Network Health

In this example, the overall health is relatively good, but improving compared to recent status. Refer to the next section for viewing the key health metrics.

## View Key Metrics of Network Health

Overall network health is a calculated average of several key health metrics: System, Network Services, and Interface health.

To view these key metrics, open the medium Network Health card. Each metric is shown with the percentage of successful validations, a trend indicator, and a distribution of the validation results.



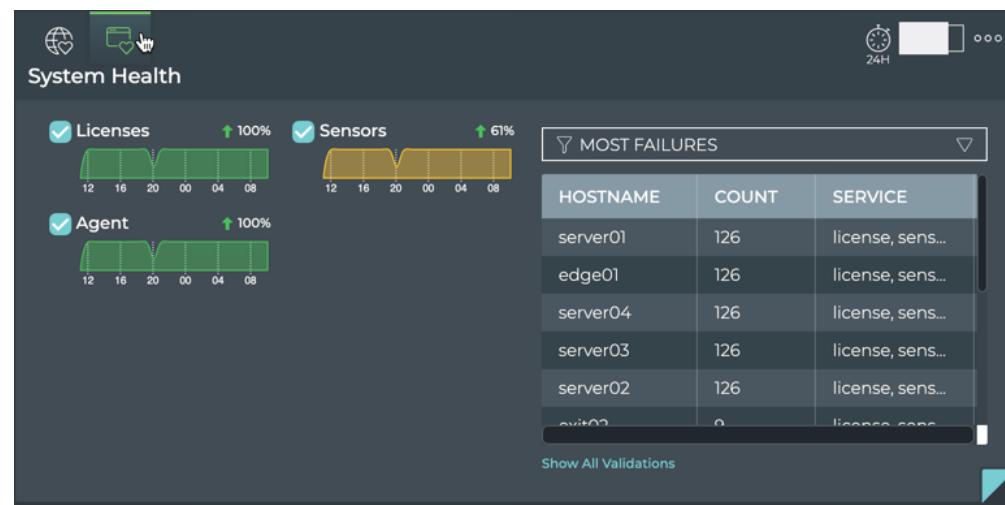
In this example, the health of each of the system and network services are good, but interface health is on the lower side. While it is improving, you might choose to dig further if it does not continue to improve. Refer to the following section for additional details.

## View System Health

The system health is a calculated average of the NetQ Agent, Cumulus Linux license, and sensor health metrics. In all cases, validation is performed on the agents and licenses. If you are monitoring platform sensors, the calculation includes these as well. You can view the overall health of the system from the medium Network Health card and information about each component from the large Network Health card.

To view information about each system component:

1. Open the large Network Health card.
2. Hover over the card and click



The health of each protocol or service is represented on the left side of the card by a distribution of the health score, a trend indicator, and a percentage of successful results. The right side of the card provides a listing of devices running the services.

## View Devices with the Most Issues

It is useful to know which devices are experiencing the most issues with their system services in general, as this can help focus troubleshooting efforts toward selected

devices versus the service itself. To view devices with the most issues, select **Most Failures** from the filter above the table on the right.



Devices with the highest number of issues are listed at the top. Scroll down to view those with fewer issues. To further investigate the critical devices, open the Event cards and filter on the indicated switches.

#### View Devices with Recent Issues

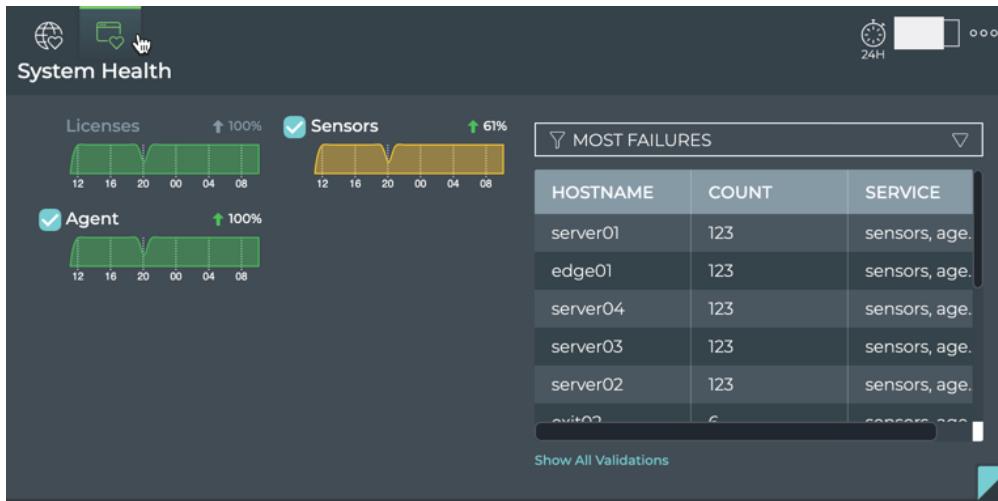
It is useful to know which devices are experiencing the most issues with their network services right now, as this can help focus troubleshooting efforts toward selected devices versus the service itself. To view devices with recent issues, select **Recent Failures** from the filter above the table on the right. Devices with the highest number of issues are listed at the top. Scroll down to view those with fewer issues. To further investigate the critical devices, open the Switch card or the Event cards and filter on the indicated switches.

#### Filter Results by System Service

You can focus the data in the table on the right, by unselecting one or more services. Click the checkbox next to the service you want to remove from the data. In this example, we have unchecked Licenses.

## Monitor Network Health

## View Network Services Health



This removes the checkbox next to the associated chart and grays out the title of the chart, temporarily removing the data related to that service from the table. Add it back by hovering over the chart and clicking the checkbox that appears.

## View Network Services Health

The network services health is a calculated average of the individual network protocol and services health metrics. In all cases, validation is performed on NTP. If you are running BGP, CLAG, EVPN, LNV, OSPF, or VXLAN protocols the calculation includes these as well. You can view the overall health of network services from the medium Network Health card and information about individual services from the large Network Health card.

To view information about each network protocol or service:

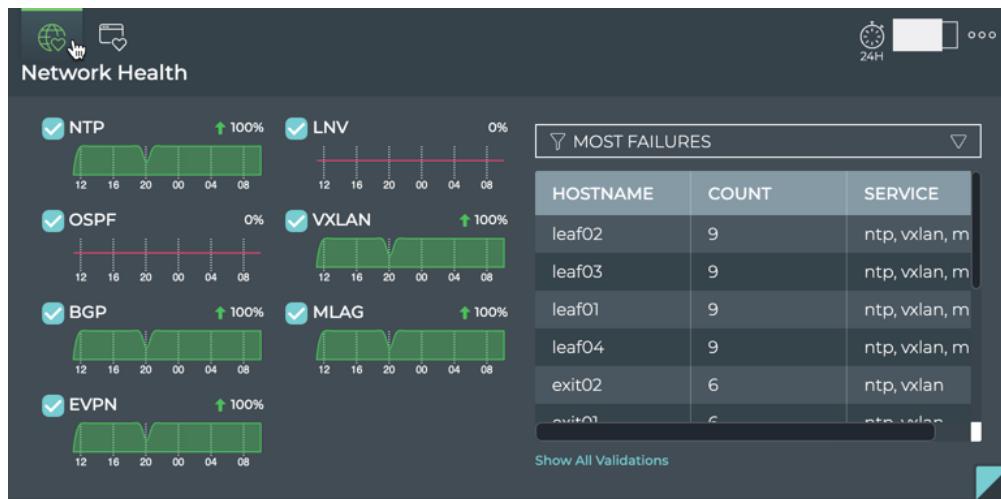
1. Open the large Network Health card.
2. Hover over the card and click



.

## Monitor Network Health

## View Network Services Health



The health of each protocol or service is represented on the left side of the card by a distribution of the health score, a trend indicator, and a percentage of successful results. The right side of the card provides a listing of devices running the services.



If you have more services running than fit naturally into the chart area, a scroll bar appears for you to access their data.

Use the scroll bars on the table to view more columns and rows.

## View Devices with the Most Issues

It is useful to know which devices are experiencing the most issues with their network services in general, as this can help focus troubleshooting efforts toward selected devices versus the protocol or service. To view devices with the most issues, open the large Network Health card. Select **Most Failures** from the dropdown above the table on the right.



## Monitor Network Health

## View Network Services Health

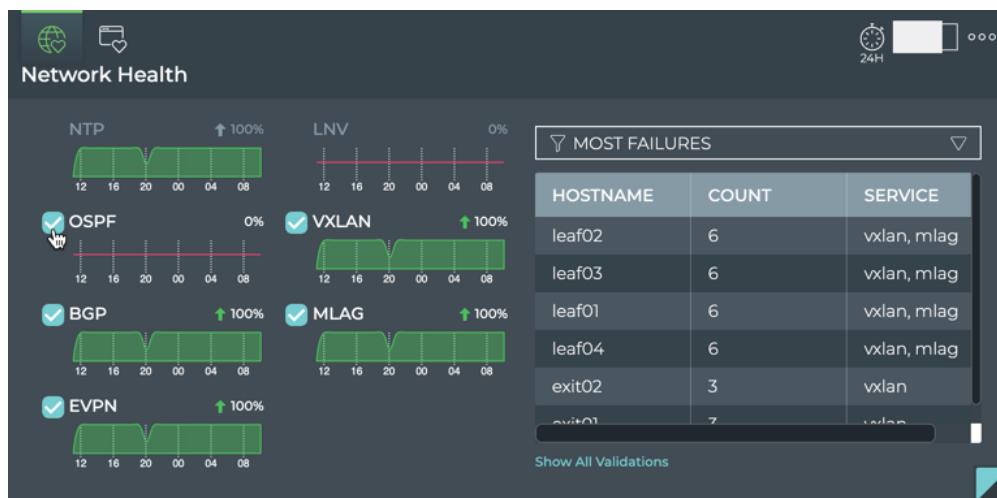
Devices with the highest number of issues are listed at the top. Scroll down to view those with fewer issues. To further investigate the critical devices, open the Event cards and filter on the indicated switches.

### View Devices with Recent Issues

It is useful to know which devices are experiencing the most issues with their network services right now, as this can help focus troubleshooting efforts toward selected devices versus the protocol or service. To view devices with the most issues, open the large Network Health card. Select **Recent Failures** from the dropdown above the table on the right. Devices with the highest number of issues are listed at the top. Scroll down to view those with fewer issues. To further investigate the critical devices, open the Switch card or the Event cards and filter on the indicated switches.

### Filter Results by Network Service

You can focus the data in the table on the right, by unselecting one or more services. Click the checkbox next to the service you want to remove. In this example, we removed NTP and LNV and are in the process of removing OSPF.



This grays out the chart title and removes the associated checkbox, temporarily removing the data related to that service from the table.

## View All Network Protocol and Service Validation Results

The Network Health card workflow enables you to view all of the results of all validations run on the network protocols and services during the designated time period.

To view all the validation results:

1. Open the full screen Network Health card.
2. Click <network protocol or service name> tab in the navigation panel.
3. Look for patterns in the data. For example, when did nodes, sessions, links, ports, or devices start failing validation? Was it at a specific time? Was it when you starting running the service on more nodes? Did sessions fail, but nodes were fine?

The screenshot shows a Network Health card with a sidebar on the left containing icons for various protocols and services: BGP, OSPF, NTP, LNV, VXLAN, MLAG, EVPN, Interfaces, VLAN, MTU, Agents, Sensors, and License. The BGP section is currently selected. The main area displays a table with the following data:

VALIDATION LABEL	TIME	CHECKED NODE COUNT	FAILED NODE COUNT	FAILED SESSION COUNT	TOTAL SESSION COUNT
BgpEvpn	10/3/19 12:27 PM	8	0	0	30
BgpEvpn (old)	10/3/19 12:27 PM	8	0	0	30
Default validation	10/3/19 12:16 PM	8	0	0	30
BgpEvpn	10/3/19 11:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 11:27 AM	8	0	0	30
Default validation	10/3/19 11:16 AM	8	0	0	30
BgpEvpn	10/3/19 10:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 10:27 AM	8	0	0	30
Default validation	10/3/19 10:16 AM	8	0	0	30
BgpEvpn	10/3/19 9:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 9:27 AM	8	0	0	30
Default validation	10/3/19 9:16 AM	8	0	0	30
BgpEvpn	10/3/19 8:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 8:27 AM	8	0	0	30
Default validation	10/3/19 8:16 AM	8	0	0	30
BgpEvpn	10/3/19 7:27 AM	8	0	0	30
BgpEvpn (old)	10/3/19 7:27 AM	8	0	0	30
Default validation	10/3/19 7:16 AM	8	0	0	30

Where to go next depends on what data you see, but a few options include:

- Look for matching event information for the failure points in a given protocol or service.
- When you find failures in one protocol, compare with higher level protocols to see if they fail at a similar time (or vice versa with supporting services).
- Export the data for use in another analytics tool, by clicking **Export** and providing a name for the data file.

# Validate Network Protocol and Service Operations

With the NetQ UI, you can validate the operation of the network protocols and services running in your network either on demand or on a scheduled basis. There are three card workflows to perform this validation: one for creating the validation request (either on-demand or scheduled) and two validation results (one for on-demand and one for scheduled).

This release supports validation of the following network protocols and services: Agents, BGP, CLAG, EVPN, Interfaces, License, MTU, NTP, OSPF, Sensors, VLAN, and VXLAN.

For a more general understanding of how well your network is operating, refer to the [Monitor Network Health](#) topic.

## Create Validation Requests

The Validation Request card workflow is used to create on-demand validation requests to evaluate the health of your network protocols and services.

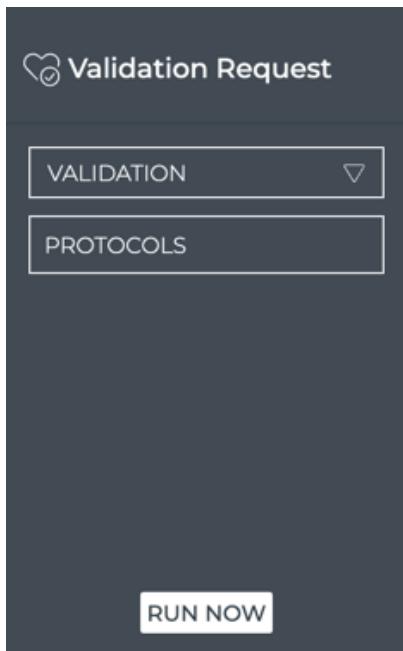
### Validation Request Card Workflow

The small Validation Request card displays:



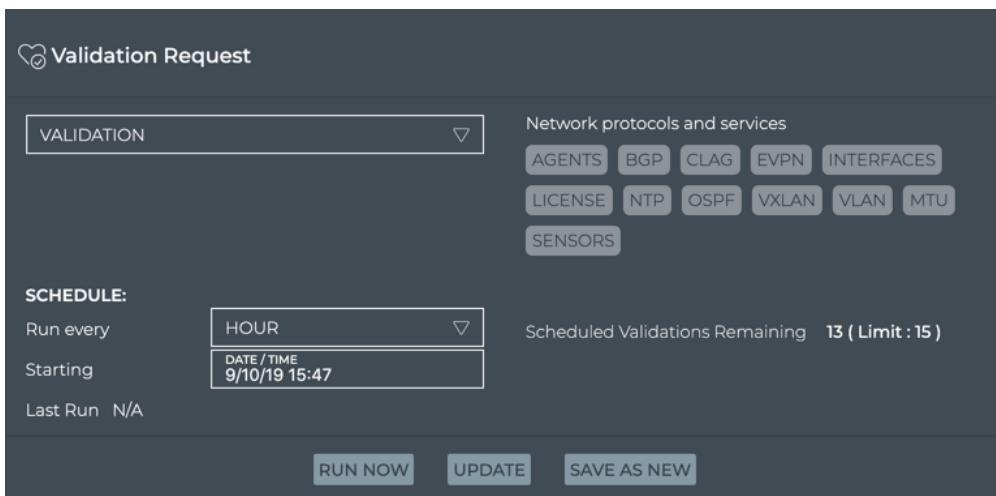
Item	Description
	Indicates a validation request
Validation	Select a scheduled request to run that request on-demand. A default validation is provided for each supported network protocol and service, which runs a network-wide validation check. These validations run every 60 minutes, but you may run them on-demand at any time.  <b>Note:</b> No new requests can be configured from this size card.
GO	Start the validation request. The corresponding On-demand Validation Result cards are opened on your workbench, one per protocol and service.

The medium Validation Request card displays:



Item	Description
	Indicates a validation request
Title	Validation Request
Validation	<p>Select a scheduled request to run that request on-demand. A default validation is provided for each supported network protocol and service, which runs a network-wide validation check. These validations run every 60 minutes, but you may run them on-demand at any time.</p> <p><b>Note:</b> No new requests can be configured from this size card.</p>
Protocols	The protocols included in a selected validation request are listed here.
Schedule	For a selected scheduled validation, the schedule and the time of the last run are displayed.
Run Now	Start the validation request

The large Validation Request card displays:

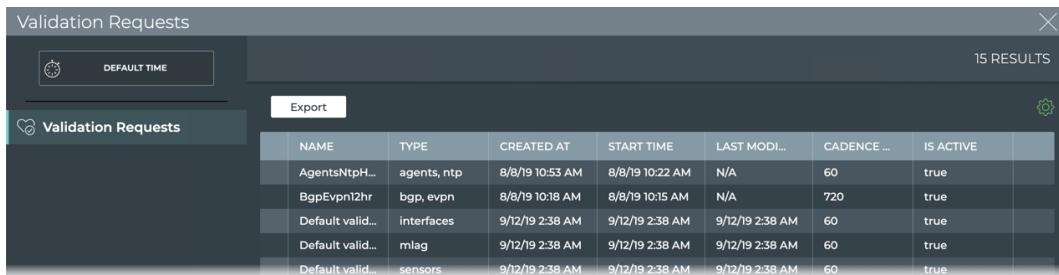


The screenshot shows the 'Validation Request' card in a dark-themed interface. At the top left is a validation request icon. Below it, the title 'Validation Request' is displayed. The main content area includes a dropdown menu labeled 'VALIDATION' with a downward arrow. To the right of the dropdown is a section titled 'Network protocols and services' containing several buttons: AGENTS, BGP, CLAG, EVPN, INTERFACES, LICENSE, NTP, OSPF, VXLAN, VLAN, MTU, and SENSORS. Below this is a 'SCHEDULE:' section with the following details: 'Run every' (set to 'HOUR'), 'Starting' (set to 'DATE / TIME 9/10/19 15:47'), and 'Last Run' (set to 'N/A'). To the right of the schedule section is a message: 'Scheduled Validations Remaining 13 (Limit : 15)'. At the bottom of the card are three buttons: 'RUN NOW', 'UPDATE', and 'SAVE AS NEW'.

Item	Description
	Indicates a validation request
Title	Validation Request
Validation	<p>Depending on user intent, this field is used to:</p> <ul style="list-style-type: none"> <li>• Select a scheduled request to run that request on-demand. A default validation is provided for each supported network protocol and service, which runs a network-wide validation check. These validations run every 60 minutes, but you may run them on-demand at any time.</li> <li>• Leave as is to create a new scheduled validation request</li> <li>• Select a scheduled request to modify</li> </ul>
Protocols	For a selected scheduled validation, the protocols included in a validation request are listed here. For new on-demand or scheduled validations, click these to include them in the validation.
Schedule:	<p>For a selected scheduled validation, the schedule and the time of the last run are displayed. For new scheduled validations, select the frequency and starting date and time.</p> <ul style="list-style-type: none"> <li>• Run Every: Select how often to run the request. Choose from 30 minutes, 1, 3, 6, or 12 hours, or 1 day.</li> <li>• Starting: Select the date and time to start the first request in the series</li> <li>• Last Run: Timestamp of when the selected validation was started</li> </ul>
Scheduled Validations	Count of scheduled validations that are currently scheduled compared to the maximum of 15 allowed

Item	Description
Run Now	Start the validation request
Update	When changes are made to a selected validation request, <b>Update</b> becomes available so that you can save your changes.
Save As New	When changes are made to a previously saved validation request, <b>Save As New</b> becomes available so that you can save the modified request as a new request.

The full screen Validation Request card displays all scheduled validation requests.



The screenshot shows a modal window titled "Validation Requests". At the top right is a close button (X). Below the title, there are two buttons: "DEFAULT TIME" and "Export". To the right of the Export button is the text "15 RESULTS". The main area contains a table with the following data:

NAME	TYPE	CREATED AT	START TIME	LAST MODI...	CADENCE ...	IS ACTIVE
AgentsNtpH...	agents, ntp	8/8/19 10:53 AM	8/8/19 10:22 AM	N/A	60	true
BgpEvpn12hr	bgp, evpn	8/8/19 10:18 AM	8/8/19 10:15 AM	N/A	720	true
Default valid...	interfaces	9/12/19 2:38 AM	9/12/19 2:38 AM	9/12/19 2:38 AM	60	true
Default valid...	mlag	9/12/19 2:38 AM	9/12/19 2:38 AM	9/12/19 2:38 AM	60	true
Default valid...	sensors	9/12/19 2:38 AM	9/12/19 2:38 AM	9/12/19 2:38 AM	60	true

Item	Description
Title	Validation Request
	Closes full screen card and returns to workbench
Default Time	No time period is displayed for this card as each validation request has its own time relationship.
Results	Number of results found for the selected tab
Validation Requests	<p>Displays all <i>scheduled</i> validation requests. By default, the requests list is sorted by the date and time that it was originally created (<b>Created At</b>). This tab provides the following additional data about each request:</p> <ul style="list-style-type: none"> <li>• <b>Name:</b> Text identifier of the validation</li> <li>• <b>Type:</b> Name of network protocols and/or services included in the validation</li> <li>• <b>Start Time:</b> Data and time that the validation request was run</li> <li>• <b>Last Modified:</b> Date and time of the most recent change made to the validation request</li> <li>• <b>Cadence (Min):</b> How often, in minutes, the validation is scheduled to run. This is empty for new on-demand requests.</li> <li>• <b>Is Active:</b> Indicates whether the request is currently running according to its schedule (<i>true</i>) or it is not running (<i>false</i>)</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

## Create On-demand and Scheduled Validation Requests

There are several types of validation requests that a user can make. Each has a slightly different flow through the Validation Request card, and is therefore described separately. The types are based on the intent of the request:

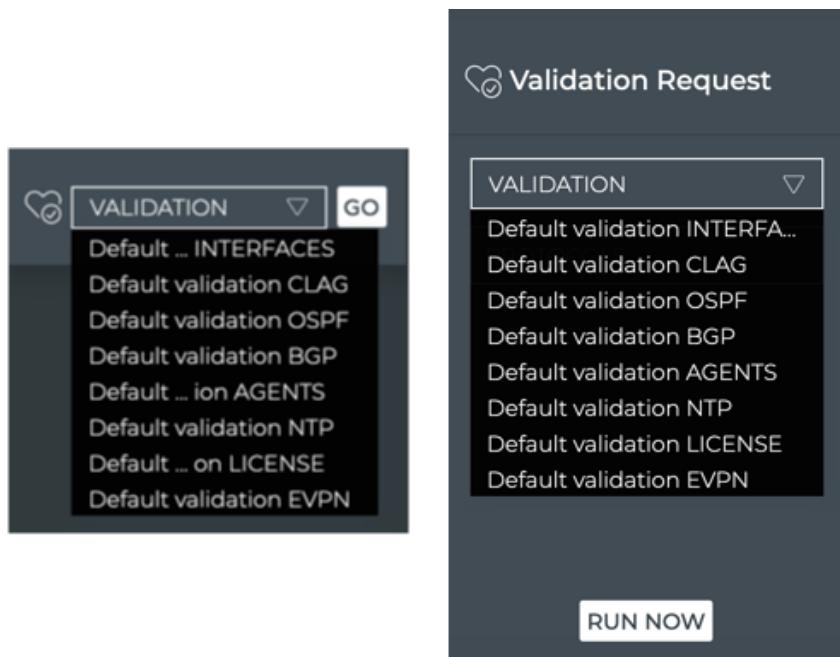
- Run an Existing Scheduled Validation Request On Demand
- Create a New On-demand Validation Request
- Create a New Scheduled Validation Request
- Modify an Existing Scheduled Validation Request

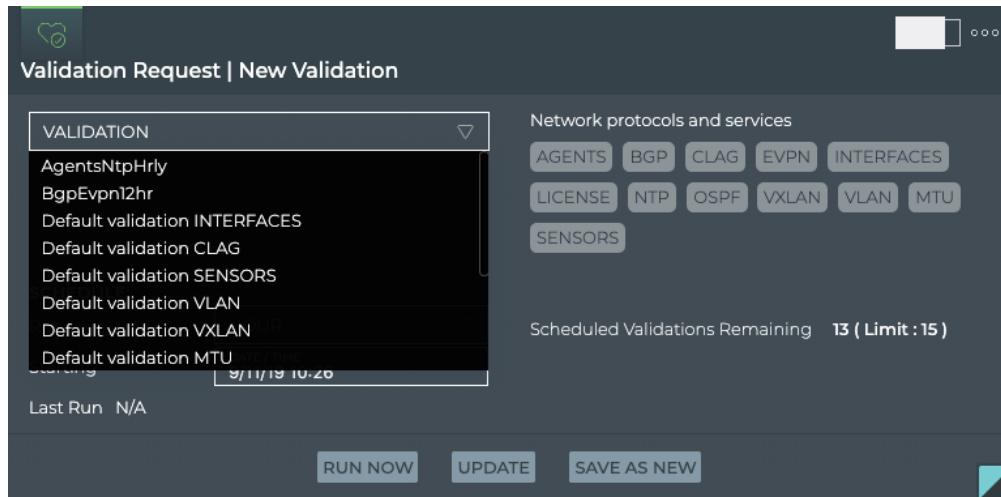
### Run an Existing Scheduled Validation Request On Demand

You may find that although you have a validation scheduled to run at a later time, you would like to run it now.

To run a scheduled validation now:

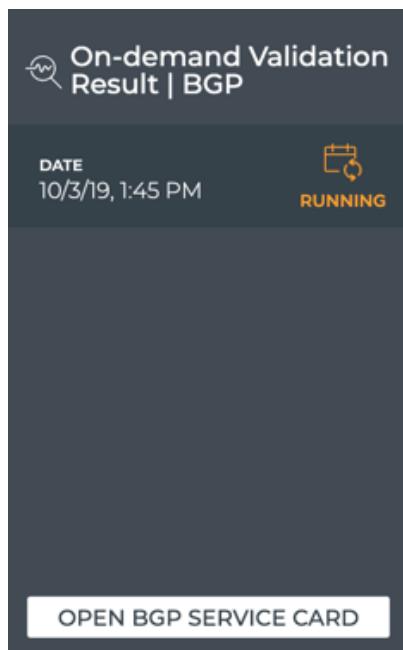
1. Open either the small, medium, or large Validation Request card.
2. Select the validation from the **Validation** dropdown list.





### 3. Click **Go** or **Run Now**.

The associated Validation Result card is opened on your workbench. Refer to [View On-demand Validation Results](#).

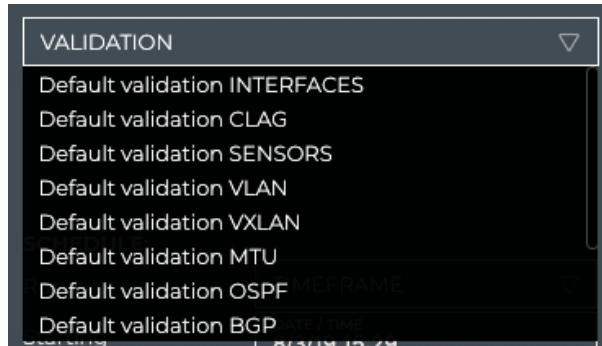


### Create a New On-demand Validation Request

When you want to validate the operation of one or more network protocols and services right now, you can create and run an on-demand validation request using the large Validation Request card.

To create and run a request for *a single* protocol or service:

1. Open the small, medium or large Validation Request card.
2. Select the validation from the **Validation** dropdown list.

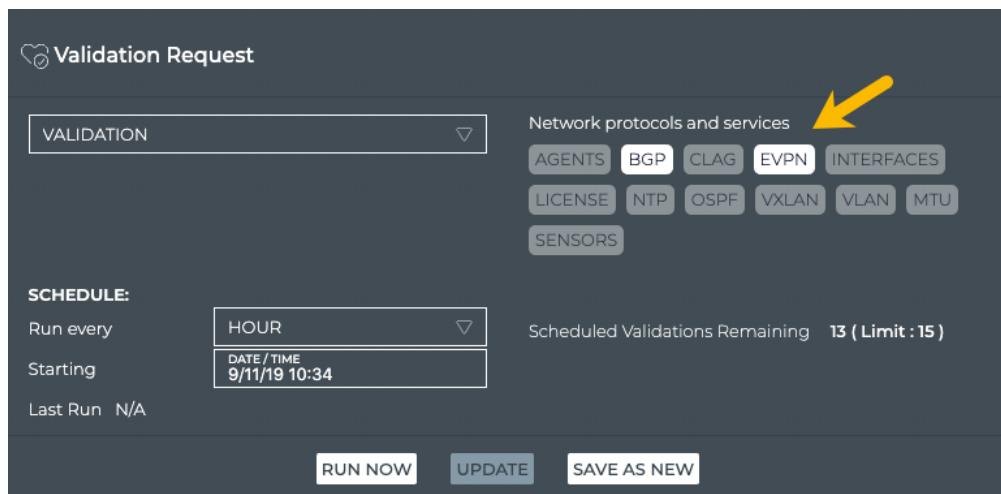


3. Click **Go** or **Run Now**.

The associated Validation Result card is opened on your workbench. Refer to [View On-demand Validation Results](#).

To create and run a request for *more than one* protocol and/or service:

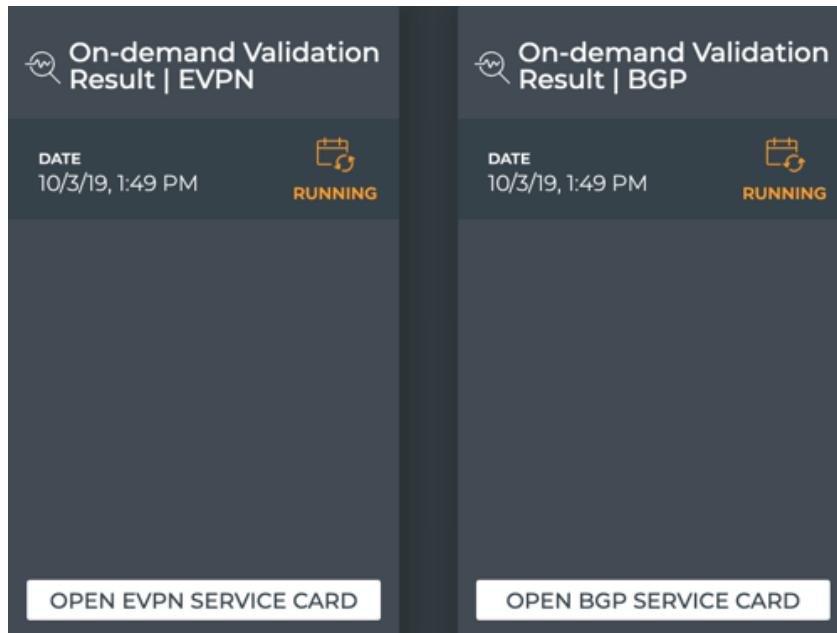
1. Open the large Validation Request card.
2. Click the names of the protocols and services you want to validate. We selected BGP and EVPN in this example.



3. Click **Run Now** to start the validation.

The associated on-demand validation result cards (one per protocol or service

selected) are opened on your current workbench. Refer to [View On-demand Validation Results](#).

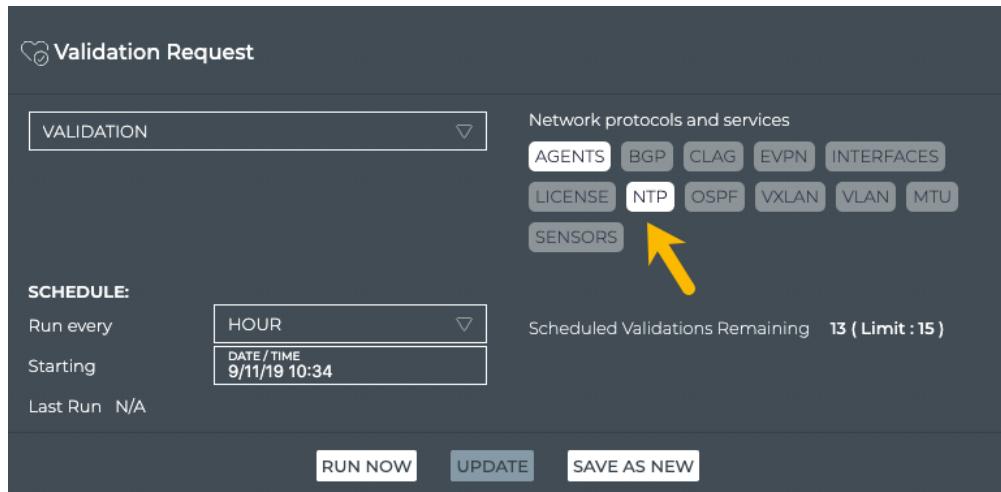


#### Create a New Scheduled Validation Request

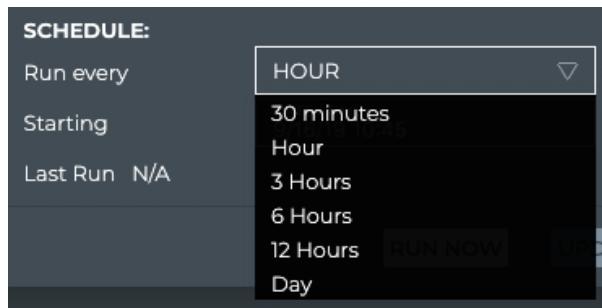
When you want to see validation results on a regular basis, it is useful to configure a scheduled validation request to avoid re-creating the request each time.

To create and run a new scheduled validation:

1. Open the large Validation Request card.
2. Select the protocols and/or services you want to include in the validation. In this example we have chosen the Agents and NTP services.

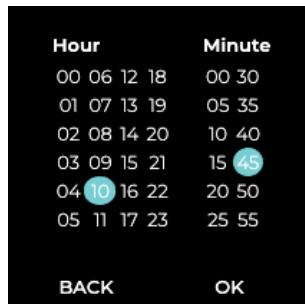


3. Enter the schedule frequency (30 min, 1 hour, 3 hours, 6 hours, 12 hours, or 1 day) by selecting it from the **Run every** list. Default is hourly.



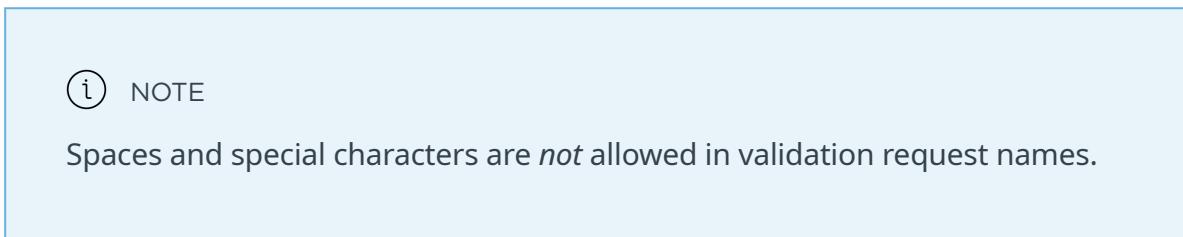
4. Select the time to start the validation runs, by clicking in the Starting field. Select a day and click **Next**, then select the starting time and click **OK**.





5. Verify the selections were made correctly.
6. Click **Save As New**.

7. Enter a name for the validation.

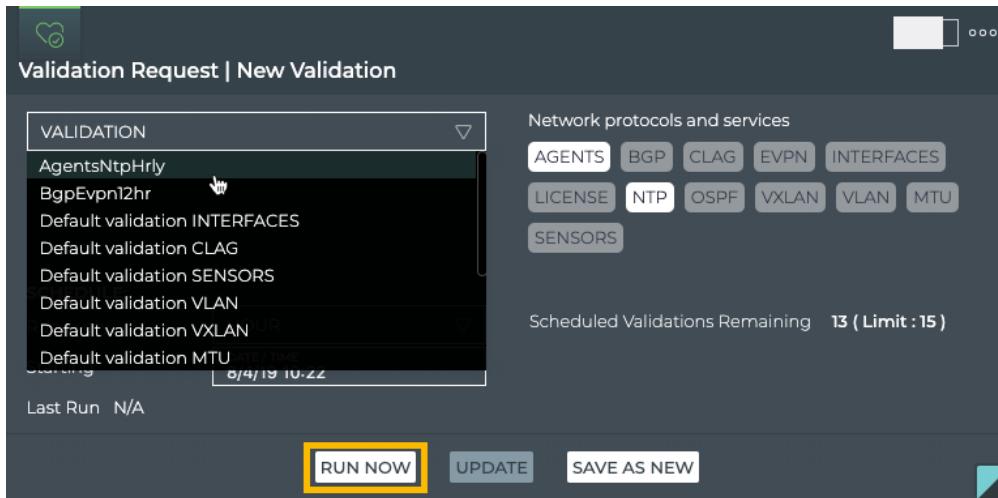


Provide a name for this new validation

SAVE
Cancel

8. Click **Save**.

The validation can now be selected from the Validation listing (on the small, medium or large size card) and run immediately using **Run Now**, or you can wait for it to run the first time according to the schedule you specified. Refer to [View Scheduled Validation Results](#). Note that the number of scheduled validations is now two (2).



### Modify an Existing Scheduled Validation Request

At some point you might want to change the schedule or validation types that are specified in a scheduled validation request.

#### IMPORTANT

When you update a scheduled request, the results for all future runs of the validation will be different than the results of previous runs of the validation.

To modify a scheduled validation:

1. Open the large Validation Request card.
2. Select the validation from the **Validation** dropdown list.
3. Edit the schedule or validation types.
4. Click **Update**.

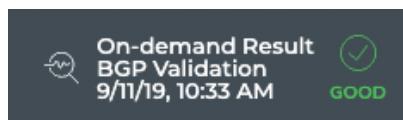
The validation can now be selected from the Validation listing (on the small, medium or large size card) and run immediately using **Run Now**, or you can wait for it to run the first time according to the schedule you specified. Refer to [View Scheduled Validation Results](#).

## View On-demand Validation Results

The On-demand Validation Result card workflow enables you to view the results of on-demand validation requests. When a request has started processing, the associated medium Validation Result card is displayed on your workbench. When multiple network protocols or services are included in a validation, a validation result card is opened for each protocol and service.

### On-Demand Validation Result Card Workflow

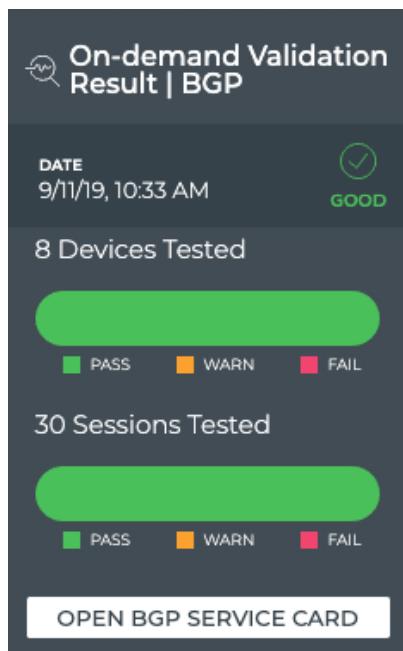
The small Validation Result card displays:



Item	Description
	Indicates an on-demand validation result
Title	On-demand Result <Network Protocol or Service Name> Validation
Timestamp	Date and time the validation was completed

Item	Description
 	<p>Status of the validation job, where:</p> <ul style="list-style-type: none"> <li>• <b>Good:</b> Job ran successfully. One or more warnings may have occurred during the run.</li> <li>• <b>Failed:</b> Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.</li> </ul>

The medium Validation Result card displays:



Item	Description
	Indicates an on-demand validation result
Title	On-demand Validation Result   <Network Protocol or Service Name>

Item	Description
Timestamp	Date and time the validation was completed
	Status of the validation job, where: <ul style="list-style-type: none"><li><b>Good:</b> Job ran successfully.</li><li><b>Warning:</b> Job encountered issues, but it did complete its run.</li><li><b>Failed:</b> Job encountered errors which prevented the job from completing.</li></ul>
Devices Tested	Chart with the total number of devices included in the validation and the distribution of the results. <ul style="list-style-type: none"><li><b>Pass:</b> Number of devices tested that had successful results</li><li><b>Warn:</b> Number of devices tested that had successful results, but also had at least one warning event</li><li><b>Fail:</b> Number of devices tested that had one or more protocol or service failures</li></ul> Hover over chart to view the number of devices and the percentage of all tested devices for each result category.

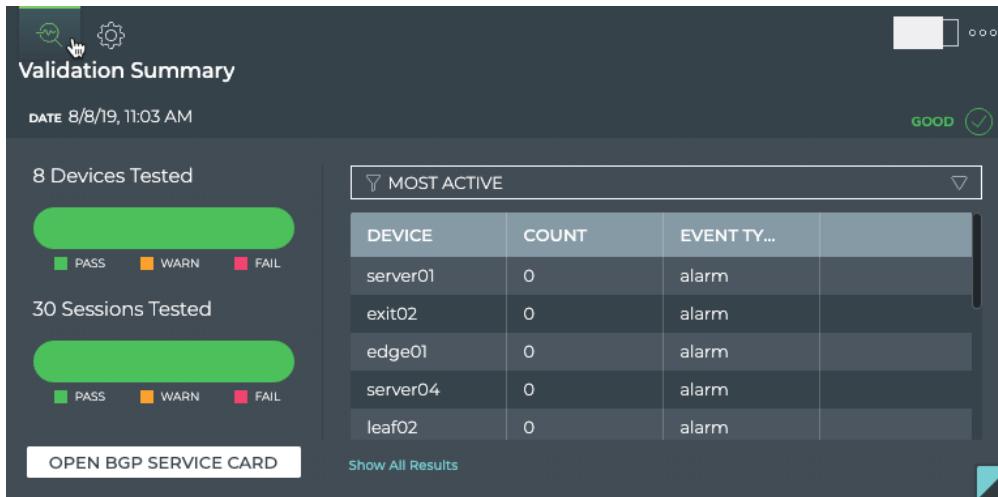
Item	Description
Sessions Tested	<p>For BGP, chart with total number of BGP sessions included in the validation and the distribution of the overall results.</p> <p>For EVPN, chart with total number of BGP sessions included in the validation and the distribution of the overall results.</p> <p>For Interfaces, chart with total number of ports included in the validation and the distribution of the overall results.</p> <p>In each of these charts:</p> <ul style="list-style-type: none"> <li>• <b>Pass:</b> Number of sessions or ports tested that had successful results</li> <li>• <b>Warn:</b> Number of sessions or ports tested that had successful results, but also had at least one warning event</li> <li>• <b>Fail:</b> Number of sessions or ports tested that had one or more failure events</li> </ul> <p>Hover over chart to view the number of devices, sessions, or ports and the percentage of all tested devices, sessions, or ports for each result category.</p> <p>This chart does not apply to other Network Protocols and Services, and thus is not displayed for those cards.</p>
Open <Network Protocol or Service Name> Service Card	Click to open the corresponding medium Network Services card, where available. Refer to <a href="#">Monitor Network Performance</a> for details about these cards and workflows.

The large Validation Result card contains two tabs.

The *Summary* tab displays:

## Validate Network Protocol and Service Operations

## View On-demand Validation Results



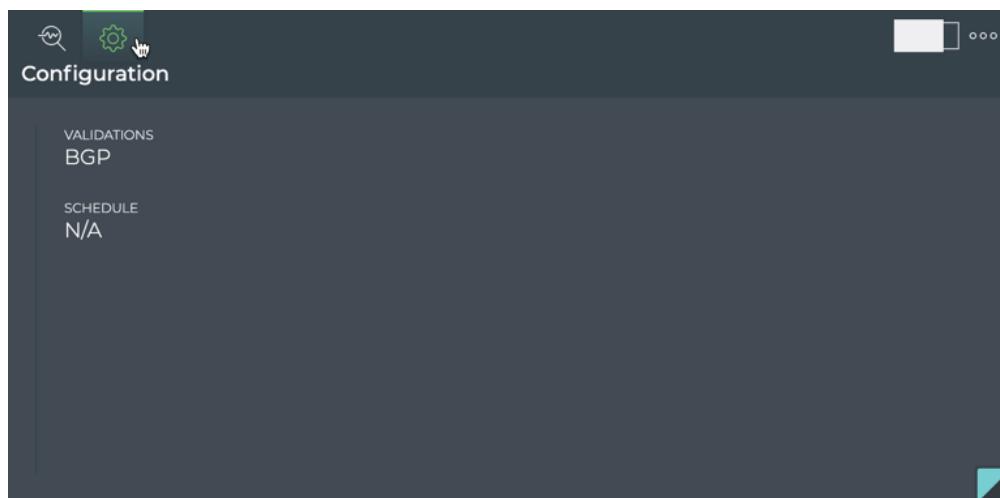
Item	Description
	Indicates an on-demand validation result
Title	On-demand Validation Result   Summary   <Network Protocol or Service Name>
Date	Day and time when the validation completed
  	Status of the validation job, where: <ul style="list-style-type: none"><li><b>Good:</b> Job ran successfully.</li><li><b>Warning:</b> Job encountered issues, but it did complete its run.</li><li><b>Failed:</b> Job encountered errors which prevented the job from completing.</li></ul>

Item	Description
Devices Tested	<p>Chart with the total number of devices included in the validation and the distribution of the results.</p> <ul style="list-style-type: none"><li>• <b>Pass:</b> Number of devices tested that had successful results</li><li>• <b>Warn:</b> Number of devices tested that had successful results, but also had at least one warning event</li><li>• <b>Fail:</b> Number of devices tested that had one or more protocol or service failures</li></ul> <p>Hover over chart to view the number of devices and the percentage of all tested devices for each result category.</p>

Item	Description
<p>Sessions Tested</p>	<p>For BGP, chart with total number of BGP sessions included in the validation and the distribution of the overall results.</p> <p>For EVPN, chart with total number of BGP sessions included in the validation and the distribution of the overall results.</p> <p>For Interfaces, chart with total number of ports included in the validation and the distribution of the overall results.</p> <p>For OSPF, chart with total number of OSPF sessions included in the validation and the distribution of the overall results.</p> <p>In each of these charts:</p> <ul style="list-style-type: none"> <li>• <b>Pass:</b> Number of sessions or ports tested that had successful results</li> <li>• <b>Warn:</b> Number of sessions or ports tested that had successful results, but also had at least one warning event</li> <li>• <b>Fail:</b> Number of sessions or ports tested that had one or more failure events</li> </ul> <p>Hover over chart to view the number of devices, sessions, or ports and the percentage of all tested devices, sessions, or ports for each result category.</p> <p>This chart does not apply to other Network Protocols and Services, and thus is not displayed for those cards.</p>
<p>Open &lt;Network Protocol or Service Name&gt; Service Card</p>	<p>Click to open the corresponding medium Network Services card, when available. Refer to <a href="#">Monitor Network Performance</a> for details about these cards and workflows.</p>

Item	Description
Table/ Filter options	<p>When the <b>Most Active</b> filter option is selected, the table displays switches and hosts running the given service or protocol in decreasing order of alarm counts—devices with the largest number of warnings and failures are listed first.</p> <p>When the <b>Most Recent</b> filter option is selected, the table displays switches and hosts running the given service or protocol sorted by <b>timestamp</b>, with the device with the most recent warning or failure listed first. The table provides the following additional information:</p> <ul style="list-style-type: none"><li>• <b>Hostname:</b> User-defined name for switch or host</li><li>• <b>Message Type:</b> Network protocol or service which triggered the event</li><li>• <b>Message:</b> Short description of the event</li><li>• <b>Severity:</b> Indication of importance of event; values in decreasing severity include critical, warning, error, info, debug</li></ul>
Show All Results	Click to open the full screen card with all on-demand validation results sorted by timestamp.

The *Configuration* tab displays:



Item	Description
	Indicates an on-demand validation request configuration
Title	On-demand Validation Result   Configuration   <Network Protocol or Service Name>
Validations	List of network protocols or services included in the request that produced these results
Schedule	Not relevant to on-demand validation results. Value is always N/A.

The full screen Validation Result card provides a tab for all on-demand validation results.

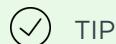
JOB ID	TIMESTAMP	TYPE	CHECKED...	FAILED SE...	FAILED N...	TOTAL SE...
667227e4-34...	8/8/19 11:03 A...	bgp	8	0	0	30

Item	Description
Title	Validation Results   On-demand
	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

Item	Description
On-demand Validation Result   <network protocol or service>	<p>Displays all unscheduled validation results. By default, the results list is sorted by <b>Timestamp</b>. This tab provides the following additional data about each result:</p> <ul style="list-style-type: none"><li>• <b>Job ID:</b> Internal identifier of the validation job that produced the given results</li><li>• <b>Timestamp:</b> Date and time the validation completed</li><li>• <b>Type:</b> Network protocol or service type</li><li>• <b>Total Node Count:</b> Total number of nodes running the given network protocol or service</li><li>• <b>Checked Node Count:</b> Number of nodes on which the validation ran</li><li>• <b>Failed Node Count:</b> Number of checked nodes that had protocol or service failures</li><li>• <b>Rotten Node Count:</b> Number of nodes that could not be reached during the validation</li><li>• <b>Unknown Node Count:</b> Applies only to the Interfaces service. Number of nodes with unknown port states.</li><li>• <b>Failed Adjacent Count:</b> Number of adjacent nodes that had protocol or service failures</li><li>• <b>Total Session Count:</b> Total number of sessions running for the given network protocol or service</li><li>• <b>Failed Session Count:</b> Number of sessions that had session failures</li></ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View On-demand Validation Results

Once an on-demand validation request has completed, the results are available in the corresponding Validation Result card.



TIP

It may take a few minutes for all results to be presented if the load on the NetQ Platform is heavy at the time of the run.

To view the results:

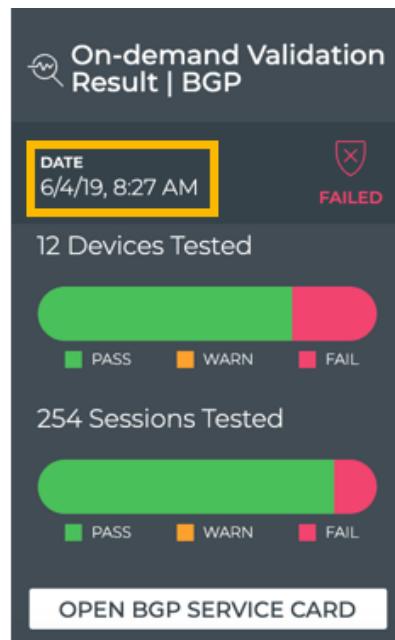
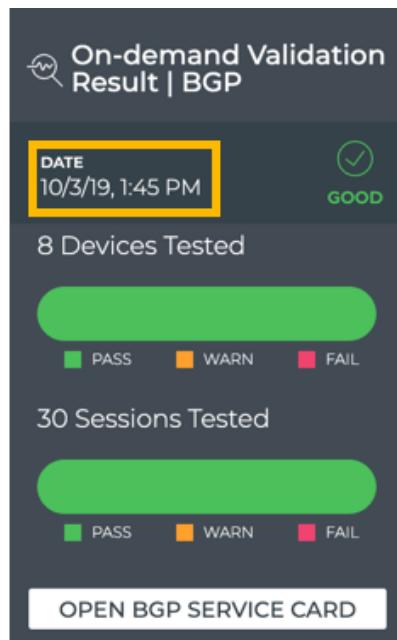
1. Locate the medium on-demand Validation Result card on your workbench for the protocol or service that was run.

You can identify it by the on-demand result icon,



, protocol or service name, and the date and time that it was run.

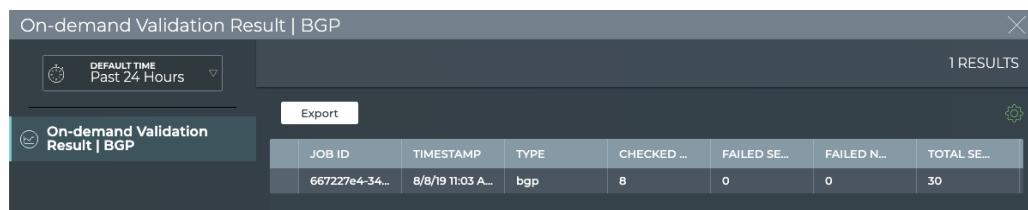
**Note:** You may have more than one card open for a given protocol or service, so be sure to use the date and time on the card to ensure you are viewing the correct card.



2. Note the total number and distribution of results for the tested devices and sessions (when appropriate). Are there many failures?
3. Hover over the charts to view the total number of warnings or failures and what percentage of the total results that represents for both devices and sessions.
4. Switch to the large on-demand Validation Result card.



5. If there are a large number of device warnings or failures, view the devices with the most issues in the table on the right. By default, this table displays the **Most Active** devices.
6. To view the most recent issues, select **Most Recent** from the filter above the table.
7. If there are a large number of devices or sessions with warnings or failures, the protocol or service may be experiencing issues. View the health of the protocol or service as a whole by clicking **Open <network service> Card** when available.
8. To view all data available for all on-demand validation results for a given protocol, switch to the full screen card.



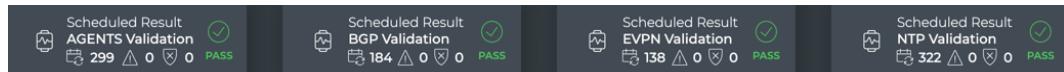
You may find that comparing various results gives you a clue as to why certain devices are experiencing more warnings or failures. For example, more failures occurred between certain times or on a particular device.

## View Scheduled Validation Results

The Scheduled Validation Result card workflow enables you to view the results of scheduled validation requests. When a request has completed processing, you can access the Validation Result card from the full screen Validation Request card. Each protocol and service has its own validation result card, but the content is similar on each.

### Scheduled Validation Result Card Workflow Summary

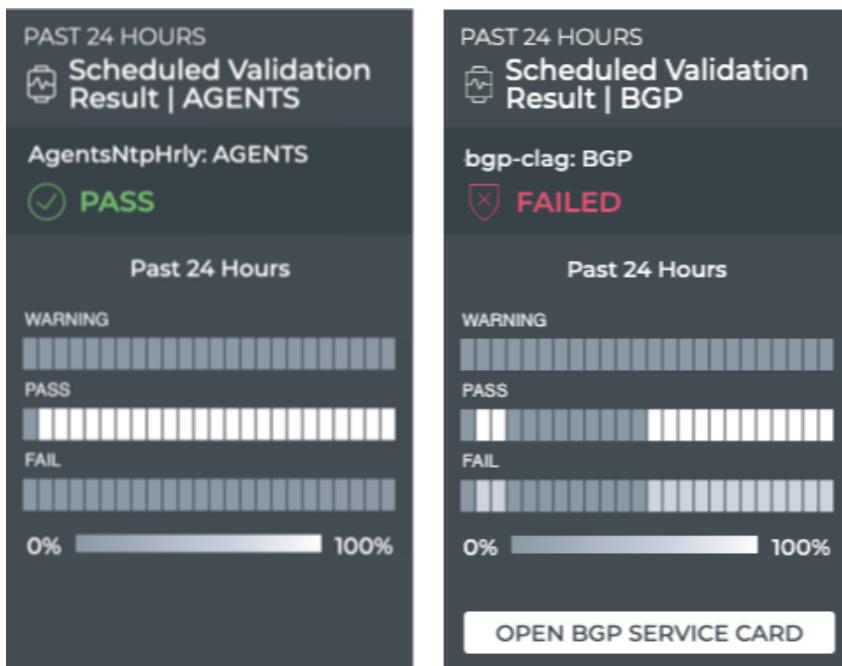
The small Validation Result card displays:



Item	Description
	Indicates a scheduled validation result
Title	Scheduled Result <Network Protocol or Service Name> Validation
Results	<p>Summary of validation results:</p> <ul style="list-style-type: none"> <li> • Number of validation runs completed in the designated time period</li> <li> • Number of runs with warnings</li> <li> • Number of runs with errors</li> </ul>

Item	Description
 	Status of the validation job, where: <ul style="list-style-type: none"> <li>• <b>Pass:</b> Job ran successfully. One or more warnings may have occurred during the run.</li> <li>• <b>Failed:</b> Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.</li> </ul>

The medium Validation Result card displays:

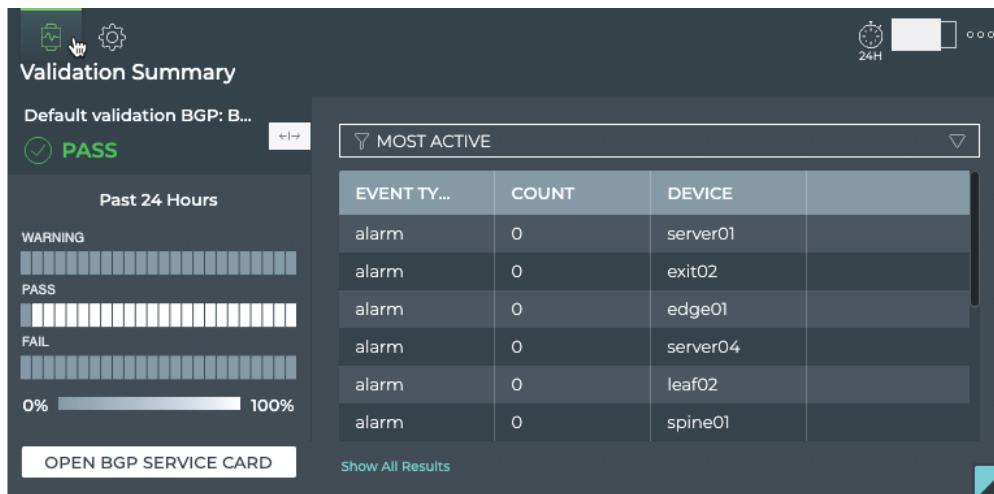


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates a scheduled validation result

Item	Description
Title	Scheduled Validation Result   <Network Protocol or Service Name>
Summary	<p>Summary of validation results:</p> <ul style="list-style-type: none"> <li>• Name of scheduled validation</li> <li>• Status of the validation job, where:           <ul style="list-style-type: none"> <li>○ <b>Pass:</b> Job ran successfully. One or more warnings may have occurred during the run.</li> <li>☒ <b>Failed:</b> Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.</li> </ul> </li> </ul>
Chart	<p>Validation results, where:</p> <ul style="list-style-type: none"> <li>• <b>Time period:</b> Range of time in which the data on the heat map was collected</li> <li>• <b>Heat map:</b> A time segmented view of the results. For each time segment, the color represents the percentage of warning, passing, and failed results. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> for details on how to interpret the results.</li> </ul>
Open <Network Protocol or Service Name> Service Card	Click to open the corresponding medium Network Services card, when available. Refer to <a href="#">Monitor Network Performance</a> for details about these cards and workflows.

The large Validation Result card contains two tabs.

The *Summary* tab displays:

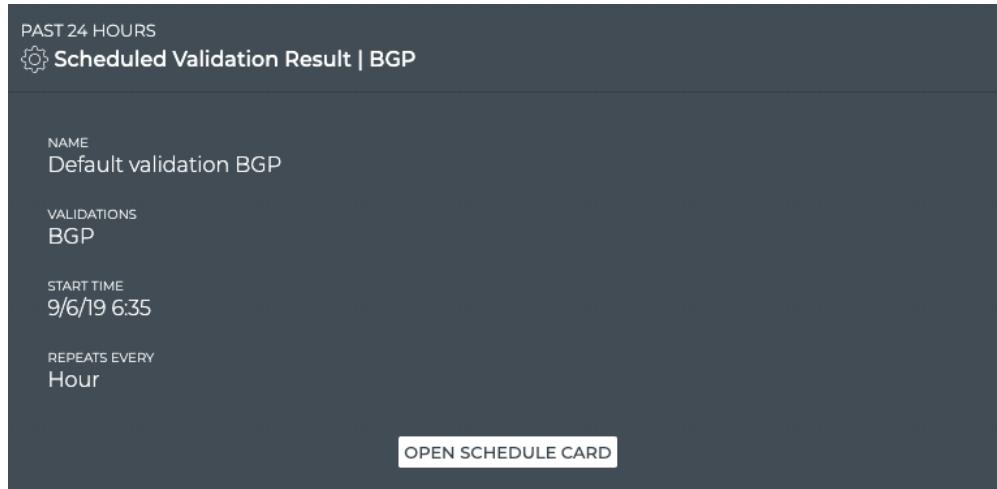


Item	Description
	Indicates a scheduled validation result
Title	Validation Summary (Scheduled Validation Result   <Network Protocol or Service Name>)
Summary	<p>Summary of validation results:</p> <ul style="list-style-type: none"> <li>• Name of scheduled validation</li> <li>• Status of the validation job, where:           <ul style="list-style-type: none"> <li> <b>Pass:</b> Job ran successfully. One or more warnings may have occurred during the run.</li> <li> <b>Failed:</b> Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.</li> </ul> </li> <li>• <b>Expand/Collapse:</b> Expand the heat map to full width of card, collapse the heat map to the left</li> </ul>

Item	Description
Chart	<p>Validation results, where:</p> <ul style="list-style-type: none"> <li>• <b>Time period:</b> Range of time in which the data on the heat map was collected</li> <li>• <b>Heat map:</b> A time segmented view of the results. For each time segment, the color represents the percentage of warning, passing, and failed results. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> for details on how to interpret the results.</li> </ul>
Open <Network Protocol or Service Name> Service Card	<p>Click to open the corresponding medium Network Services card, when available. Refer to <a href="#">Monitor Network Performance</a> for details about these cards and workflows.</p>
Table/Filter options	<p>When the <b>Most Active</b> filter option is selected, the table displays switches and hosts running the given service or protocol in decreasing order of alarm counts—devices with the largest number of warnings and failures are listed first.</p> <p>When the <b>Most Recent</b> filter option is selected, the table displays switches and hosts running the given service or protocol sorted by <b>timestamp</b>, with the device with the most recent warning or failure listed first. The table provides the following additional information:</p> <ul style="list-style-type: none"> <li>• <b>Hostname:</b> User-defined name for switch or host</li> <li>• <b>Message Type:</b> Network protocol or service which triggered the event</li> <li>• <b>Message:</b> Short description of the event</li> <li>• <b>Severity:</b> Indication of importance of event; values in decreasing severity include critical, warning, error, info, debug</li> </ul>

Item	Description
Show All Results	Click to open the full screen card with all scheduled validation results sorted by timestamp.

The *Configuration* tab displays:



Item	Description
	Indicates a scheduled validation configuration
Title	Configuration (Scheduled Validation Result   <Network Protocol or Service Name>)
Name	User-defined name for this scheduled validation
Validations	List of validations included in the validation request that created this result
Schedule	User-defined schedule for the validation request that created this result

Item	Description
Open Schedule Card	Opens the large Validation Request card for editing this configuration

The full screen Validation Result card provides tabs for all scheduled validation results for the service.

The screenshot shows a full-screen card titled "Scheduled Validation Result | BGP". At the top left is a clock icon with a dropdown menu labeled "DEFAULT TIME Past 24 Hours". On the right side, it says "97 RESULTS". Below the title, there's a sub-header "Scheduled Validation Result | BGP". In the center is a table with the following columns: JOB ID, TIMESTAMP, TYPE, CHECKED ..., FAILED SE..., FAILED N..., and TOTAL SE... . The table contains seven rows of data, each with a unique job ID, timestamp, type (all BGP), checked count (all 8), failed service count (all 0), failed node count (all 0), and total service count (all 30).

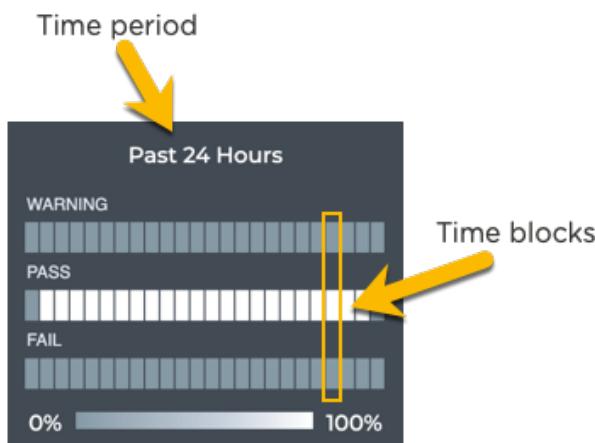
JOB ID	TIMESTAMP	TYPE	CHECKED ...	FAILED SE...	FAILED N...	TOTAL SE...
d10438db-37...	8/8/19 11:14 A...	bgp	8	0	0	30
8c9fa185-9a...	8/8/19 11:07 ...	bgp	8	0	0	30
6a0e1f2f-88c...	8/8/19 10:58 ...	bgp	8	0	0	30
06ff3316-7e4...	8/8/19 10:50 ...	bgp	8	0	0	30
7ace78c4-a6...	8/8/19 10:25 ...	bgp	8	0	0	30
d10438db-37...	8/8/19 10:14 ...	bgp	8	0	0	30

Item	Description
Title	Scheduled Validation Results   <Network Protocol or Service>
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

Item	Description
Scheduled Validation Result   <network protocol or service>	<p>Displays all unscheduled validation results. By default, the results list is sorted by timestamp. This tab provides the following additional data about each result:</p> <ul style="list-style-type: none"> <li>• <b>Job ID:</b> Internal identifier of the validation job that produced the given results</li> <li>• <b>Timestamp:</b> Date and time the validation completed</li> <li>• <b>Type:</b> Protocol or Service Name</li> <li>• <b>Total Node Count:</b> Total number of nodes running the given network protocol or service</li> <li>• <b>Checked Node Count:</b> Number of nodes on which the validation ran</li> <li>• <b>Failed Node Count:</b> Number of checked nodes that had protocol or service failures</li> <li>• <b>Rotten Node Count:</b> Number of nodes that could not be reached during the validation</li> <li>• <b>Unknown Node Count:</b> Applies only to the Interfaces service. Number of nodes with unknown port states.</li> <li>• <b>Failed Adjacent Count:</b> Number of adjacent nodes that had protocol or service failures</li> <li>• <b>Total Session Count:</b> Total number of sessions running for the given network protocol or service</li> <li>• <b>Failed Session Count:</b> Number of sessions that had session failures</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

## Granularity of Data Shown Based on Time Period

On the medium and large Validation Result cards, the status of the runs is represented in heat maps stacked vertically; one for passing runs, one for runs with warnings, and one for runs with failures. Depending on the time period of data on the card, the number of smaller time blocks used to indicate the status varies. A vertical stack of time blocks, one from each map, includes the results from all checks during that time. The results are shown by how saturated the color is for each block. If all validations during that time period pass, then the middle block is 100% saturated (white) and the warning and failure blocks are zero % saturated (gray). As warnings and errors increase in saturation, the passing block is proportionally reduced in saturation. An example heat map for a time period of 24 hours is shown here with the most common time periods in the table showing the resulting time blocks and regions.



Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day

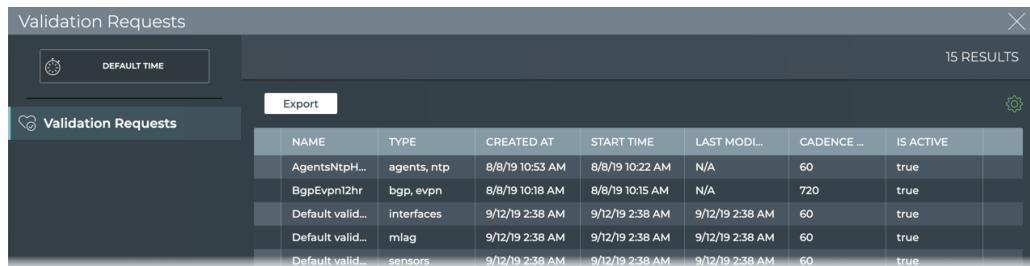
Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
1 quarter	7,000	13	1 week

### View Scheduled Validation Results

Once a scheduled validation request has completed, the results are available in the corresponding Validation Result card.

To view the results:

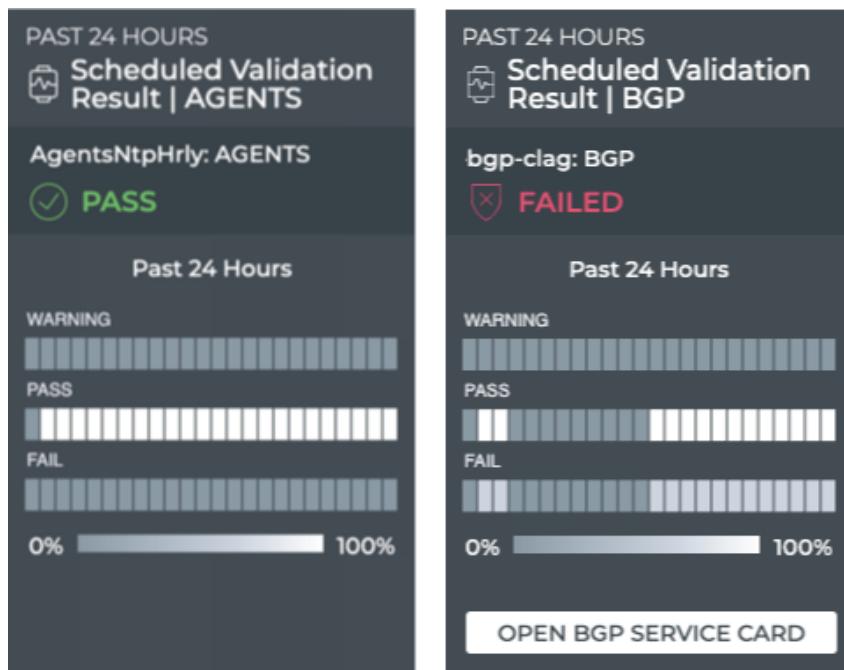
1. Open the full size Validation Request card to view all scheduled validations.



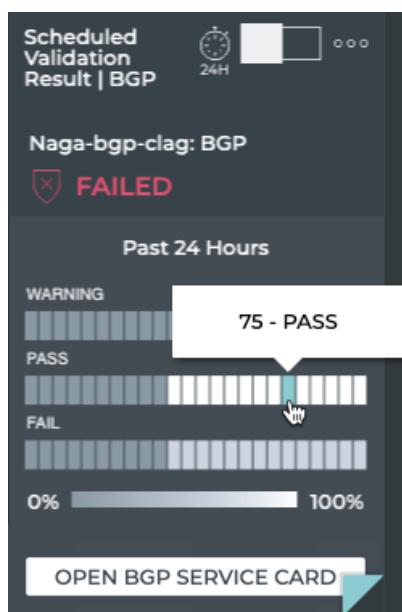
The screenshot shows a card titled "Validation Requests". At the top left is a clock icon and a "DEFAULT TIME" button. To the right is a "15 RESULTS" indicator. Below the header is a table with the following columns: NAME, TYPE, CREATED AT, START TIME, LAST MODI..., CADENCE ..., and IS ACTIVE. The table contains five rows of data:

NAME	TYPE	CREATED AT	START TIME	LAST MODI...	CADENCE ...	IS ACTIVE
AgentsNtpH...	agents, ntp	8/8/19 10:53 AM	8/8/19 10:22 AM	N/A	60	true
BgpEvpn12hr	bgp, evpn	8/8/19 10:18 AM	8/8/19 10:15 AM	N/A	720	true
Default valid...	interfaces	9/12/19 2:38 AM	9/12/19 2:38 AM	9/12/19 2:38 AM	60	true
Default valid...	mlag	9/12/19 2:38 AM	9/12/19 2:38 AM	9/12/19 2:38 AM	60	true
Default valid...	sensors	9/12/19 2:38 AM	9/12/19 2:38 AM	9/12/19 2:38 AM	60	true

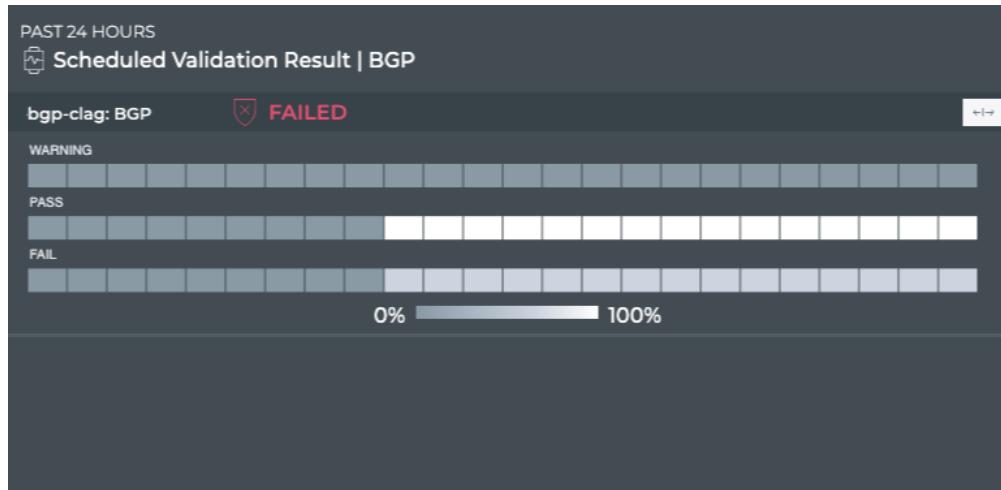
2. Select the validation results you want to view by clicking in the first column of the result and clicking the check box.
3. On the Edit Menu that appears at the bottom of the window, click  (Open Cards). This opens the medium Scheduled Validation Results card(s) for the selected items.



4. Note the distribution of results. Are there many failures? Are they concentrated together in time? Has the protocol or service recovered after the failures?
5. Hover over the heat maps to view the status numbers and what percentage of the total results that represents for a given region. The tooltip also shows the number of devices included in the validation and the number with warnings and/or failures. This is useful when you see the failures occurring on a small set of devices, as it might point to an issue with the devices rather than the network service.

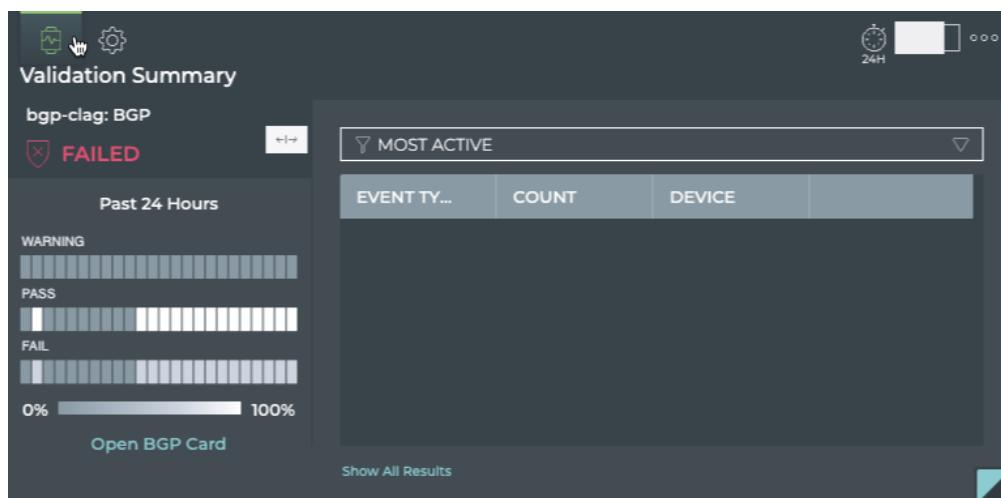


6. Optionally, click **Open <network service> Card** link to open the medium individual Network Services card. Your current card is not closed.
7. Switch to the large Scheduled Validation card.
8. Click  
↔ to expand the chart.



9. Collapse the heat map by clicking  
↔

.



10. If there are a large number of warnings or failures, view the devices with the most issues by clicking **Most Active** in the filter above the table. This might help narrow the failures down to a particular device or small set of devices that you can investigate further.

11. Select the **Most Recent** filter above the table to see the events that have occurred in the near past at the top of the list.
12. Optionally, view the health of the protocol or service as a whole by clicking **Open <network service> Card** (when available).
13. You can view the configuration of the request that produced the results shown on this card workflow, by hovering over the card and clicking  . If you want to change the configuration, click **Edit Config** to open the large Validation Request card, pre-populated with the current configuration. Follow the instructions in [Modify an Existing Scheduled Validation Request](#) to make your changes.
14. To view all data available for all scheduled validation results for the given protocol or service, click **Show All Results** or switch to the full screen card.

Scheduled Validation Result | BGP

 DEFAULT TIME Past 24 Hours ▾

97 RESULTS

Export 

Scheduled Validation Result | BGP

JOB ID	TIMESTAMP	TYPE	CHECKED ...	FAILED SE...	FAILED N...	TOTAL SE...
d10438d8-37...	8/8/19 11:14 A...	bgp	8	0	0	30
8c9fa185-9a...	8/8/19 11:07 ...	bgp	8	0	0	30
6a0e1f2f-8c...	8/8/19 10:58 ...	bgp	8	0	0	30
06ff3316-7e4...	8/8/19 10:50 ...	bgp	8	0	0	30
7ace78c4-a6...	8/8/19 10:25 ...	bgp	8	0	0	30
d10438d8-37...	8/8/19 10:14 ...	bgp	8	0	0	30

15. Look for changes and patterns in the results. Scroll to the right. Are there more failed sessions or nodes during one or more validations?
16. Return to the full screen Validation Results card to view another Scheduled Validation Result.

# Monitor Network Inventory

With NetQ, a network administrator can monitor both the switch hardware and its operating system for misconfigurations or misbehaving services. The Devices Inventory card workflow provides a view into the switches and hosts installed in your network and their various hardware and software components. The workflow contains a small card with a count of each device type in your network, a medium card displaying the operating systems running on each set of devices, large cards with component information statistics, and full-screen cards displaying tables with attributes of all switches and all hosts in your network.

The Devices Inventory card workflow helps answer questions such as:

- What switches do I have in the network?
- What is the distribution of ASICs across my network?
- Do all switches have valid licenses?
- Are NetQ agents running on all of my switches?

For monitoring inventory and performance on a switch-by-switch basis, refer to the [Monitor Switches](#).

## Devices Inventory Card Workflow Summary

The small Devices Inventory card displays:



## Monitor Network Inventory

## Devices Inventory Card Workflow Summary

Item	Description
	Indicates data is for device inventory
	Total number of switches in inventory during the designated time period
	Total number of hosts in inventory during the designated time period
	Total number of chassis in inventory during the designated time period. Not monitored in this release.

The medium Devices Inventory card displays:



Item	Description
	Indicates data is for device inventory

## Monitor Network Inventory

## Devices Inventory Card Workflow Summary

Item	Description
Title	Inventory   Devices
	Total number of switches in inventory during the designated time period
	Total number of hosts in inventory during the designated time period

The large Devices Inventory card has one tab.

The *Switches* tab displays:



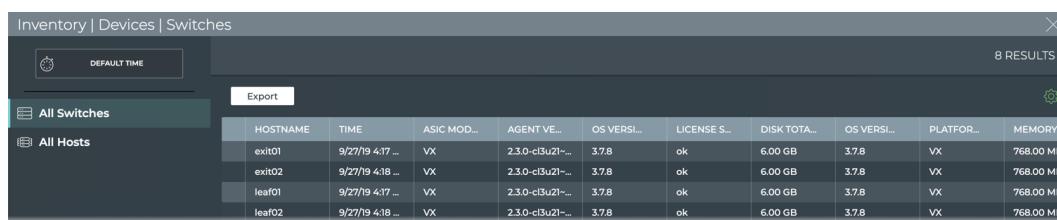
Item	Description
Time period	Always Now for inventory by default
	Indicates data is for device inventory

## Monitor Network Inventory

## Devices Inventory Card Workflow Summary

Item	Description
Title	Inventory   Devices
	Total number of switches in inventory during the designated time period
	Link to full screen listing of all switches
Component	Switch components monitored—ASIC, Operating System (OS), Cumulus Linux license, NetQ Agent version, and Platform
Distribution charts	Distribution of switch components across the network
Unique	Number of unique items of each component type. For example, for License, you might have CL 2.7.2 and CL 2.7.4, giving you a unique count of two.

The full screen Devices Inventory card provides tabs for all switches and all hosts.



HOSTNAME	TIME	ASIC MOD.	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	MEMORY
exit01	9/27/19 4:17 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
exit02	9/27/19 4:18 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
leaf01	9/27/19 4:17 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
leaf02	9/27/19 4:18 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi

Item	Description
Title	Inventory   Devices   Switches
	Closes full screen card and returns to workbench

## Monitor Network Inventory

## Devices Inventory Card Workflow Summary

Item	Description
Time period	Time period does not apply to the Inventory cards. This is always Default Time.
Results	Number of results found for the selected tab

All Switches and All Hosts tabs	<p>Displays all monitored switches and hosts in your network. By default, the device list is sorted by <b>hostname</b>. These tabs provide the following additional data about each device:</p> <ul style="list-style-type: none"><li>• <b>Agent</b><ul style="list-style-type: none"><li>◦ State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).</li><li>◦ Version: Software version number of the NetQ Agent on a given device. This should match the version number of the NetQ software loaded on your server or appliance; for example, 2.1.0.</li></ul></li><li>• <b>ASIC</b><ul style="list-style-type: none"><li>◦ Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.</li><li>◦ Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.</li><li>◦ Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.</li><li>◦ Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.</li><li>◦ Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.</li></ul></li><li>• <b>CPU</b><ul style="list-style-type: none"><li>◦ Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.</li><li>◦ Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.</li><li>◦ Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.</li><li>◦ Nos: Number of cores. Example values include 2, 4, and 8.</li></ul></li><li>• <b>Disk Total Size:</b> Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.</li><li>• <b>License State:</b> Indicator of validity. Values include ok and bad.</li><li>• <b>Memory Size:</b> Total amount of local RAM. Example values include 8192 MB and 2048 MB.</li><li>• <b>OS</b><ul style="list-style-type: none"><li>◦ Vendor: Operating System manufacturer. Values include Cumulus Networks, RedHat, Ubuntu, and CentOS.</li><li>◦ Version: Software version number of the OS. Example values</li></ul></li></ul>
---	---

## View the Number of Each Device Type in Your Network

You can view the number of switches and hosts deployed in your network. As you grow your network this can be useful for validating that devices have been added as scheduled.

To view the quantity of devices in your network, open the small Devices Inventory card.



### TIP

Chassis are not monitored in this release, so an N/A (not applicable) value is displayed for these devices, even if you have chassis in your network.

## View Which Operating Systems Are Running on Your Network Devices

You can view the distribution of operating systems running on your switches and hosts. This is useful for verifying which versions of the OS are deployed and for upgrade planning. It also provides a view into the relative dependence on a given OS in your network.

To view the OS distribution, open the medium Devices Inventory card if it is not already on your workbench.

## Monitor Network Inventory

## View Switch Components



## View Switch Components

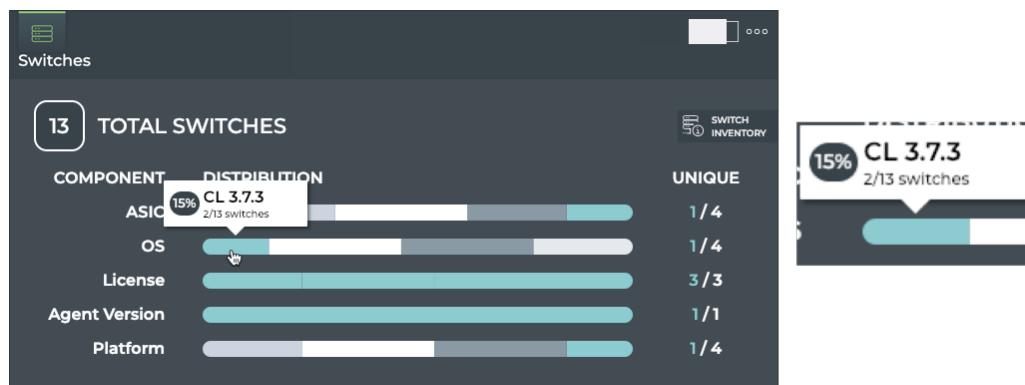
To view switch components, open the large Devices Inventory card. By default the Switches tab is shown displaying the total number of switches, ASIC vendor, OS versions, license status, NetQ Agent versions, and specific platforms deployed on all of your switches.



### Highlight a Selected Component Type

You can hover over any of the segments in a component distribution chart to highlight a specific type of the given component. When you *hover*, a tooltip appears displaying:

- the name or value of the component type, such as the version number or status
- the total number of switches with that type of component deployed compared to the total number of switches
- percentage of this type with respect to all component types.



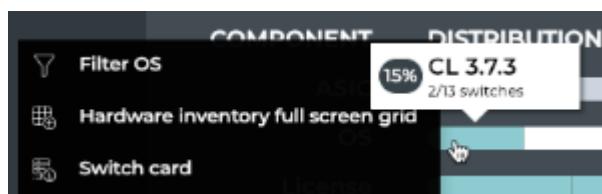
Additionally, sympathetic highlighting is used to show the related component types relevant to the highlighted segment and the number of unique component types associated with this type (shown in blue here).

### Focus on a Selected Component Type

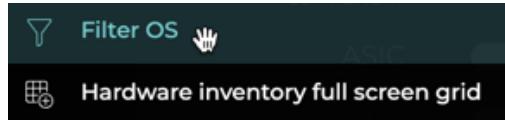
To dig deeper on a particular component type, you can filter the card data by that type. In this procedure, the result of filtering on the OS is shown.

To view component type data:

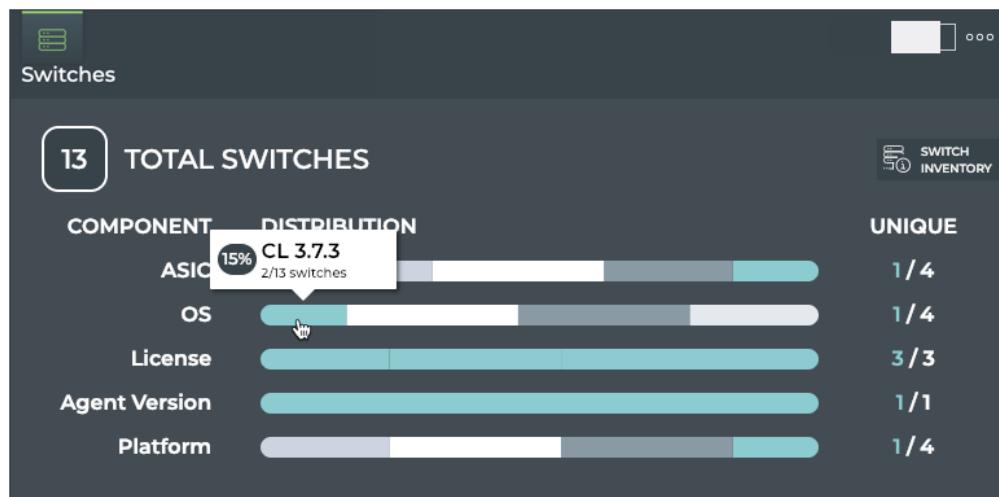
1. Click a segment of the component distribution charts.



2. Select the first option from the popup, *Filter <component name>*. The card data is filtered to show only the components associated with selected component type. A filter tag appears next to the total number of switches indicating the filter criteria.



3. Hover over the segments to view the related components.



4. To return to the full complement of components, click the in the filter tag.

#### Navigate to the Switch Inventory Workflow

While the Device Inventory cards provide a network-wide view, you may want to see more detail about your switch inventory. This can be found in the Switches Inventory card workflow. To open that workflow, click the **Switch Inventory** button at the top right of the Switches card.



## View All Switches

You can view all stored attributes for all switches in your network. To view all switch details, open the full screen Devices Inventory card and click the **All Switches** tab in the navigation panel.

The figure shows a table of network device attributes for 8 results. The columns include Hostname, Time, ASIC Model, Agent Version, OS Version, License Status, Disk Total, OS Version, Platform, and Memory. The data shows four distinct switch entries: exit01, exit02, leaf01, and leaf02, each with identical specifications.

	HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	MEMORY
1	exit01	9/27/19 4:17 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
2	exit02	9/27/19 4:18 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
3	leaf01	9/27/19 4:17 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi
4	leaf02	9/27/19 4:18 ...	VX	2.3.0-c13u2!...	3.7.8	ok	6.00 GB	3.7.8	VX	768.00 Mi

To return to your workbench, click in the top right corner of the card.

## View All Hosts

You can view all stored attributes for all hosts in your network. To view all hosts details, open the full screen Devices Inventory card and click the **All Hosts** tab in the navigation panel.

The screenshot shows a table titled "Inventory | Devices | Switches" with 5 results. The table has columns for HOSTNAME, TIME, ASIC MOD., AGENT VERSI..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., PLATFOR..., and MEMORY. The rows list five devices: edge01, server01, server02, server03, and server04. The "All Hosts" filter is selected in the sidebar.

HOSTNAME	TIME	ASIC MOD...	AGENT VERSI...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	MEMORY
edge01	9/27/19 4:16 ...	N/A	2.3.0-ub16.0...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	768.00 MB
server01	9/27/19 4:21 ...	N/A	2.3.0-ub16.0...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	512.00 MB
server02	9/27/19 4:21 ...	N/A	2.3.0-ub16.0...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	512.00 MB
server03	9/27/19 4:21 ...	N/A	2.3.0-ub16.0...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	512.00 MB
server04	9/27/19 4:21 ...	N/A	2.3.0-ub16.0...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	512.00 MB

To return to your workbench, click



in the top right corner of the card.

# Monitor Events

Two event workflows, the Alarms card workflow and the Info card workflow, provide a view into the events occurring in the network. The Alarms card workflow tracks critical severity events, whereas the Info card workflow tracks all warning, info, and debug severity events.

To focus on events from a single device perspective, refer to [Monitor Switches](#).

# Monitor Alarms

You can easily monitor critical events occurring across your network using the Alarms card. You can determine the number of events for the various system, interface, and network protocols and services components in the network. The content of the cards in the workflow is described first, and then followed by common tasks you would perform using this card workflow.

## Alarms Card Workflow Summary

The small Alarms card displays:



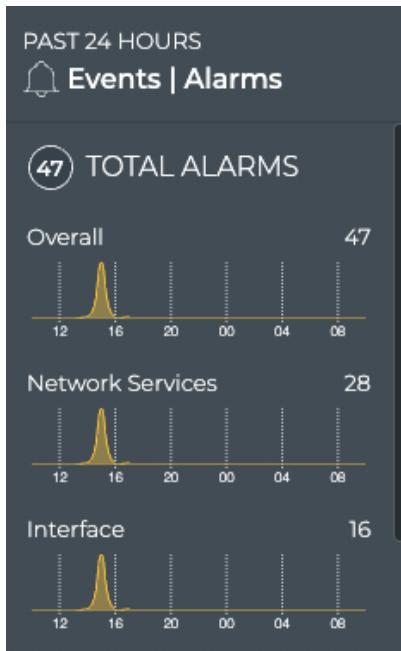
Item	Description
	Indicates data is for all critical severity events in the network

Item	Description
Alarm trend	<p>Trend of alarm count, represented by an arrow:</p> <ul style="list-style-type: none"> <li>• <b>Pointing upward and bright pink:</b> alarm count is higher than the last two time periods, an increasing trend</li> <li>• <b>Pointing downward and green:</b> alarm count is lower than the last two time periods, a decreasing trend</li> <li>• <b>No arrow:</b> alarm count is unchanged over the last two time periods, trend is steady</li> </ul>
Alarm score	Current count of alarms during the designated time period
Alarm rating	<p>Count of alarms relative to the average count of alarms during the designated time period:</p> <ul style="list-style-type: none"> <li>• <b>Low:</b> Count of alarms is below the average count; a nominal count</li> <li>• <b>Med:</b> Count of alarms is in range of the average count; some room for improvement</li> <li>• <b>High:</b> Count of alarms is above the average count; user intervention recommended</li> </ul> 
Chart	Distribution alarms received during the designated time period and a total count of all alarms present in the system

The medium Alarms card displays:

## Monitor Events

## Monitor Alarms



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all critical events in the network
Count	Total number of alarms received during the designated time period
Alarm trend	Trend of alarm count, represented by an arrow: <ul style="list-style-type: none"><li>• <b>Pointing upward and bright pink:</b> alarm count is higher than the last two time periods, an increasing trend</li><li>• <b>Pointing downward and green:</b> alarm count is lower than the last two time periods, a decreasing trend</li><li>• <b>No arrow:</b> alarm count is unchanged over the last two time periods, trend is steady</li></ul>
Alarm score	Current count of alarms received from each category (overall, system, interface, and network services) during the designated time period

## Monitor Events

## Monitor Alarms

Item	Description
Chart	Distribution of all alarms received from each category during the designated time period

The large Alarms card has one tab.

The *Alarm Summary* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all system, trace and interface critical events in the network

Item	Description
Alarm Distribution	<p><b>Chart:</b> Distribution of all alarms received from each category (NetQ Agent, BTRFS Information, CL Support, Config Diff, CL License, Link, LLDP, MTU, Node, Package Versions, Port, Resource, Running Config Diff, Sensor, Services, and SSD Utilization) during the designated time period</p> <p><b>Count:</b> Total number of alarms received from each category during the designated time period</p>
Table	<p>Listing of items that match the filter selection for the selected alarm categories:</p> <ul style="list-style-type: none"> <li>• <b>Events by Most Recent:</b> Most recent event are listed at the top</li> <li>• <b>Devices by Event Count:</b> Devices with the most events are listed at the top</li> </ul>
Show All Events	Opens full screen Events   Alarms card with a listing of all events

The full screen Alarms card provides tabs for all events.

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
server02	Sync state changed from yes to no for server02	ntp	critical	8/6/19 4:03 PM
server01	Sync state changed from yes to no for server01	ntp	critical	8/6/19 4:03 PM
server03	Sync state changed from yes to no for server03	ntp	critical	8/6/19 4:03 PM
server04	Sync state changed from yes to no for server04	ntp	critical	8/6/19 4:03 PM
exit02	Service zebra status changed from active to inactive	services	critical	8/6/19 4:02 PM
exit02	Service bgpd status changed from active to inactive	services	critical	8/6/19 4:02 PM
leaf04	Service zebra status changed from active to inactive	services	critical	8/6/19 4:02 PM
leaf04	Service bgpd status changed from active to inactive	services	critical	8/6/19 4:02 PM

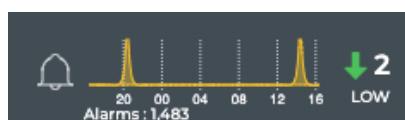
Item	Description
Title	Events   Alarms

Item	Description
×	Closes full screen card and returns to workbench
Default Time	Range of time in which the displayed data was collected
Results	Number of results found for the selected tab
All Events	<p>Displays all events (both alarms and info) received in the time period. By default, the requests list is sorted by the date and time that the event occurred (<b>Time</b>). This tab provides the following additional data about each request:</p> <ul style="list-style-type: none"> <li>• <b>Source:</b> Hostname of the given event</li> <li>• <b>Message:</b> Text describing the alarm or info event that occurred</li> <li>• <b>Type:</b> Name of network protocol and/or service that triggered the given event</li> <li>• <b>Severity:</b> Importance of the event—critical, warning, info, or debug</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
⚙️	Enables manipulation of table display; choose columns to display and reorder columns

### View Alarm Status Summary

A summary of the critical alarms in the network includes the number of alarms, a trend indicator, a performance indicator, and a distribution of those alarms.

To view the summary, open the small Alarms card.

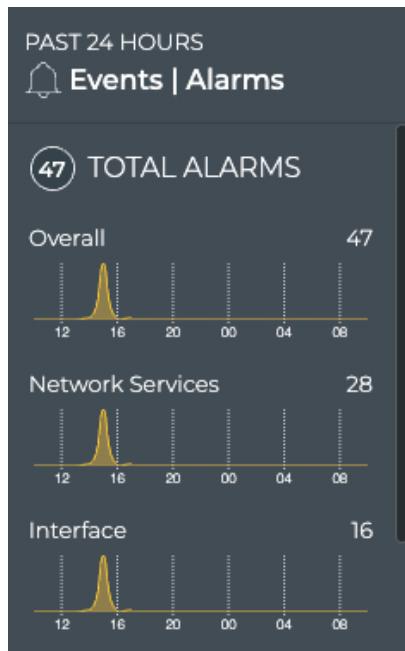


In this example, there are a small number of alarms (2), the number of alarms is decreasing (down arrow), and there are fewer alarms right now than the average number of alarms during this time period. This would indicate no further investigation is needed. Note that with such a small number of alarms, the rating may be a bit skewed.

### View the Distribution of Alarms

It is helpful to know where and when alarms are occurring in your network. The Alarms card workflow enables you to see the distribution of alarms based on its source—network services, interfaces, or other system services. You can also view the trend of alarms in each source category.

To view the alarm distribution, open the medium Alarms card. Scroll down to view all of the charts.



### Monitor System and Interface Alarm Details

The Alarms card workflow enables users to easily view and track critical severity system and interface alarms occurring anywhere in your network.

## Monitor Events

## Monitor Alarms

### VIEW ALL SYSTEM AND INTERFACE ALARMS

You can view the alarms associated with the system and interfaces using the Alarms card workflow. You can sort alarms based on their occurrence or view devices with the most network services alarms.

To view network services alarms, open the large Alarms card.



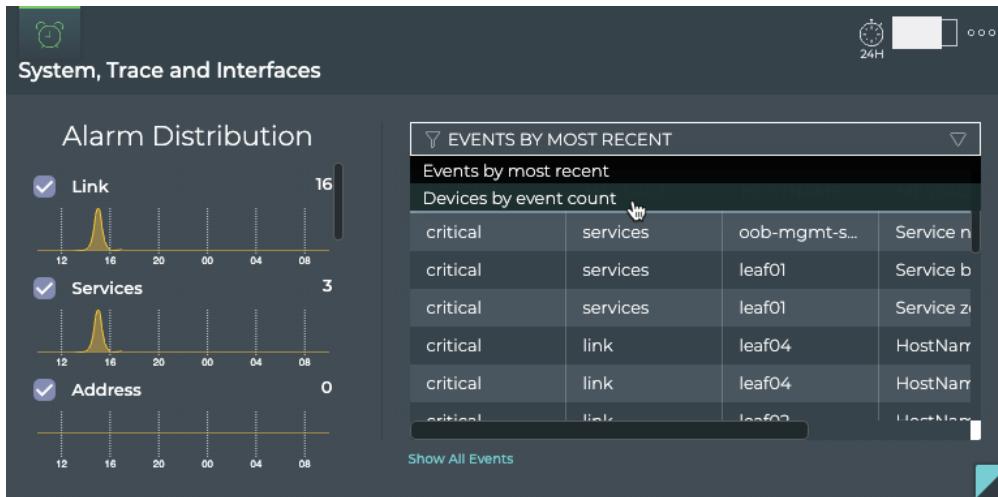
From this card, you can view the distribution of alarms for each of the categories over time. Scroll down to view any hidden charts. A list of the associated alarms is also displayed.

By default, the list of the most recent alarms for the systems and interfaces is displayed when viewing the large cards.

### VIEW DEVICES WITH THE MOST ALARMS

You can filter instead for the devices that have the most alarms.

To view devices with the most alarms, open the large Alarms card, and then select **Devices by event count** from the dropdown.



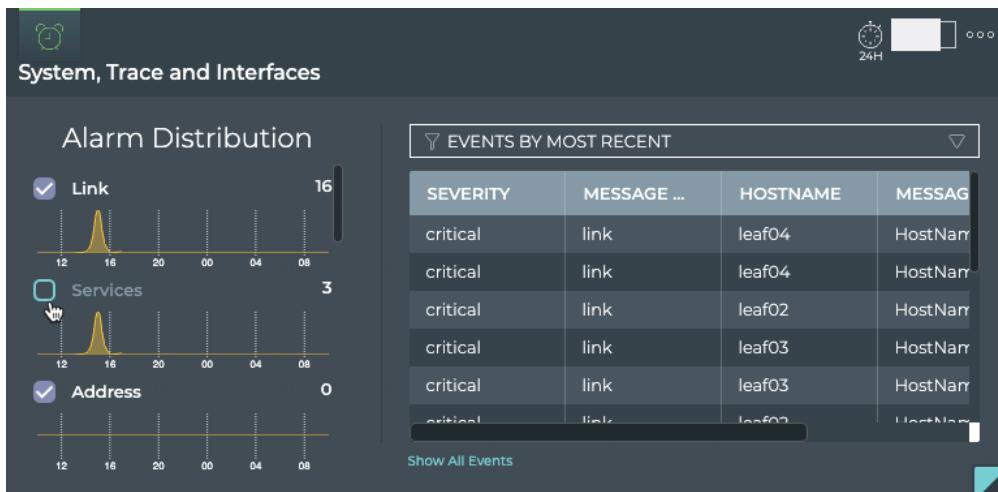
#### FILTER ALARMS BY SYSTEM OR INTERFACE

You can focus your view to include alarms for selected system or interface categories.

To filter for selected categories:

1. Click the checkbox to the left of one or more charts to remove that set of alarms from the table on the right.
2. Select the **Devices by event count** to view the devices with the most alarms for the selected categories.
3. Switch back to most recent events by selecting **Events by most recent**.
4. Click the checkbox again to return a category's data to the table.

In this example, we removed the Services from the event listing.



## COMPARE ALARMS WITH A PRIOR TIME

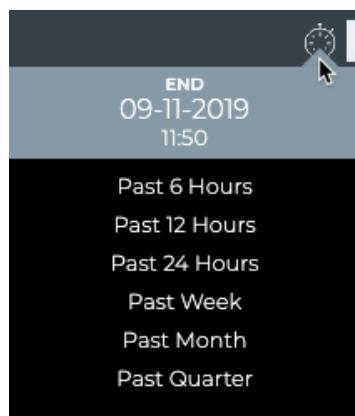
You can change the time period for the data to compare with a prior time. If the same devices are consistently indicating the most alarms, you might want to look more carefully at those devices using the Switches card workflow.

To compare two time periods:

1. Open a second Alarm Events card. Remember it goes to the bottom of the workbench.
2. Switch to the large size view.
3. Move the card to be next to the original Alarm Events card. Note that moving large cards can take a few extra seconds since they contain a large amount of data.
4. Hover over the card and click



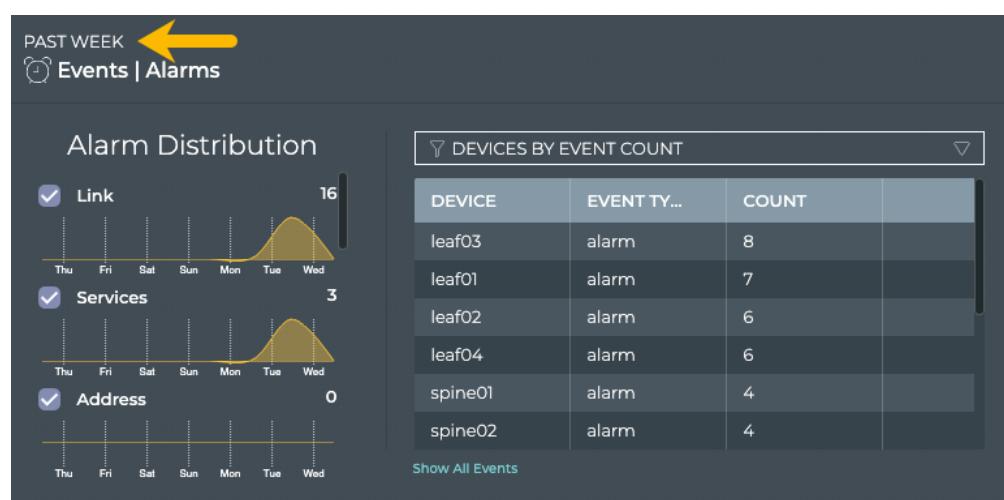
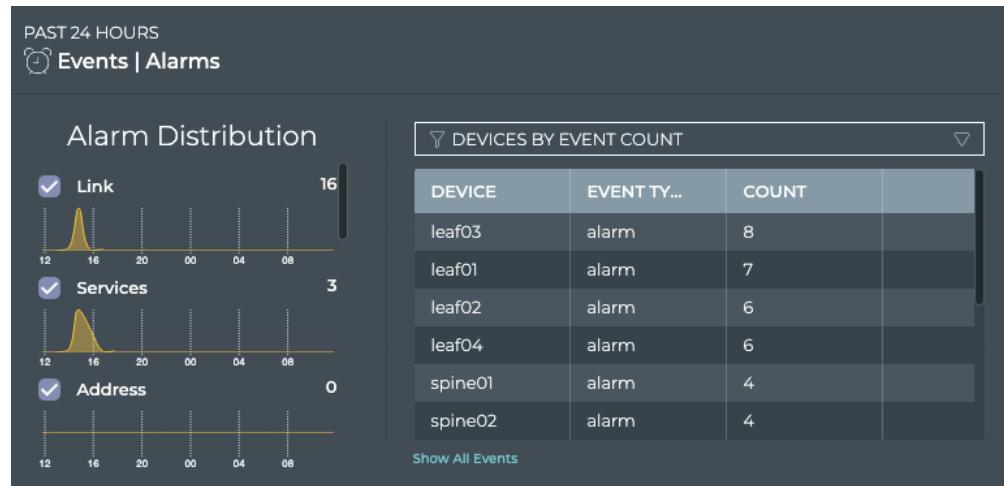
.



5. Select a different time period.

## Monitor Events

## Monitor Alarms



6. Compare the two cards with the **Devices by event count** filter applied.

In this example, both the total alarm count and the devices with the most alarms in each time period are unchanged. You could go back further in time to see if this changes or investigate the current status of the largest offenders.

### [View All Events](#)

You can view all events in the network either by clicking the **Show All Events** link under the table on the large Alarm Events card, or by opening the full screen Alarm Events card.

## Monitor Events

## Monitor Info Events



OR

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
server02	Sync state changed from yes to no for server02	ntp	critical	8/6/19 4:03 PM
server01	Sync state changed from yes to no for server01	ntp	critical	8/6/19 4:03 PM
server03	Sync state changed from yes to no for server03	ntp	critical	8/6/19 4:03 PM
server04	Sync state changed from yes to no for server04	ntp	critical	8/6/19 4:03 PM
exit02	Service zebra status changed from active to inactive	services	critical	8/6/19 4:02 PM
exit02	Service bgpd status changed from active to inactive	services	critical	8/6/19 4:02 PM
leaf04	Service zebra status changed from active to inactive	services	critical	8/6/19 4:02 PM
leaf04	Service bgpd status changed from active to inactive	services	critical	8/6/19 4:02 PM

To return to your workbench, click



in the top right corner of the card.

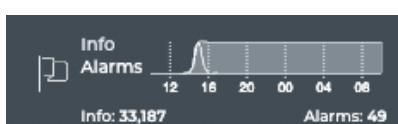
## Monitor Info Events

You can easily monitor warning, info, and debug severity events occurring across your network using the Info card. You can determine the number of events for the various system, interface, and network protocols and services components in the network. The content of the cards in the workflow is described first, and then followed by common tasks you would perform using this card workflow.

### Info Card Workflow Summary

The Info card workflow enables users to easily view and track informational alarms occurring anywhere in your network.

The small Info card displays:

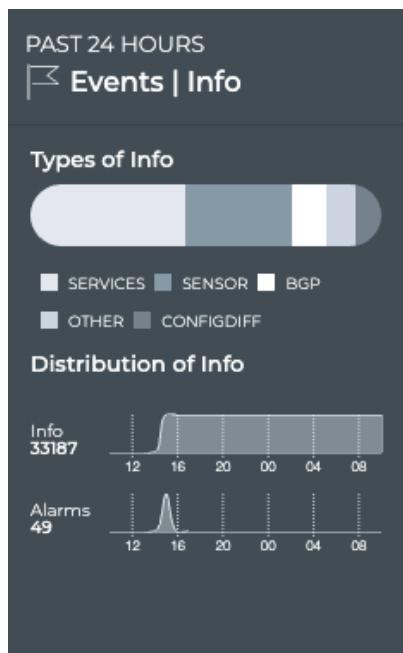


## Monitor Events

## Monitor Info Events

Item	Description
⊕	Indicates data is for all warning, info, and debug severity events in the network
Info count	Number of info events received during the designated time period
Alarm count	Number of alarm events received during the designated time period
Chart	Distribution of all info events and alarms received during the designated time period

The medium Info card displays:

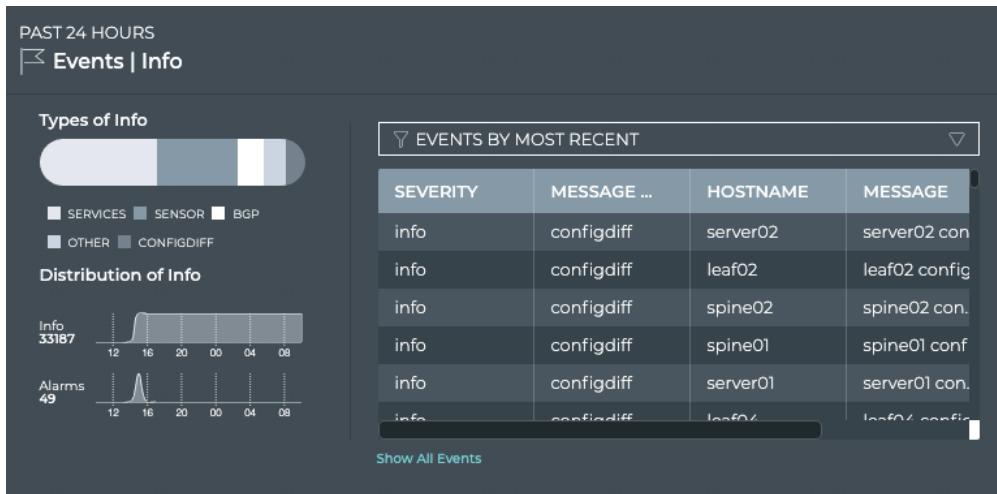


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all warning, info, and debug severity events in the network
Types of Info	Chart which displays the services that have triggered events during the designated time period. Hover over chart to view a count for each type.
Distribution of Info	<p>Info Status</p> <ul style="list-style-type: none"> <li><b>Count:</b> Number of info events received during the designated time period</li> <li><b>Chart:</b> Distribution of all info events received during the designated time period</li> </ul> <p>Alarms Status</p> <ul style="list-style-type: none"> <li><b>Count:</b> Number of alarm events received during the designated time period</li> <li><b>Chart:</b> Distribution of all alarm events received during the designated time period</li> </ul>

The large Info card displays:

## Monitor Events

## Monitor Info Events



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
Events	Indicates data is for all warning, info, and debug severity events in the network
Types of Info	Chart which displays the services that have triggered events during the designated time period. Hover over chart to view a count for each type.
Distribution of Info	<p>Info Status</p> <ul style="list-style-type: none"> <li><b>Count:</b> Current number of info events received during the designated time period</li> <li><b>Chart:</b> Distribution of all info events received during the designated time period</li> </ul> <p>Alarms Status</p> <ul style="list-style-type: none"> <li><b>Count:</b> Current number of alarm events received during the designated time period</li> <li><b>Chart:</b> Distribution of all alarm events received during the designated time period</li> </ul>

## Monitor Events

## Monitor Info Events

Item	Description
Table	<p>Listing of items that match the filter selection:</p> <ul style="list-style-type: none"> <li>• <b>Events by Most Recent:</b> Most recent event are listed at the top</li> <li>• <b>Devices by Event Count:</b> Devices with the most events are listed at the top</li> </ul>
Show All Events	Opens full screen Events   Info card with a listing of all events

The full screen Info card provides tabs for all events.

The screenshot shows a 'Events | Info' card with a title bar and a search/filter section. Below it is a table with columns: SOURCE, MESSAGE, TYPE, SEVERITY, and TIME. The table contains six rows of log entries from various devices (server02, leaf02, spine02, spine01, server01, leaf04) indicating configuration file creation.

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
server02	server02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
leaf02	leaf02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
spine02	spine02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
spine01	spine01 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
server01	server01 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
leaf04	leaf04 config file lldpd was created	configdiff	info	9/10/19 3:19 PM

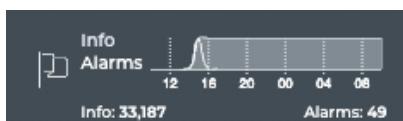
Item	Description
Title	Events   Info
×	Closes full screen card and returns to workbench
Default Time	Range of time in which the displayed data was collected
Results	Number of results found for the selected tab

Item	Description
All Events	<p>Displays all events (both alarms and info) received in the time period. By default, the requests list is sorted by the date and time that the event occurred (<b>Time</b>). This tab provides the following additional data about each request:</p> <ul style="list-style-type: none"> <li>• <b>Source:</b> Hostname of the given event</li> <li>• <b>Message:</b> Text describing the alarm or info event that occurred</li> <li>• <b>Type:</b> Name of network protocol and/or service that triggered the given event</li> <li>• <b>Severity:</b> Importance of the event—critical, warning, info, or debug</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
⚙️	Enables manipulation of table display; choose columns to display and reorder columns

### View Info Status Summary

A summary of the informational events occurring in the network can be found on the small, medium, and large Info cards. Additional details are available as you increase the size of the card.

To view the summary with the *small* Info card, simply open the card. This card gives you a high-level view in a condensed visual, including the number and distribution of the info events along with the alarms that have occurred during the same time period.

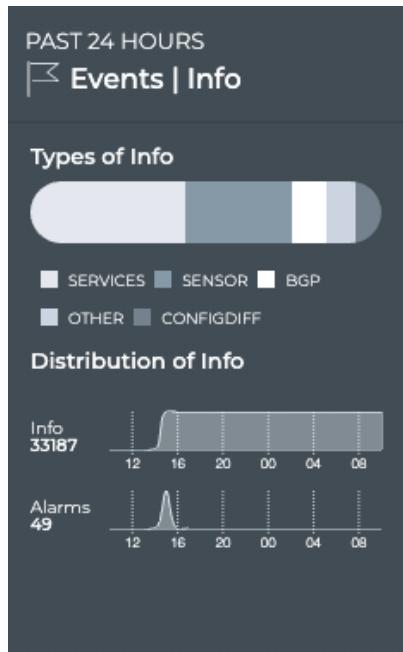


To view the summary with the *medium* Info card, simply open the card. This card gives you the same count and distribution of info and alarm events, but it also provides

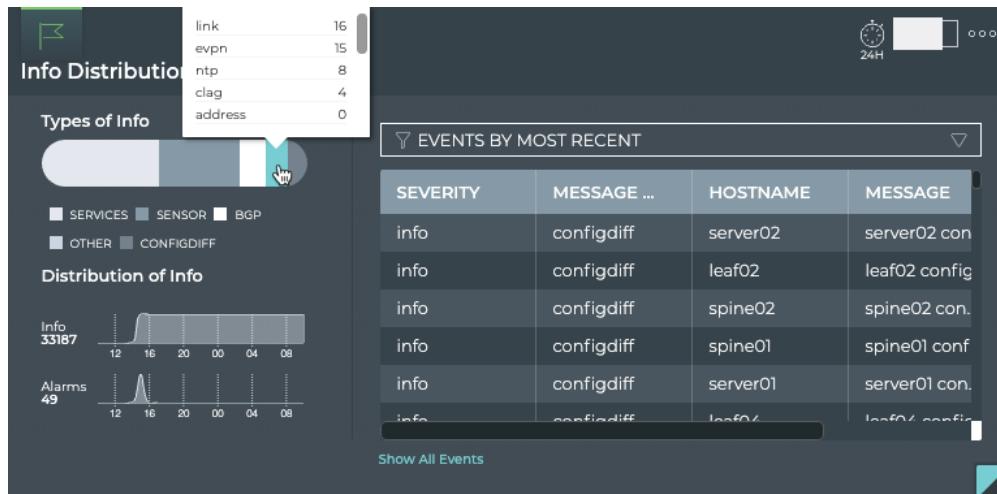
## Monitor Events

## Monitor Info Events

information about the sources of the info events and enables you to view a small slice of time using the distribution charts.



Use the chart at the top of the card to view the various sources of info events. The four or so types with the most info events are called out separately, with all others collected together into an *Other* category. Hover over segment of chart to view the count for each type.



To view the summary with the large Info card, open the card. The left side of the card provides the same capabilities as the medium Info card.

### Compare Timing of Info and Alarm Events

While you can see the relative relationship between info and alarm events on the small Info card, the medium and large cards provide considerably more information. Open either of these to view individual line charts for the events. Generally, alarms have some corollary info events. For example, when a network service becomes unavailable, a critical alarm is often issued, and when the service becomes available again, an info event of severity warning is generated. For this reason, you might see some level of tracking between the info and alarm counts and distributions. Some other possible scenarios:

- When a critical alarm is resolved, you may see a temporary increase in info events as a result.
- When you get a burst of info events, you may see a follow-on increase in critical alarms, as the info events may have been warning you of something beginning to go wrong.
- You set logging to debug, and a large number of info events of severity debug are seen. You would not expect to see an increase in critical alarms.

### View All Info Events Sorted by Time of Occurrence

You can view all info events using the large Info card. Open the large card and confirm the **Events By Most Recent** option is selected in the filter above the table on the right. When this option is selected, all of the info events are listed with the most recently occurring event at the top. Scrolling down shows you the info events that have occurred at an earlier time within the selected time period for the card.

## Monitor Events

## Monitor Info Events

The card displays "PAST 24 HOURS" and a "Events | Info" section. It includes a "Types of Info" chart and a "Distribution of Info" chart. A table titled "EVENTS BY MOST RECENT" lists five entries:

SEVERITY	MESSAGE ...	HOSTNAME	MESSAGE
info	configdiff	server02	server02 con
info	configdiff	leaf02	leaf02 config
info	configdiff	spine02	spine02 con.
info	configdiff	spine01	spine01 conf

[Show All Events](#)

### View Devices with the Most Info Events

You can filter instead for the devices that have the most info events by selecting the **Devices by Event Count** option from the filter above the table.

The card shows a filter dropdown set to "Devices by event count". It includes a "Types of Info" chart and a "Distribution of Info" chart. A table titled "DEVICES BY EVENT COUNT" lists six devices:

DEVICE	EVENT TY...	COUNT
leaf01	info	53
leaf02	info	51
leaf03	info	50
leaf04	info	50
spine02	info	48
exit01	info	46

[Show All Events](#)

### View All Events

You can view all events in the network either by clicking the **Show All Events** link under the table on the large Info Events card, or by opening the full screen Info Events card.



OR

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
server02	server02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
leaf02	leaf02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
spine02	spine02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
spine01	spine01 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
server01	server01 config file lldpd was created	configdiff	info	9/10/19 3:19 PM
leaf04	leaf04 config file lldpd was created	configdiff	info	9/10/19 3:19 PM

To return to your workbench, click



in the top right corner of the card.

## Events Reference

The following table lists all event messages organized by type.

NOTE

The messages can be viewed through third-party notification applications. For details about configuring notifications using the NetQ CLI, refer to [Integrate NetQ with Notification Applications](#).

Type	Trigger	Severity	Message Format
agent	NetQ Agent state changed to Rotten (not heard from in over 15 seconds)	Critical	Agent state changed to rotten
agent	NetQ Agent rebooted	Critical	Netq-agent rebooted at (@last_boot)
agent	Node running NetQ Agent rebooted	Critical	Switch rebooted at (@sys_uptime)
agent	NetQ Agent state changed to Fresh	Info	Agent state changed to fresh
agent	NetQ Agent state was reset	Info	Agent state was paused and resumed at (@last_reinit)

Type	Trigger	Severity	Message Format
agent	Version of NetQ Agent has changed	Info	Agent version has been changed old_version:@old_version and new_version:@new_version. Agent reset at @sys_uptime
bgp	BGP Session state changed	Critical	BGP session with peer @peer @neighbor vrf @vrf state changed from @old_state to @new_state
bgp	BGP Session state changed from Failed to Established	Info	BGP session with peer @peer @peerhost @neighbor vrf @vrf session state changed from Failed to Established
bgp	BGP Session state changed from Established to Failed	Info	BGP session with peer @peer @neighbor vrf @vrf state changed from established to failed

Type	Trigger	Severity	Message Format
bgp	The reset time for a BGP session changed	Info	BGP session with peer @peer @neighbor vrf @vrf reset time changed from @old_last_reset_time to @new_last_reset_time
btrfsinfo	Disk space available after BTRFS allocation is less than 80% of partition size or only 2 GB remain.	Critical	@info : @details
btrfsinfo	Indicates if space would be freed by a rebalance operation on the disk	Critical	@info : @details
cable	Link speed is not the same on both ends of the link	Critical	@ifname speed @speed, mismatched with peer @peer @peer_if speed @peer_speed
cable	The speed setting for a given port changed	Info	@ifname speed changed from @old_speed to @new_speed

Type	Trigger	Severity	Message Format
cable	The transceiver status for a given port changed	Info	@ifname transceiver changed from @old_transceiver to @new_transceiver
cable	The vendor of a given transceiver changed	Info	@ifname vendor name changed from @old_vendor_name to @new_vendor_name
cable	The part number of a given transceiver changed	Info	@ifname part number changed from @old_part_number to @new_part_number
cable	The serial number of a given transceiver changed	Info	@ifname serial number changed from @old_serial_number to @new_serial_number

Type	Trigger	Severity	Message Format
cable	The status of forward error correction (FEC) support for a given port changed	Info	@ifname supported fec changed from @old_supported_fec to @new_supported_fec
cable	The advertised support for FEC for a given port changed	Info	@ifname supported fec changed from @old_advertised_fec to @new_advertised_fec
cable	The FEC status for a given port changed	Info	@ifname fec changed from @old_fec to @new_fec
clag	CLAG remote peer state changed from up to down	Critical	Peer state changed to down

Type	Trigger	Severity	Message Format
clag	Local CLAG host MTU does not match its remote peer MTU	Critical	SVI @svi1 on vlan @vlan mtu @mtu1 mismatched with peer mtu @mtu2
clag	CLAG SVI on VLAN is missing from remote peer state	Warning	SVI on vlan @vlan is missing from peer
clag	CLAG peerlink is not operating at full capacity. At least one link is down.	Warning	Clag peerlink not at full redundancy, member link @slave is down
clag	CLAG remote peer state changed from down to up	Info	Peer state changed to up
clag	Local CLAG host state changed from down to up	Info	Clag state changed from down to up

Type	Trigger	Severity	Message Format
clag	CLAG bond in Conflicted state was updated with new bonds	Info	Clag conflicted bond changed from @old_conflicted_bonds to @new_conflicted_bonds
clag	CLAG bond changed state from protodown to up state	Info	Clag conflicted bond changed from @old_state_protodownbond to @new_state_protodownbond
clsupport	A new CL Support file has been created for the given node	Critical	HostName @hostname has new CL SUPPORT file
configdiff	Configuration file deleted on a device	Critical	@hostname config file @type was deleted
configdiff	Configuration file has been created	Info	@hostname config file @type was created

Type	Trigger	Severity	Message Format
configdiff	Configuration file has been modified	Info	@hostname config file @type was modified
evpn	A VNI was configured and moved from the up state to the down state	Critical	VNI @vni state changed from up to down
evpn	A VNI was configured and moved from the down state to the up state	Info	VNI @vni state changed from down to up
evpn	The kernel state changed on a VNI	Info	VNI @vni kernel state changed from @old_in_kernel_state to @new_in_kernel_state
evpn	A VNI state changed from not advertising all VNIs to advertising all VNIs	Info	VNI @vni vni state changed from @old_adv_all_vni_state to @new_adv_all_vni_state

Type	Trigger	Severity	Message Format
license	License state is missing or invalid	Critical	License check failed, name @lic_name state @state
license	License state is missing or invalid on a particular device	Critical	License check failed on @hostname
link	Link operational state changed from up to down	Critical	HostName @hostname changed state from @old_state to @new_state Interface:@ifname
link	Link operational state changed from down to up	Info	HostName @hostname changed state from @old_state to @new_state Interface:@ifname
lldp	Local LLDP host has new neighbor information	Info	LLDP Session with host @hostname and @ifname modified fields @changed_fields

Type	Trigger	Severity	Message Format
lldp	Local LLDP host has new peer interface name	Info	LLDP Session with host @hostname and @ifname @old_peer_ifname changed to @new_peer_ifname
lldp	Local LLDP host has new peer hostname	Info	LLDP Session with host @hostname and @ifname @old_peer_hostname changed to @new_peer_hostname
inv	VXLAN registration daemon, vxrd, is not running	Critical	vxrd service not running
mtu	VLAN interface link MTU is smaller than that of its parent MTU	Warning	vlan interface @link mtu @mtu is smaller than parent @parent mtu @parent_mtu
mtu	Bridge interface MTU is smaller than the member interface with the smallest MTU	Warning	bridge @link mtu @mtu is smaller than least of member interface mtu @min

Type	Trigger	Severity	Message Format
ntp	NTP sync state changed from in sync to not in sync	Critical	Sync state changed from @old_state to @new_state for @hostname
ntp	NTP sync state changed from not in sync to in sync	Info	Sync state changed from @old_state to @new_state for @hostname
ospf	OSPF session state on a given interface changed from Full to a down state	Critical	OSPF session @ifname with @peer_address changed from Full to @down_state

Type	Trigger	Severity	Message Format
ospf	OSPF session state on a given interface changed from a down state to full	Info	OSPF session @ifname with @peer_address changed from @down_state to Full
packageinfo	Package version on device does not match the version identified in the existing manifest	Critical	@package_name manifest version mismatch
ptm	Physical interface cabling does not match configuration specified in <i>topology.dot</i> file	Critical	PTM cable status failed

Type	Trigger	Severity	Message Format
ptm	Physical interface cabling matches configuration specified in <i>topology.dot</i> file	Critical	PTM cable status passed
resource	A physical resource has been deleted from a device	Critical	Resource Utils deleted for @hostname
resource	Root file system access on a device has changed from Read/Write to Read Only	Critical	@hostname root file system access mode set to Read Only
resource	Root file system access on a device has changed from Read Only to Read/Write	Info	@hostname root file system access mode set to Read/Write

Type	Trigger	Severity	Message Format
resource	A physical resource has been added to a device	Info	Resource Utils added for @hostname
runningconfigdiff	A fan or power supply unit sensor has changed state	Info	@commandname config result was modified
sensor	A fan or power supply unit sensor has changed state	Critical	Sensor @sensor state changed from @old_s_state to @new_s_state
sensor	A temperature sensor has crossed the maximum threshold for that sensor	Critical	Sensor @sensor max value @new_s_max exceeds threshold @new_s_crit
sensor	A temperature sensor has crossed the minimum threshold for that sensor	Critical	Sensor @sensor min value @new_s_lcrit fall behind threshold @new_s_min

Type	Trigger	Severity	Message Format
sensor	A temperature, fan, or power supply sensor state changed	Info	Sensor @sensor state changed from @old_state to @new_state
sensor	A fan or power supply sensor state changed	Info	Sensor @sensor state changed from @old_s_state to @new_s_state
services	A service status changed from down to up	Critical	Service @name status changed from @old_status to @new_status
services	A service status changed from up to down	Critical	Service @name status changed from @old_status to @new_status

Type	Trigger	Severity	Message Format
services	A service changed state from inactive to active	Info	Service @name changed state from inactive to active
ssdutil	3ME3 disk health has dropped below 10%	Critical	@info: @details
ssdutil	A dip in 3ME3 disk health of more than 2% has occurred within the last 24 hours	Critical	@info: @details
version	An unknown version of the operating system was detected	Critical	unexpected os version @my_ver

Type	Trigger	Severity	Message Format
version	Desired version of the operating system is not available	Critical	os version @ver
version	An unknown version of a software package was detected	Critical	expected release version @ver
version	Desired version of a software package is not available	Critical	different from version @ver
vxlan	Replication list is contains an inconsistent set of nodes	Critical	VNI @vni replication list inconsistent with @conflicts diff:@diff

# Monitor the BGP Service

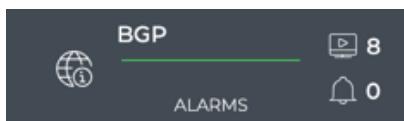
The Cumulus NetQ UI enables operators to view the health of the BGP service on a network-wide and a per session basis, giving greater insight into all aspects of the service. This is accomplished through two card workflows, one for the service and one for the session. They are described separately here.

## Monitor the BGP Service (All Sessions)

With NetQ, you can monitor the number of nodes running the BGP service, view switches with the most established and unestablished BGP sessions, and view alarms triggered by the BGP service. For an overview and how to configure BGP to run in your data center network, refer to [Border Gateway Protocol - BGP](#).

### BGP Service Card Workflow

The small BGP Service card displays:



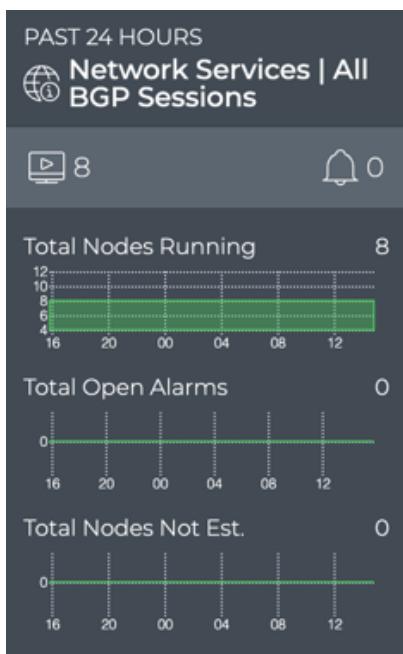
Item	Description
	Indicates data is for all sessions of a Network Service or Protocol
Title	BGP: All BGP Sessions, or the BGP Service

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
	Total number of switches and hosts with the BGP service enabled during the designated time period
	Total number of BGP-related alarms received during the designated time period
Chart	Distribution of new BGP-related alarms received during the designated time period

The medium BGP Service card displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
Title	Network Services   All BGP Sessions
	Total number of switches and hosts with the BGP service enabled during the designated time period
	Total number of BGP-related alarms received during the designated time period
Total Nodes Running chart	<p>Distribution of switches and hosts with the BGP service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running BGP last week or last month might be more or less than the number of nodes running BGP currently.</p>
Total Open Alarms chart	<p>Distribution of BGP-related alarms received during the designated time period, and the total number of current BGP-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
Total Nodes Not Est. chart	<p>Distribution of switches and hosts with unestablished BGP sessions during the designated time period, and the total number of unestablished sessions in the network currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of unestablished session last week or last month might be more or less than the number of nodes with unestablished sessions currently.</p>

The large BGP service card contains two tabs.

The *Sessions Summary* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	Sessions Summary (visible when you hover over card)

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

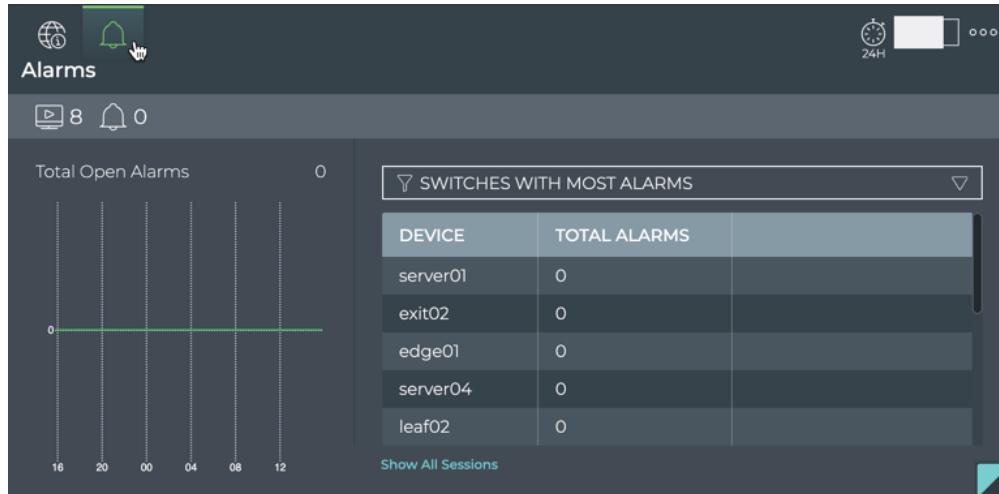
Item	Description
	Total number of switches and hosts with the BGP service enabled during the designated time period
	Total number of BGP-related alarms received during the designated time period
Total Nodes Running chart	<p>Distribution of switches and hosts with the BGP service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running BGP last week or last month might be more or less than the number of nodes running BGP currently.</p>
Total Nodes Not Est. chart	<p>Distribution of switches and hosts with unestablished BGP sessions during the designated time period, and the total number of unestablished sessions in the network currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of unestablished session last week or last month might be more or less than the number of nodes with unestablished sessions currently.</p>
Table/Filter options	<p>When the <b>Switches with Most Sessions</b> filter option is selected, the table displays the switches and hosts running BGP sessions in decreasing order of session count—devices with the largest number of sessions are listed first</p> <p>When the <b>Switches with Most Unestablished Sessions</b> filter option is selected, the table switches and hosts running BGP sessions in decreasing order of unestablished sessions—devices with the largest number of unestablished sessions are listed first</p>

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
Show All Sessions	Link to view data for all BGP sessions in the full screen card

The *Alarms* tab displays:



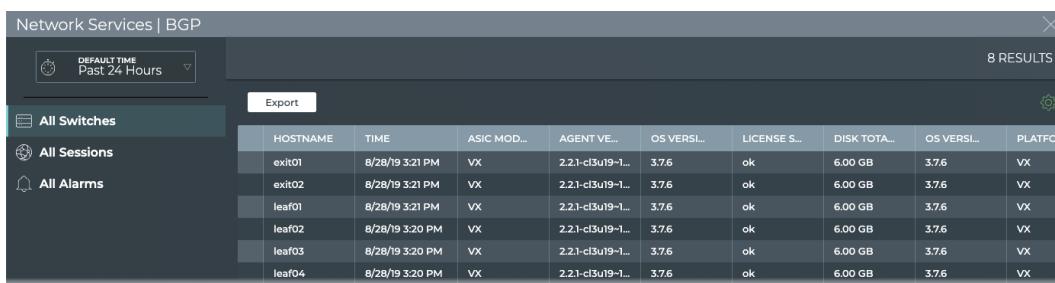
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
(in header)	Indicates data is for all alarms for all BGP sessions
Title	Alarms (visible when you hover over card)
	Total number of switches and hosts with the BGP service enabled during the designated time period

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
 (in summary bar)	Total number of BGP-related alarms received during the designated time period
Total Alarms chart	<p>Distribution of BGP-related alarms received during the designated time period, and the total number of current BGP-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Table/Filter options	When the selected filter option is <b>Switches with Most Alarms</b> , the table displays switches and hosts running BGP in decreasing order of the count of alarms—devices with the largest number of BGP alarms are listed first
Show All Sessions	Link to view data for all BGP sessions in the full screen card

The full screen BGP Service card provides tabs for all switches, all sessions, and all alarms.



The screenshot shows a table titled "Network Services | BGP" with the following data:

HOSTNAME	TIME	ASIC MOD...	AGENT VERSI...	OS VERSI...	LICENSE S...	DISK TOTAl...	OS VERSI...	PLATFO...
exit01	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf04	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
Title	Network Services   BGP
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

All Switches tab	<p>Displays all switches and hosts running the BGP service. By default, the device list is sorted by <b>hostname</b>. This tab provides the following additional data about each device:</p> <ul style="list-style-type: none"><li>• <b>Agent</b><ul style="list-style-type: none"><li>◦ State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).</li><li>◦ Version: Software version number of the NetQ Agent on a given device. This should match the version number of the NetQ software loaded on your server or appliance; for example, 2.2.0.</li></ul></li><li>• <b>ASIC</b><ul style="list-style-type: none"><li>◦ Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.</li><li>◦ Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.</li><li>◦ Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.</li><li>◦ Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.</li><li>◦ Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.</li></ul></li><li>• <b>CPU</b><ul style="list-style-type: none"><li>◦ Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.</li><li>◦ Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.</li><li>◦ Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.</li><li>◦ Nos: Number of cores. Example values include 2, 4, and 8.</li></ul></li><li>• <b>Disk Total Size:</b> Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.</li><li>• <b>License State:</b> Indicator of validity. Values include ok and bad.</li><li>• <b>Memory Size:</b> Total amount of local RAM. Example values include 8192 MB and 2048 MB.</li><li>• <b>OS</b></li></ul>
------------------------	--

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

All Sessions tab	<p>Displays all BGP sessions network-wide. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"><li>• <b>ASN</b>: Autonomous System Number, identifier for a collection of IP networks and routers. Example values include 633284,655435.</li><li>• <b>Conn Dropped</b>: Number of dropped connections for a given session</li><li>• <b>Conn Estd</b>: Number of connections established for a given session</li><li>• <b>DB State</b>: Session state of DB</li><li>• <b>Evpn Pfx Rcvd</b>: Address prefix received for EVPN traffic. Examples include 115, 35.</li><li>• <b>Ipv4, and Ipv6 Pfx Rcvd</b>: Address prefix received for IPv4 or IPv6 traffic. Examples include 31, 14, 12.</li><li>• <b>Last Reset Time</b>: Date and time at which the session was last established or reset</li><li>• <b>Objid</b>: Object identifier for service</li><li>• <b>OPID</b>: Customer identifier. This is always zero.</li><li>• <b>Peer</b><ul style="list-style-type: none"><li>◦ ASN: Autonomous System Number for peer device</li><li>◦ Hostname: User-defined name for peer device</li><li>◦ Name: Interface name or hostname of peer device</li><li>◦ Router Id: IP address of router with access to the peer device</li></ul></li><li>• <b>Reason</b>: Text describing the cause of, or trigger for, an event</li><li>• <b>Rx and Tx Families</b>: Address families supported for the receive and transmit session channels. Values include ipv4, ipv6, and evpn.</li><li>• <b>State</b>: Current state of the session. Values include Established and NotEstd (not established).</li><li>• <b>Timestamp</b>: Date and time session was started, deleted, updated or marked dead (device is down)</li><li>• <b>Upd8 Rx</b>: Count of protocol messages received</li><li>• <b>Upd8 Tx</b>: Count of protocol messages transmitted</li><li>• <b>Up Time</b>: Number of seconds the session has been established, in EPOCH notation. Example: 1550147910000</li><li>• <b>Vrf</b>: Name of the Virtual Route Forwarding interface. Examples: default, mgmt, DataVrf1081</li><li>• <b>Vrfid</b>: Integer identifier of the VRF interface when used. Examples: 14, 25, 37</li></ul>
------------------	--

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

Item	Description
All Alarms tab	<p>Displays all BGP events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"><li>• <b>Source:</b> Hostname of network device that generated the event</li><li>• <b>Message:</b> Text description of a BGP-related event. Example: BGP session with peer tor-1 swp7 vrf default state changed from failed to Established</li><li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of <i>bgp</i> in this card workflow.</li><li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li></ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
⚙️	Enables manipulation of table display; choose columns to display and reorder columns

### View Service Status Summary

A summary of the BGP service is available from the Network Services card workflow, including the number of nodes running the service, the number of BGP-related alarms, and a distribution of those alarms.

To view the summary, open the small BGP Service card.



For more detail, select a different size BGP Service card.

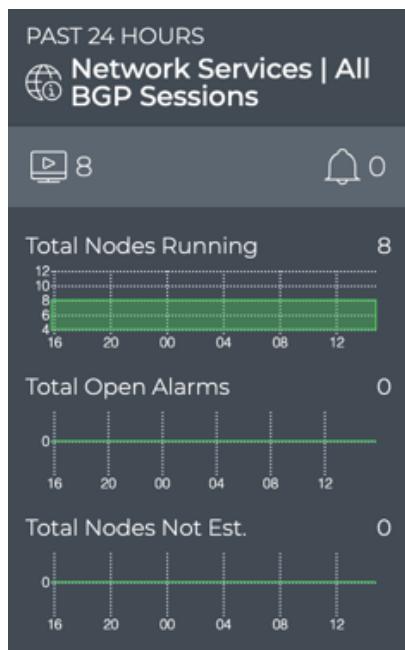
## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

### View the Distribution of Sessions and Alarms

It is useful to know the number of network nodes running the BGP protocol over a period of time, as it gives you insight into the amount of traffic associated with and breadth of use of the protocol. It is also useful to compare the number of nodes running BGP with unestablished sessions with the alarms present at the same time to determine if there is any correlation between the issues and the ability to establish a BGP session.

To view these distributions, open the medium BGP Service card.



If a visual correlation is apparent, you can dig a little deeper with the large BGP Service card tabs.

### View Devices with the Most BGP Sessions

You can view the load from BGP on your switches and hosts using the large Network Services card. This data enables you to see which switches are handling the most BGP traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

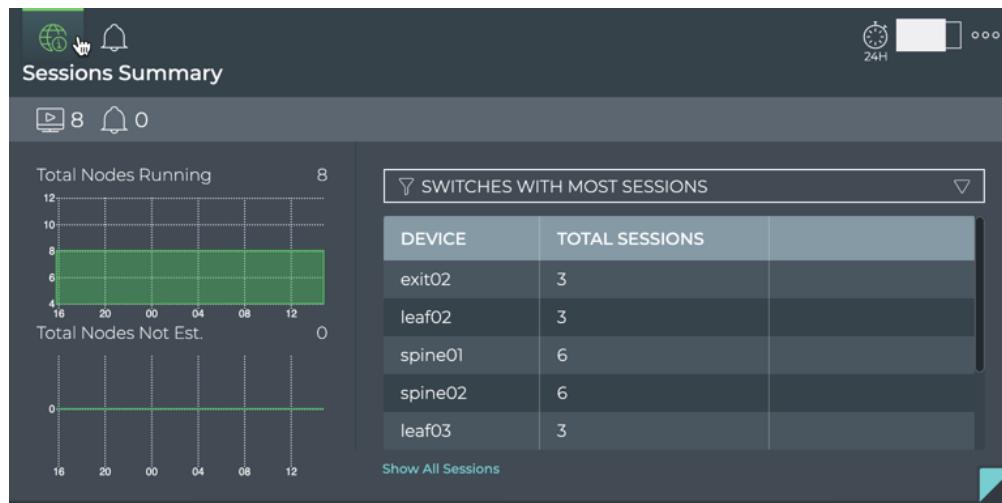
## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

To view switches and hosts with the most BGP sessions:

1. Open the large BGP Service card.
2. Select **Switches With Most Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most BGP sessions at the top. Scroll down to view those with the fewest sessions.

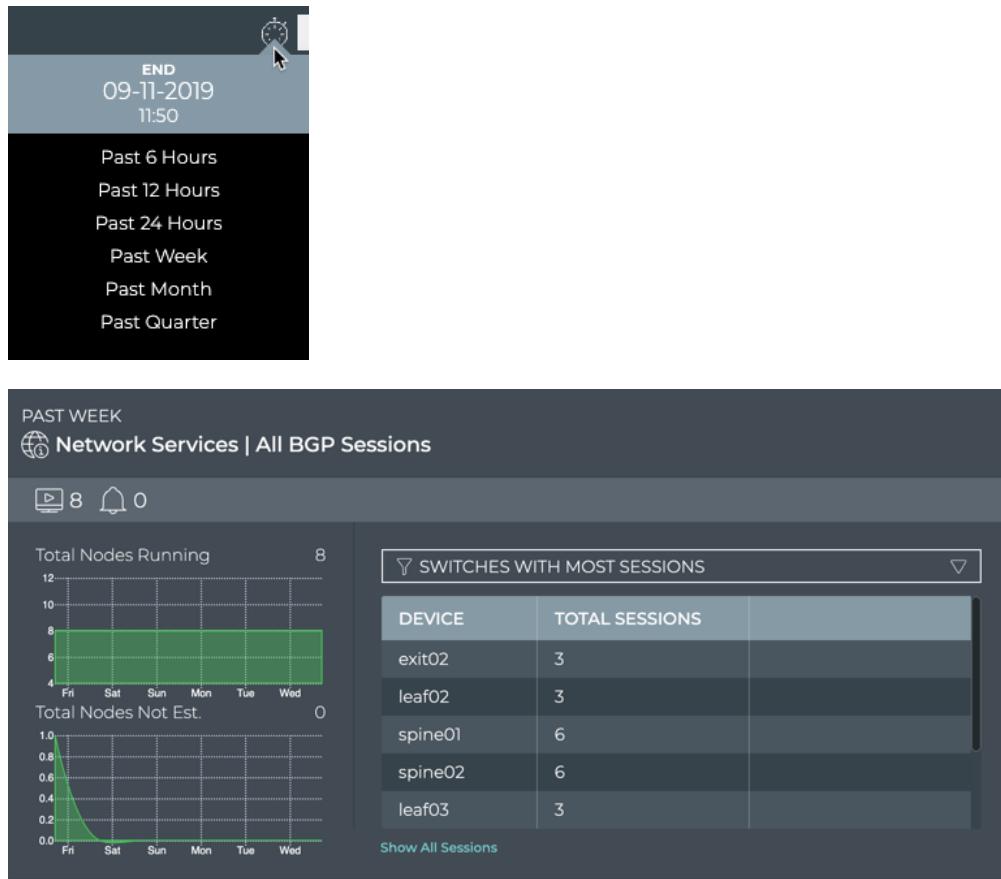


To compare this data with the same data at a previous time:

1. Open another large BGP Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking .  
.
4. Select the time period that you want to compare with the original time. We chose *Past Week* for this example.

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)



You can now see whether there are significant differences between this time and the original time. If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running BGP than previously, looking for changes in the topology, and so forth.

### View Devices with the Most Unestablished BGP Sessions

You can identify switches and hosts that are experiencing difficulties establishing BGP sessions; both currently and in the past.

To view switches with the most unestablished BGP sessions:

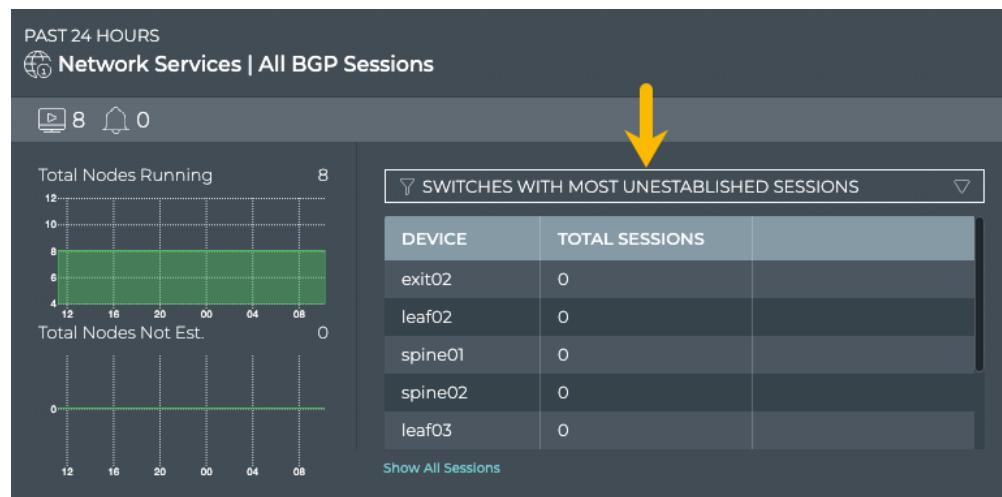
1. Open the large BGP Service card.
2. Select **Switches with Most Unestablished Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

unestablished BGP sessions at the top. Scroll down to view those with the fewest unestablished sessions.



Where to go next depends on what data you see, but a couple of options include:

- Change the time period for the data to compare with a prior time.

If the same switches are consistently indicating the most unestablished sessions, you might want to look more carefully at those switches using the Switches card workflow to determine probable causes. Refer to [Monitor Switches](#).

- Click **Show All Sessions** to investigate all BGP sessions with events in the full screen card.

### View Devices with the Most BGP-related Alarms

Switches or hosts experiencing a large number of BGP alarms may indicate a configuration or performance issue that needs further investigation. You can view the devices sorted by the number of BGP alarms and then use the Switches card workflow or the Alarms card workflow to gather more information about possible causes for the alarms.

To view switches with the most BGP alarms:

1. Open the large BGP Service card.

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

2. Hover over the header and click



.

3. Select **Switches with Most Alarms** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most BGP alarms at the top. Scroll down to view those with the fewest alarms.



Where to go next depends on what data you see, but a few options include:

- Change the time period for the data to compare with a prior time. If the same switches are consistently indicating the most alarms, you might want to look more carefully at those switches using the Switches card workflow.
- Click **Show All Sessions** to investigate all BGP sessions with events in the full screen card.

### View All BGP Events

The BGP Network Services card workflow enables you to view all of the BGP events in the designated time period.

To view all BGP events:

1. Open the full screen BGP Service card.

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)

2. Click **All Alarms** tab in the navigation panel.

By default, events are listed in most recent to least recent order.

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
spine01	BGP session with peer swp29 vrf default state changed from Established to NotEstd	bgp	critical	9/10/19 3:29 PM
spine01	BGP session with peer swp30 vrf default state changed from Established to NotEstd	bgp	critical	9/10/19 3:29 PM
spine02	BGP session with peer swp4 vrf default state changed from Established to NotEstd	bgp	critical	9/10/19 3:29 PM
spine02	BGP session with peer swp1 vrf default state changed from Established to NotEstd	bgp	critical	9/10/19 3:29 PM
spine02	BGP session with peer swp3 vrf default state changed from Established to NotEstd	bgp	critical	9/10/19 3:29 PM

Where to go next depends on what data you see, but a couple of options include:

- Sort the list by message to see how many devices have had the same issue.
- Open one of the other full screen tabs in this flow to focus on devices or sessions.
- Export the data for use in another analytics tool, by clicking **Export** and providing a name for the data file.

To return to your workbench, click



in the top right corner.

## View Details for All Devices Running BGP

You can view all stored attributes of all switches and hosts running BGP in your network in the full screen card.

To view all device details, open the full screen BGP Service card and click the **All Switches** tab.

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFO
exit01	8/28/19 3:21 PM	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 PM	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/28/19 3:21 PM	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/28/19 3:20 PM	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 PM	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf04	8/28/19 3:20 PM	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

To return to your workbench, click

## Monitor the BGP Service

## Monitor the BGP Service (All Sessions)



in the top right corner.

### View Details for All BGP Sessions

You can view all stored attributes of all BGP sessions in your network in the full-screen card.

To view all session details, open the full screen BGP Service card and click the **All Sessions** tab.

Network Services   BGP											
DEFAULT TIME Past 24 Hours		30 RESULTS									
		Export									
All Switches		All Sessions									
IPV6_PFX...	PEER ROU...	UPD8 TX	HOSTNAME	TIMESTAMP	PEER ASN	STATE	VRF	RX FAMILI...	IP		
0	10.0.0.21	80	exit01	9/11/19 3:18 PM	65020	Established	default	ipv4,evpn	8		
0	10.0.0.22	80	exit01	9/11/19 3:18 PM	65020	Established	default	ipv4,evpn	8		
0	10.0.0.253	15	exit01	9/11/19 3:18 PM	25253	Established	vrf1	ipv4	2		
0	10.0.0.21	85	exit02	9/11/19 3:18 PM	65020	Established	default	ipv4,evpn	8		
0	10.0.0.22	85	exit02	9/11/19 3:18 PM	65020	Established	default	ipv4,evpn	8		

To return to your workbench, click



in the top right corner.

### Take Actions on Data Displayed in Results List

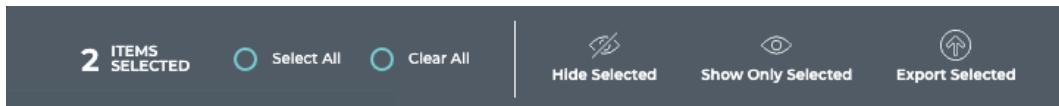
In the full screen BGP Service card, you can determine which results are displayed in the results list, and which are exported.

To take actions on the data, click in the blank column at the very left of a row. A checkbox appears, selecting that switch, session, or alarm, and an edit menu is shown at the bottom of the card (shown enlarged here).

Network Services   BGP											
DEFAULT TIME Past 24 Hours		8 RESULTS									
		Export									
All Switches		All Sessions									
HOSTNAME	TIME	ASIC MOD...	AGENT VERS...	OS VERSI...	LICENSE S...	DISK TOTA...	OS.VERS...	PLATFOR...	M		
exit01	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76		
exit02	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76		
<input checked="" type="checkbox"/> leaf01	8/28/19 3:21 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76		
<input checked="" type="checkbox"/> leaf02	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76		
leaf03	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76		
leaf04	8/28/19 3:20 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	76		

## Monitor the BGP Service

## Monitor a Single BGP Session



You can perform the following actions on the results list:

Option	Action or Behavior on Click
Select All	Selects all items in the results list
Clear All	Clears all existing selections of items in the results list. This also hides the edit menu.
Open Cards	Open the corresponding validation or trace result card.
Hide Selected	Hide selected items (switches, sessions, alarms, and so forth) from the results list.
Show Only Selected	Hide unselected items (switches, sessions, alarms, and so forth) from the results list.
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the <b>Export</b> button.

To return to original display of results, click the associated tab.

## Monitor a Single BGP Session

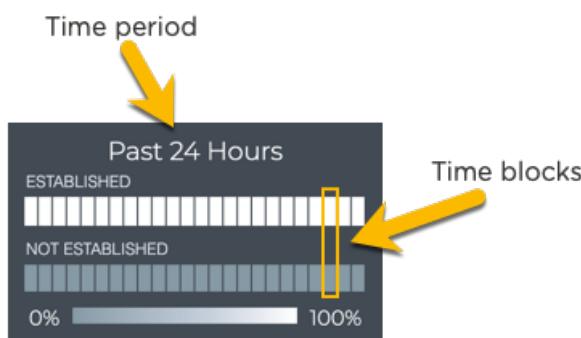
With NetQ, you can monitor a single session of the BGP service, view session state changes, and compare with alarms occurring at the same time, as well as monitor the running BGP configuration and changes to the configuration file. For an overview and how to configure BGP to run in your data center network, refer to [Border Gateway Protocol - BGP](#).

**NOTE**

To access the single session cards, you must open the full screen BGP Service, click the All Sessions tab, select the desired session, then click  (Open Cards).

**Granularity of Data Shown Based on Time Period**

On the medium and large single BGP session cards, the status of the sessions is represented in heat maps stacked vertically; one for established sessions, and one for unestablished sessions. Depending on the time period of data on the card, the number of smaller time blocks used to indicate the status varies. A vertical stack of time blocks, one from each map, includes the results from all checks during that time. The results are shown by how saturated the color is for each block. If all sessions during that time period were established for the entire time block, then the top block is 100% saturated (white) and the not established block is zero percent saturated (gray). As sessions that are not established increase in saturation, the sessions that are established block is proportionally reduced in saturation. An example heat map for a time period of 24 hours is shown here with the most common time periods in the table showing the resulting time blocks.



6 hours

18

6

1 hour

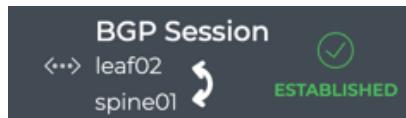
## Monitor the BGP Service

## Monitor a Single BGP Session

Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

### BGP Session Card Workflow Summary

The small BGP Session card displays:

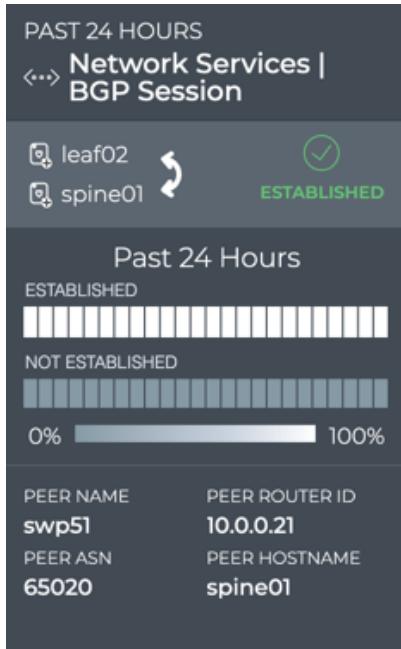


Item	Description
<::>	Indicates data is for a single session of a Network Service or Protocol
Title	BGP Session
	Hostnames of the two devices in a session. Arrow points from the host to the peer.
✓ ✗	Current status of the session, either established or not established

The medium BGP Session card displays:

## Monitor the BGP Service

## Monitor a Single BGP Session

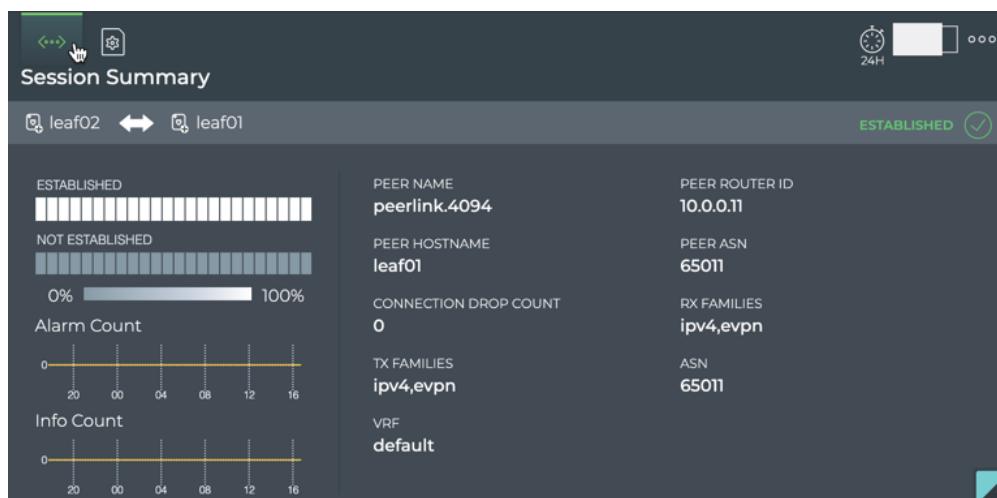


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
↔	Indicates data is for a single session of a Network Service or Protocol
Title	Network Services   BGP Session
	Hostnames of the two devices in a session. Arrow points in the direction of the session.
✓ / ✘	Current status of the session, either established or not established
Time period for chart	Time period for the chart data

Item	Description
Session State Changes Chart	Heat map of the state of the given session over the given time period. The status is sampled at a rate consistent with the time period. For example, for a 24 hour period, a status is collected every hour. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> .
Peer Name	Interface name on or hostname for peer device
Peer ASN	Autonomous System Number for peer device
Peer Router ID	IP address of router with access to the peer device
Peer Hostname	User-defined name for peer device

The large BGP Session card contains two tabs.

The *Session Summary* tab displays:



## Monitor the BGP Service

## Monitor a Single BGP Session

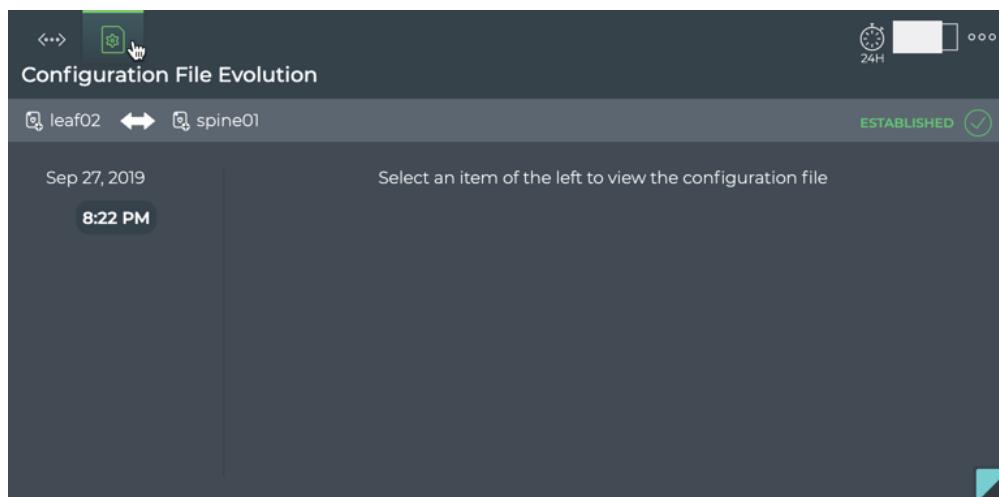
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
↔↔↔	Indicates data is for a single session of a Network Service or Protocol
Title	Session Summary (Network Services   BGP Session)
Summary bar	<p>Hostnames of the two devices in a session. Arrow points in the direction of the session.</p> <p>Current status of the session—either established  <input checked="" type="checkbox"/> , or not established  <input type="checkbox"/></p>
Session State Changes Chart	Heat map of the state of the given session over the given time period. The status is sampled at a rate consistent with the time period. For example, for a 24 hour period, a status is collected every hour. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> .
Alarm Count Chart	Distribution and count of BGP alarm events over the given time period.
Info Count Chart	Distribution and count of BGP info events over the given time period.
Connection Drop Count	Number of times the session entered the not established state during the time period
ASN	Autonomous System Number for host device
RX/TX Families	Receive and Transmit address types supported. Values include IPv4, IPv6, and EVPN.
Peer Hostname	User-defined name for peer device

## Monitor the BGP Service

## Monitor a Single BGP Session

Item	Description
Peer Interface	Interface on which the session is connected
Peer ASN	Autonomous System Number for peer device
Peer Router ID	IP address of router with access to the peer device

The *Configuration File Evolution* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates configuration file information for a single session of a Network Service or Protocol
Title	(Network Services   BGP Session) Configuration File Evolution

## Monitor the BGP Service

## Monitor a Single BGP Session

Item	Description
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Click on  to open associated device card.
 	Indication of host role, primary or secondary 
Timestamps	When changes to the configuration file have occurred, the date and time are indicated. Click the time to see the changed file.
Configuration File	<p>When <b>File</b> is selected, the configuration file as it was at the selected time is shown.</p> <p>When <b>Diff</b> is selected, the configuration file at the selected time is shown on the left and the configuration file at the previous timestamp is shown on the right. Differences are highlighted.</p> <p><b>Note:</b> If no configuration file changes have been made, only the original file date is shown.</p>

The full screen BGP Session card provides tabs for all BGP sessions and all events.

The screenshot shows the Network Services | BGP card interface. At the top, there's a search bar and a filter dropdown set to "DEFAULT TIME Past 24 Hours". Below the header, there are two tabs: "All BGP Sessions" (which is currently selected, indicated by a dark blue background) and "All Events". The main area contains a table with the following data:

IPV6 PFX ...	PEER ROU...	UPD8 TX	HOSTNAME	TIMESTAMP	PEER ASN	STATE	VRF	RX FAMILI...
0	10.0.0.22	43	leaf01	9/10/19 3:17 P...	65020	Established	default	ipv4.evpn
0	10.0.0.22	43	leaf01	9/10/19 3:18 P...	65020	Established	default	ipv4.evpn
0	10.0.0.22	64	leaf01	9/10/19 3:28 ...	65020	Established	default	ipv4.evpn
0	0.0.0.0	0	leaf01	9/10/19 3:29 ...	0	NotEstd	default	
0	10.0.0.22	53	leaf01	9/10/19 3:29 ...	65020	Established	default	ipv4.evpn

At the bottom right of the card, there are "5 RESULTS" and a gear icon for settings.

## Monitor the BGP Service

## Monitor a Single BGP Session

Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
Title	Network Services   BGP

All BGP Sessions tab	<p>Displays all BGP sessions running on the host device. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"><li>• <b>ASN:</b> Autonomous System Number, identifier for a collection of IP networks and routers. Example values include 633284,655435.</li><li>• <b>Conn Dropped:</b> Number of dropped connections for a given session</li><li>• <b>Conn Estd:</b> Number of connections established for a given session</li><li>• <b>DB State:</b> Session state of DB</li><li>• <b>Evpn Pfx Rcvd:</b> Address prefix for EVPN traffic. Examples include 115, 35.</li><li>• <b>Ipv4, and Ipv6 Pfx Rcvd:</b> Address prefix for IPv4 or IPv6 traffic. Examples include 31, 14, 12.</li><li>• <b>Last Reset Time:</b> Time at which the session was last established or reset</li><li>• <b>Objid:</b> Object identifier for service</li><li>• <b>OPID:</b> Customer identifier. This is always zero.</li><li>• <b>Peer</b><ul style="list-style-type: none"><li>◦ ASN: Autonomous System Number for peer device</li><li>◦ Hostname: User-defined name for peer device</li><li>◦ Name: Interface name or hostname of peer device</li><li>◦ Router Id: IP address of router with access to the peer device</li></ul></li><li>• <b>Reason:</b> Event or cause of failure</li><li>• <b>Rx and Tx Families:</b> Address families supported for the receive and transmit session channels. Values include ipv4, ipv6, and evpn.</li><li>• <b>State:</b> Current state of the session. Values include Established and NotEstd (not established).</li><li>• <b>Timestamp:</b> Date and time session was started, deleted, updated or marked dead (device is down)</li><li>• <b>Upd8 Rx:</b> Count of protocol messages received</li><li>• <b>Upd8 Tx:</b> Count of protocol messages transmitted</li><li>• <b>Up Time:</b> Number of seconds the session has been established, in EPOCH notation. Example: 1550147910000</li><li>• <b>Vrf:</b> Name of the Virtual Route Forwarding interface. Examples: default, mgmt, DataVrf1081</li><li>• <b>Vrfid:</b> Integer identifier of the VRF interface when used. Examples: 14, 25, 37</li></ul>
----------------------	---

Item	Description
All Events tab	<p>Displays all events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of a BGP-related event. Example: BGP session with peer tor-1 swp7 vrf default state changed from failed to Established</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of bgp in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Session Status Summary

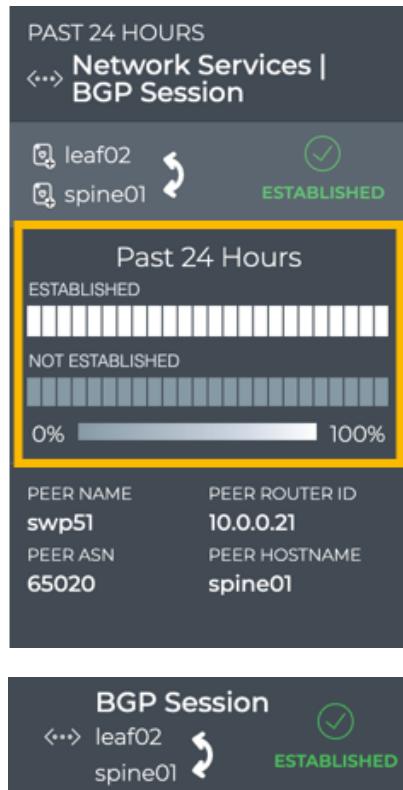
A summary of the BGP session is available from the BGP Session card workflow, showing the node and its peer and current status.

To view the summary:

1. Add the Network Services | All BGP Sessions card.
2. Switch to the full screen card.
3. Click the **All Sessions** tab.
4. Double-click the session of interest. The full screen card closes automatically.
5. Optionally, switch to the small BGP Session card.

## Monitor the BGP Service

## Monitor a Single BGP Session



### View BGP Session State Changes

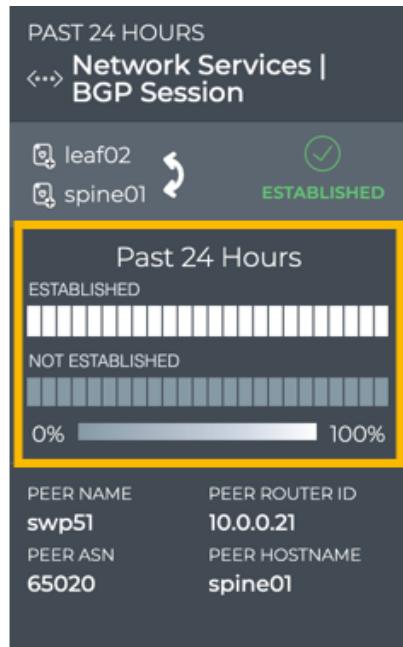
You can view the state of a given BGP session from the medium and large BGP Session Network Service cards. For a given time period, you can determine the stability of the BGP session between two devices. If you experienced connectivity issues at a particular time, you can use these cards to help verify the state of the session. If it was not established more than it was established, you can then investigate further into possible causes.

To view the state transitions for a given BGP session, on the *medium* BGP Session card:

1. Add the Network Services | All BGP Sessions card.
2. Switch to the full screen card.
3. Open the large BGP Service card.
4. Click the **All Sessions** tab.
5. Double-click the session of interest. The full screen card closes automatically.

## Monitor the BGP Service

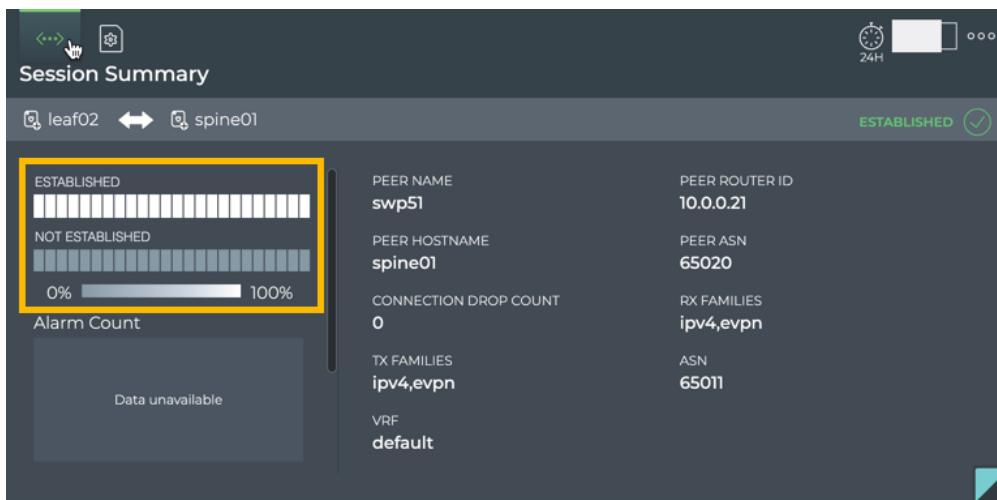
## Monitor a Single BGP Session



The heat map indicates the status of the session over the designated time period. In this example, the session has been established for the entire time period.

From this card, you can also view the Peer ASN, name, hostname and router id identifying the session in more detail.

To view the state transitions for a given BGP session on the large BGP Session card, follow the same steps to open the medium BGP Session card and then switch to the large card.



## Monitor the BGP Service

## Monitor a Single BGP Session

From this card, you can view the alarm and info event counts, Peer ASN, hostname, and router id, VRF, and Tx/Rx families identifying the session in more detail. The Connection Drop Count gives you a sense of the session performance.

### View Changes to the BGP Service Configuration File

Each time a change is made to the configuration file for the BGP service, NetQ logs the change and enables you to compare it with the last version. This can be useful when you are troubleshooting potential causes for alarms or sessions losing their connections.

To view the configuration file changes:

1. Open the large BGP Session card.
2. Hover over the card and click  to open the **BGP Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.
4. Choose between the **File** view and the **Diff** view (selected option is dark; File by default).

The File view displays the content of the file for you to review.



PAST 24 HOURS

Network Services | BGP Session

leaf01 ← spine02 ESTABLISHED ✓

Jun 11, 2019

● 7:05 PM

7:02 PM

FILE DIFF

```
1 frr defaults datacenter
2 hostname leaf01
3 username cumulus nopassword
4 !
5 service integrated-vtysh-config
6 !
7 log syslog informational
8 !
9 vrf vrf1
```

## Monitor the BGP Service

## Monitor a Single BGP Session

The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted, as seen in this example.

PAST 24 HOURS

Network Services | BGP Session

leaf01 ← spine02

ESTABLISHED ✓

Jun 11, 2019

FILE DIFF

Line	Log Entry
7	log syslog informational
8	!
9	vrf vrf1
10	- vni 104001
11	!
12	interface swp51
13	ipv6 nd ra-interval 10
14	no ipv6 nd suppress-ra

### View All BGP Session Details

You can view all stored attributes of all of the BGP sessions associated with the two devices on this card.

To view all session details, open the full screen BGP Session card, and click the **All BGP Sessions** tab.

Network Services | BGP

DEFAULT TIME Past 24 Hours

5 RESULTS

All BGP Sessions

All Events

IPV4 PFX...	PEER ROU...	UPD8 TX	HOSTNAME	TIMESTAMP	PEER ASN	STATE	VRF	RX FAMILY
0	10.0.0.22	43	leaf01	9/10/19 3:17 P...	65020	Established	default	ipv4,evpn
0	10.0.0.22	43	leaf01	9/10/19 3:18 P...	65020	Established	default	ipv4,evpn
0	10.0.0.22	64	leaf01	9/10/19 3:28 ...	65020	Established	default	ipv4,evpn
0	0.0.0.0	0	leaf01	9/10/19 3:29 ...	0	NotEstd	default	
0	10.0.0.22	53	leaf01	9/10/19 3:29 ...	65020	Established	default	ipv4,evpn

To return to your workbench, click



in the top right corner.

### View All Events

You can view all of the alarm and info events for the two devices on this card.

To view all events, open the full screen BGP Session card, and click the **All Events** tab.

## Monitor the BGP Service

## Monitor a Single BGP Session

Network Services   BGP						
DEFAULT TIME Past 24 Hours		50 RESULTS				
All BGP Sessions		Export				
All Events						
SOURCE	MESSAGE	TYPE	SEVERITY	TIME		
exit02	BGP session with peer spine01 swp51 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		
leaf03	BGP session with peer spine01 swp51 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		
exit01	BGP session with peer spine01 swp51 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		
leaf01	BGP session with peer spine01 swp51 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		
leaf04	BGP session with peer spine01 swp51 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		
spine01	BGP session with peer leaf04 swp4 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		
spine01	BGP session with peer leaf01 swp1 vrf default state changed from Establishing to Established.	bgp	critical	9/12/19 7:46 PM		

To return to your workbench, click



in the top right corner.

# Monitor the EVPN Service

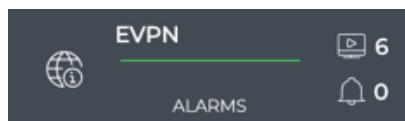
The Cumulus NetQ UI enables operators to view the health of the EVPN service on a network-wide and a per session basis, giving greater insight into all aspects of the service. This is accomplished through two card workflows, one for the service and one for the session. They are described separately here.

## Monitor the EVPN Service (All Sessions)

With NetQ, you can monitor the number of nodes running the EVPN service, view switches with the sessions, total number of VNIs, and alarms triggered by the EVPN service. For an overview and how to configure EVPN in your data center network, refer to [Ethernet Virtual Private Network-EVPN](#).

### EVPN Service Card Workflow Summary

The small EVPN Service card displays:



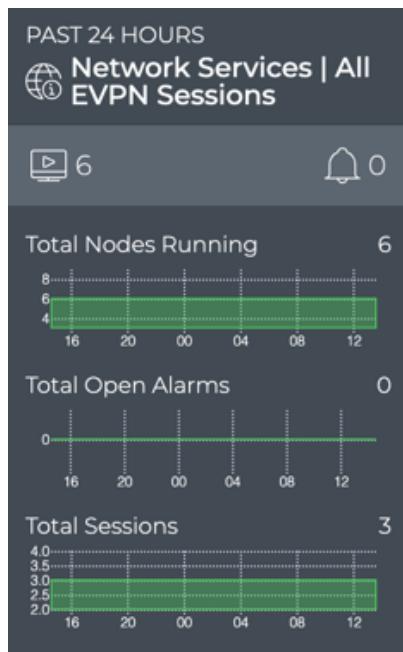
Item	Description
	Indicates data is for all sessions of a Network Service or Protocol
Title	EVPN: All EVPN Sessions, or the EVPN Service

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

Item	Description
	Total number of switches and hosts with the EVPN service enabled during the designated time period
	Total number of EVPN-related alarms received during the designated time period
Chart	Distribution of EVPN-related alarms received during the designated time period

The medium EVPN Service card displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

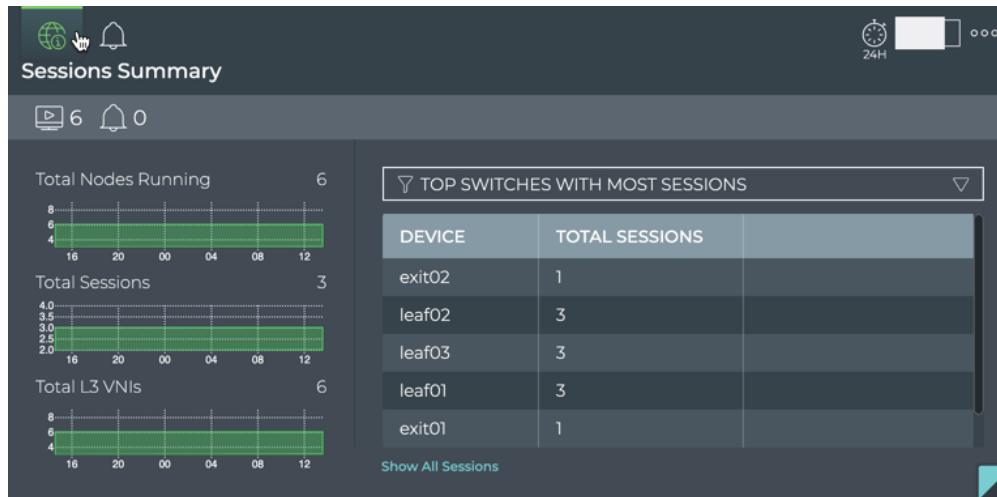
Item	Description
Title	Network Services   All EVPN Sessions
	Total number of switches and hosts with the EVPN service enabled during the designated time period
	Total number of EVPN-related alarms received during the designated time period
Total Nodes Running chart	<p>Distribution of switches and hosts with the EVPN service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running EVPN last week or last month might be more or less than the number of nodes running EVPN currently.</p>
Total Open Alarms chart	<p>Distribution of EVPN-related alarms received during the designated time period, and the total number of current EVPN-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Total Sessions chart	Distribution of EVPN sessions during the designated time period, and the total number of sessions running on the network currently.

The large EVPN service card contains two tabs.

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

The *Sessions Summary* tab which displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	Sessions Summary (visible when you hover over card)
	Total number of switches and hosts with the EVPN service enabled during the designated time period
	Total number of EVPN-related alarms received during the designated time period

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

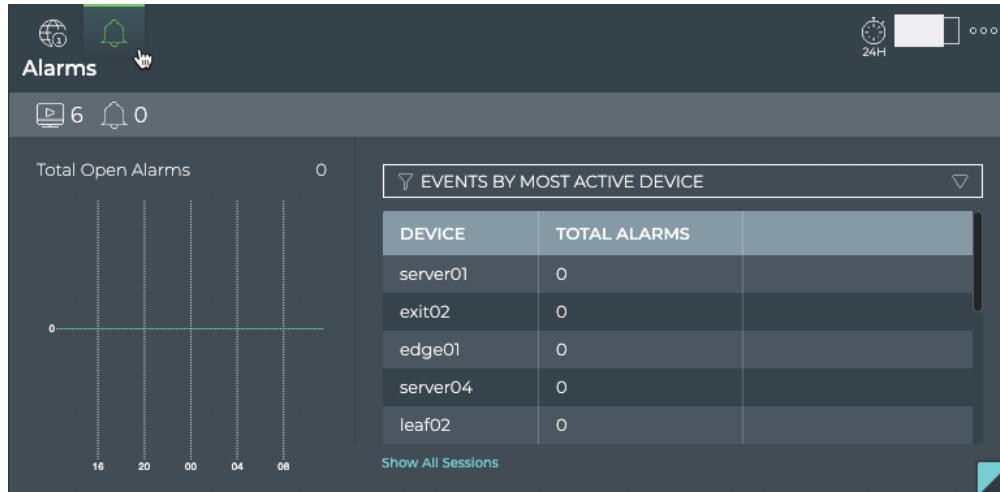
Item	Description
Total Nodes Running chart	<p>Distribution of switches and hosts with the EVPN service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running EVPN last week or last month might be more or less than the number of nodes running EVPN currently.</p>
Total Sessions chart	Distribution of EVPN sessions during the designated time period, and the total number of sessions running on the network currently.
Total L3 VNIIs chart	Distribution of layer 3 VXLAN Network Identifiers during this time period, and the total number of VNIs in the network currently.
Table/Filter options	<p>When the <b>Top Switches with Most Sessions</b> filter is selected, the table displays devices running EVPN sessions in decreasing order of session count—devices with the largest number of sessions are listed first.</p> <p>When the <b>Switches with Most L2 EVPN</b> filter is selected, the table displays devices running layer 2 EVPN sessions in decreasing order of session count—devices with the largest number of sessions are listed first.</p> <p>When the <b>Switches with Most L3 EVPN</b> filter is selected, the table displays devices running layer 3 EVPN sessions in decreasing order of session count—devices with the largest number of sessions are listed first.</p>

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

Item	Description
Show All Sessions	Link to view data for all EVPN sessions network-wide in the full screen card

The *Alarms* tab which displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
🔔 (in header)	Indicates data is for all alarms for all sessions of a Network Service or Protocol
Title	Alarms (visible when you hover over card)
▶	Total number of switches and hosts with the EVPN service enabled during the designated time period

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

Item	Description
 (in summary bar)	Total number of EVPN-related alarms received during the designated time period
Total Alarms chart	<p>Distribution of EVPN-related alarms received during the designated time period, and the total number of current BGP-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Table/Filter options	When the <b>Events by Most Active Device</b> filter is selected, the table displays devices running EVPN sessions in decreasing order of alarm count—devices with the largest number of alarms are listed first
Show All Sessions	Link to view data for all EVPN sessions in the full screen card

The full screen EVPN Service card provides tabs for all switches, all sessions, all alarms.



The screenshot shows a table titled "Network Services | EVPN" with the following data:

HOSTNAME	TIME	ASIC MOD..	AGENT VE..	OS VERSL..	LICENSE S..	DISK TOTA..	OS VERSI..	PLATFOR..
exit01	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

Item	Description
Title	Network Services   EVPN
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

All Switches tab	<p>Displays all switches and hosts running the EVPN service. By default, the device list is sorted by <b>hostname</b>. This tab provides the following additional data about each device:</p> <ul style="list-style-type: none"><li>• <b>Agent</b><ul style="list-style-type: none"><li>◦ State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).</li><li>◦ Version: Software version number of the NetQ Agent on a given device. This should match the version number of the NetQ software loaded on your server or appliance; for example, 2.1.0.</li></ul></li><li>• <b>ASIC</b><ul style="list-style-type: none"><li>◦ Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.</li><li>◦ Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.</li><li>◦ Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.</li><li>◦ Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.</li><li>◦ Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.</li></ul></li><li>• <b>CPU</b><ul style="list-style-type: none"><li>◦ Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.</li><li>◦ Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.</li><li>◦ Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.</li><li>◦ Nos: Number of cores. Example values include 2, 4, and 8.</li></ul></li><li>• <b>Disk Total Size:</b> Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.</li><li>• <b>License State:</b> Indicator of validity. Values include ok and bad.</li><li>• <b>Memory Size:</b> Total amount of local RAM. Example values include 8192 MB and 2048 MB.</li><li>• <b>OS</b></li></ul>
------------------------	---

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

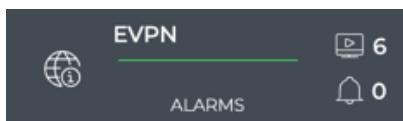
Item	Description
All Sessions tab	<p>Displays all EVPN sessions network-wide. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"><li>• <b>Adv All Vni:</b> Indicates whether the VNI state is advertising all VNIs (true) or not (false)</li><li>• <b>Adv Gw Ip:</b> Indicates whether the host device is advertising the gateway IP address (true) or not (false)</li><li>• <b>DB State:</b> Session state of the DB</li><li>• <b>Export RT:</b> IP address and port of the export route target used in the filtering mechanism for BGP route exchange</li><li>• <b>Import RT:</b> IP address and port of the import route target used in the filtering mechanism for BGP route exchange</li><li>• <b>In Kernel:</b> Indicates whether the associated VNI is in the kernel (in kernel) or not (not in kernel)</li><li>• <b>Is L3:</b> Indicates whether the session is part of a layer 3 configuration (true) or not (false)</li><li>• <b>Origin Ip:</b> Host device's local VXLAN tunnel IP address for the EVPN instance</li><li>• <b>OPID:</b> LLDP service identifier</li><li>• <b>Rd:</b> Route distinguisher used in the filtering mechanism for BGP route exchange</li><li>• <b>Timestamp:</b> Date and time the session was started, deleted, updated or marked as dead (device is down)</li><li>• <b>Vni:</b> Name of the VNI where session is running</li></ul>

Item	Description
All Alarms tab	<p>Displays all EVPN events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of a EVPN-related event. Example: VNI 3 kernel state changed from down to up</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of <i>evpn</i> in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Service Status Summary

A summary of the EVPN service is available from the Network Services card workflow, including the number of nodes running the service, the number of EVPN-related alarms, and a distribution of those alarms.

To view the summary, open the small EVPN Network Service card.



For more detail, select a different size EVPN Network Service card.

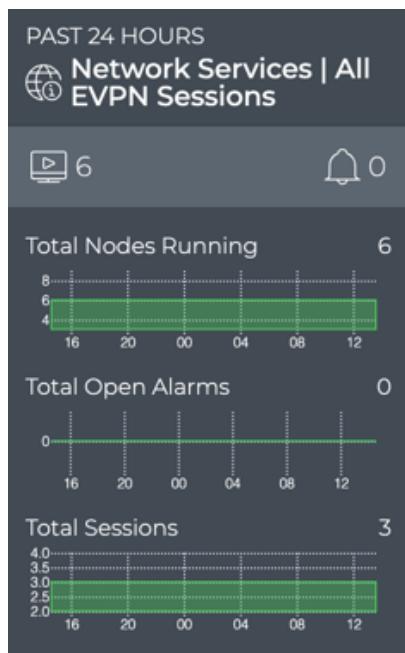
## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

### View the Distribution of Sessions and Alarms

It is useful to know the number of network nodes running the EVPN protocol over a period of time, as it gives you insight into the amount of traffic associated with and breadth of use of the protocol. It is also useful to compare the number of nodes running EVPN with the alarms present at the same time to determine if there is any correlation between the issues and the ability to establish an EVPN session.

To view these distributions, open the medium EVPN Service card.



If a visual correlation is apparent, you can dig a little deeper with the large EVPN Service card tabs.

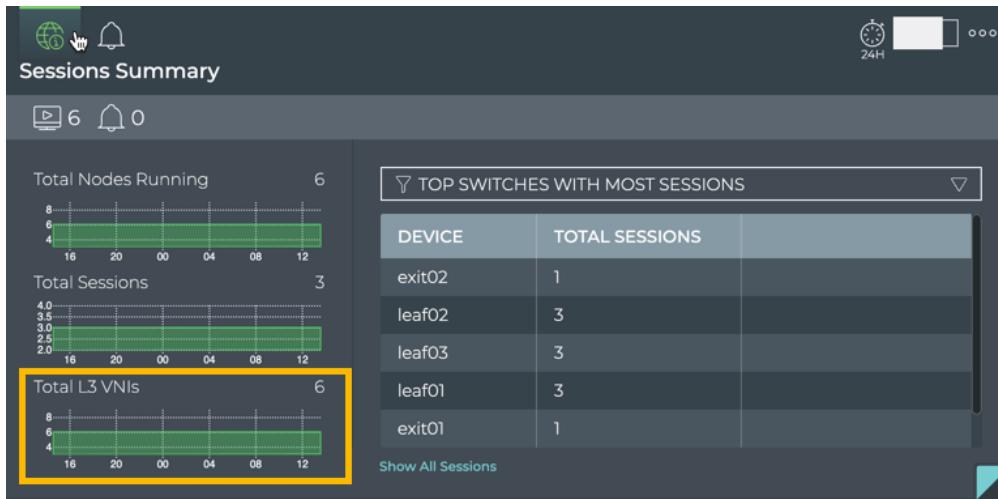
### View the Distribution of Layer 3 VNIs

It is useful to know the number of layer 3 VNIs, as it gives you insight into the complexity of the VXLAN.

To view this distribution, open the large EVPN Service card and view the bottom chart on the left.

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)



### View Devices with the Most EVPN Sessions

You can view the load from EVPN on your switches and hosts using the large EVPN Service card. This data enables you to see which switches are handling the most EVPN traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

To view switches and hosts with the most EVPN sessions:

1. Open the large EVPN Service card.
2. Select **Top Switches with Most Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most EVPN sessions at the top. Scroll down to view those with the fewest sessions.



## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

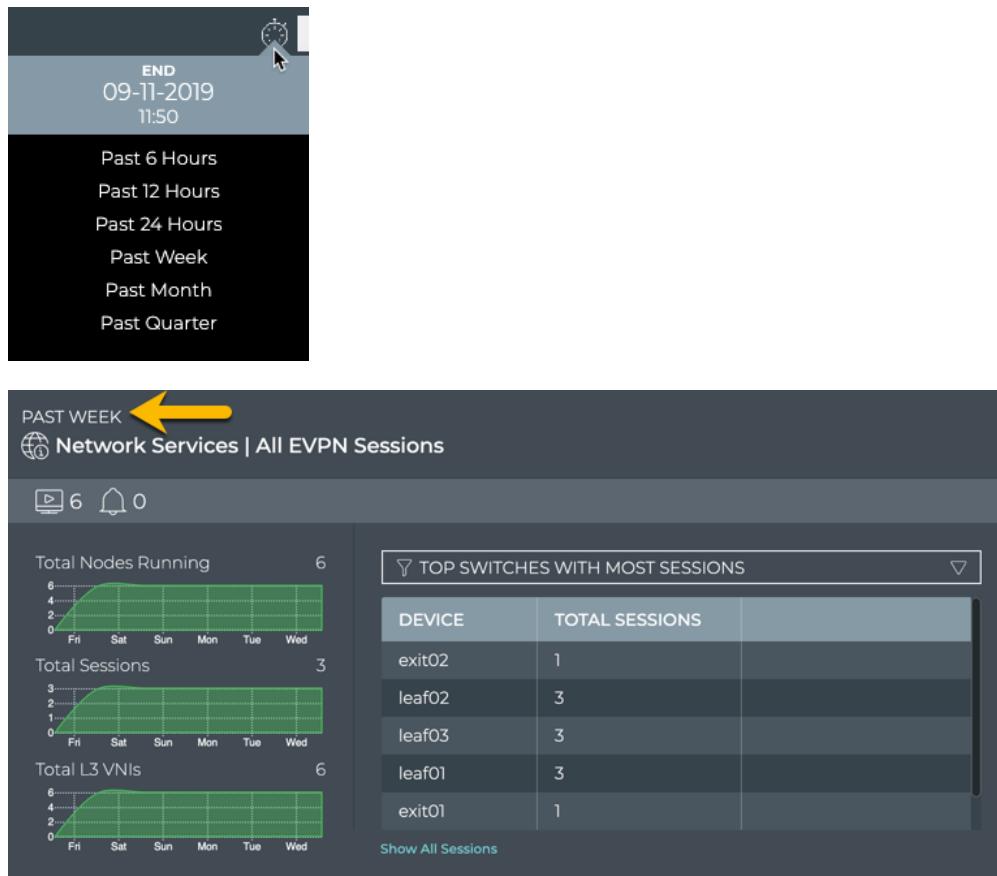
To compare this data with the same data at a previous time:

1. Open another large EVPN Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking



4. Select the time period that you want to compare with the current time.

You can now see whether there are significant differences between this time period and the previous time period.



If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running EVPN than previously, looking for changes in the topology, and so forth.

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

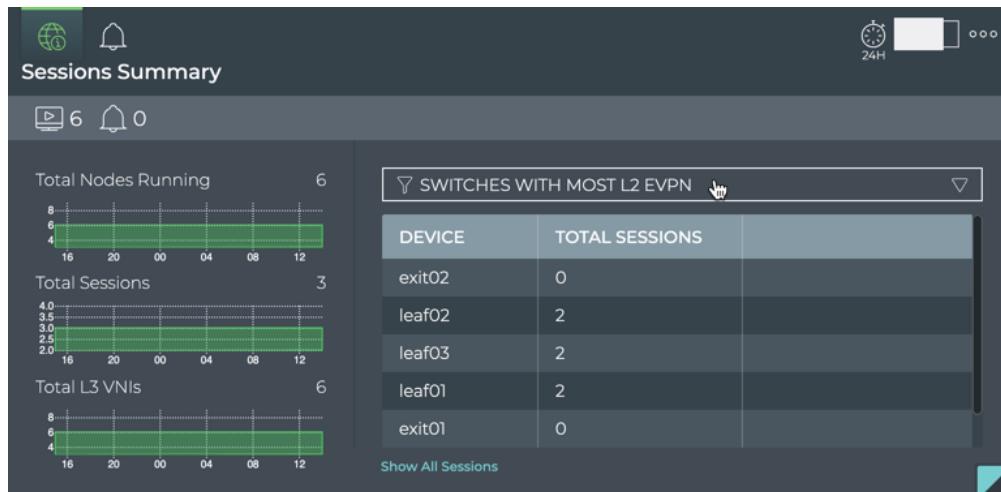
### View Devices with the Most Layer 2 EVPN Sessions

You can view the number layer 2 EVPN sessions on your switches and hosts using the large EVPN Service card. This data enables you to see which switches are handling the most EVPN traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

To view switches and hosts with the most layer 2 EVPN sessions:

1. Open the large EVPN Service card.
2. Select **Switches with Most L2 EVPN** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most layer 2 EVPN sessions at the top. Scroll down to view those with the fewest sessions.



To compare this data with the same data at a previous time:

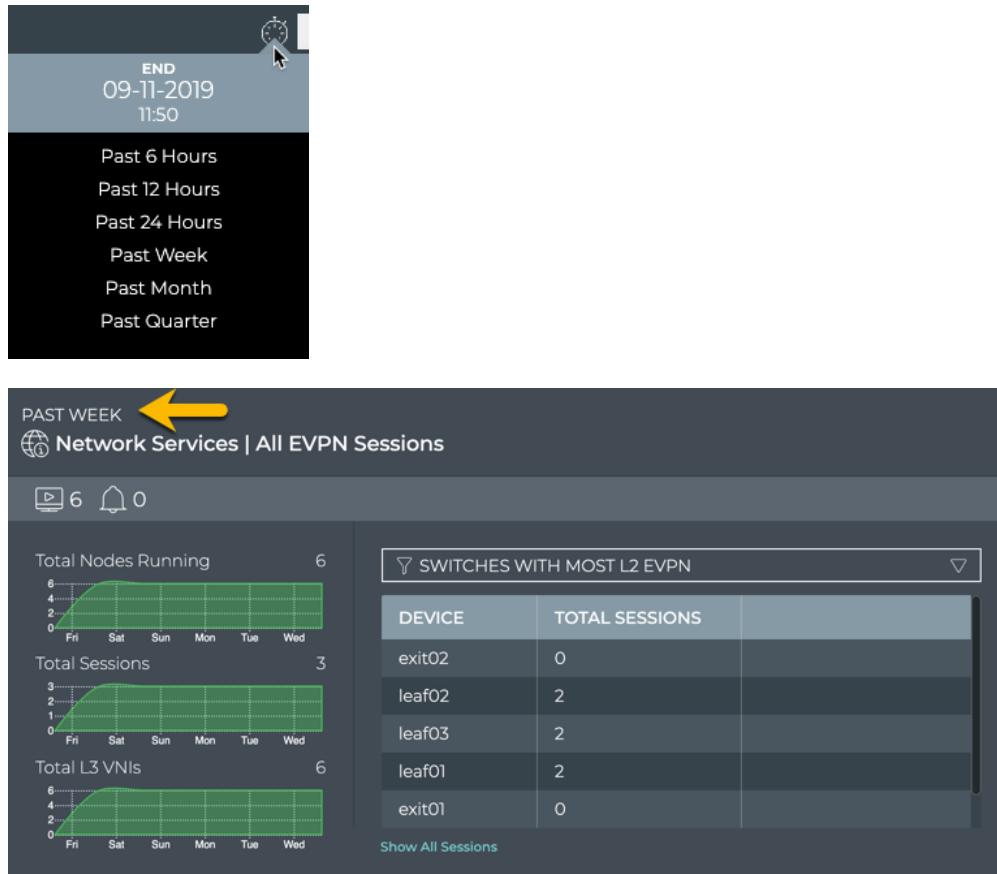
1. Open another large EVPN Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

4. Select the time period that you want to compare with the current time.

You can now see whether there are significant differences between this time period and the previous time period.



If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running EVPN than previously, looking for changes in the topology, and so forth.

### View Devices with the Most Layer 3 EVPN Sessions

You can view the number layer 3 EVPN sessions on your switches and hosts using the large EVPN Service card. This data enables you to see which switches are handling the most EVPN traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

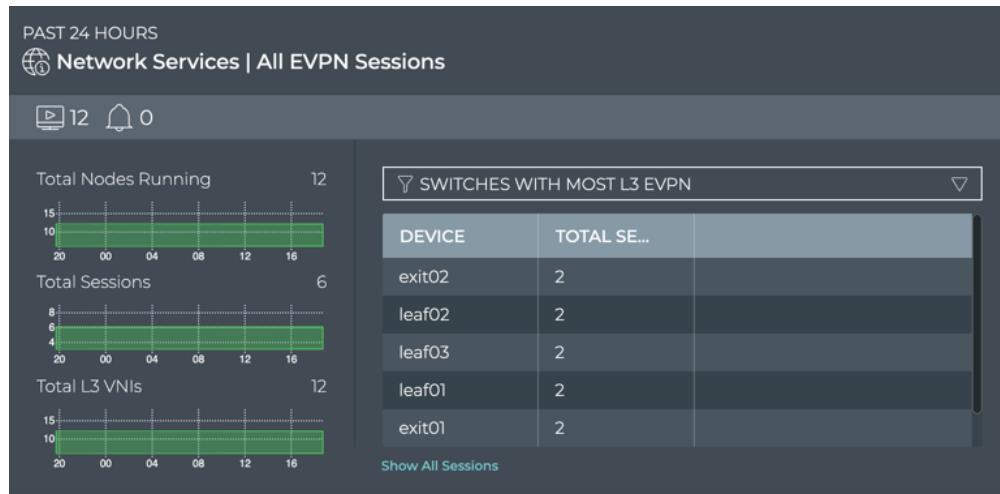
## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

To view switches and hosts with the most layer 3 EVPN sessions:

1. Open the large EVPN Service card.
2. Select **Switches with Most L3 EVPN** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most layer 3 EVPN sessions at the top. Scroll down to view those with the fewest sessions.



To compare this data with the same data at a previous time:

1. Open another large EVPN Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking

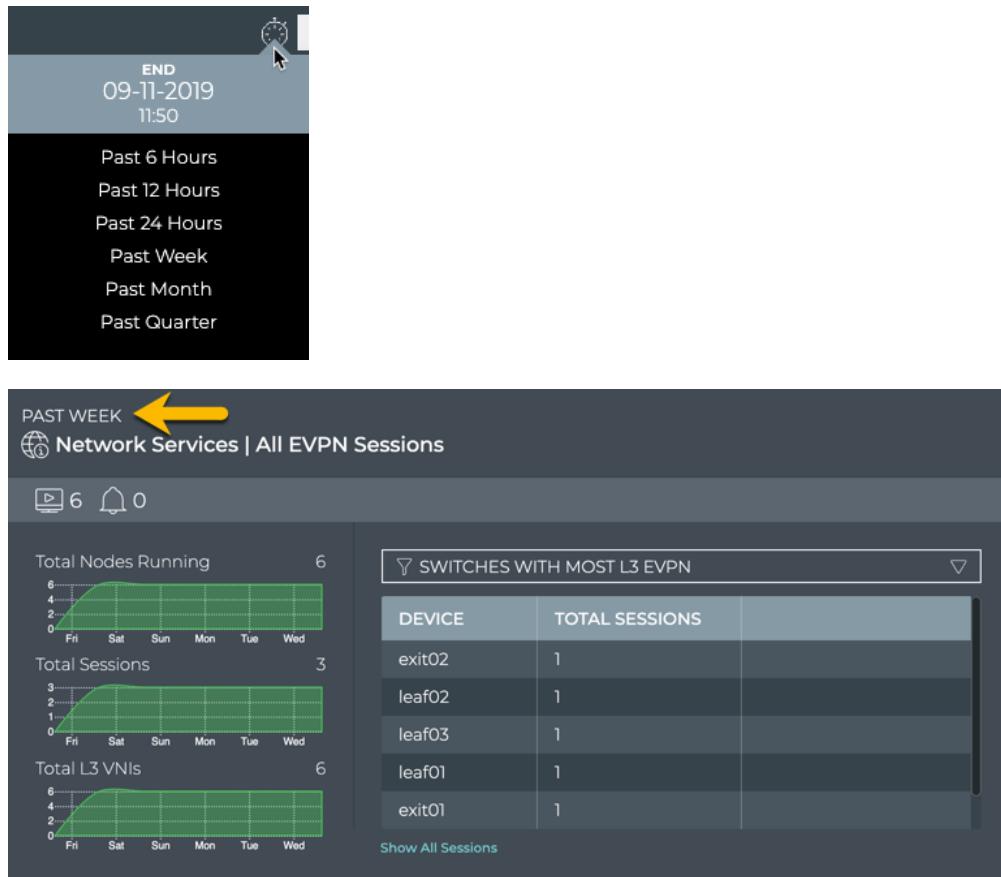


4. Select the time period that you want to compare with the current time.

You can now see whether there are significant differences between this time period and the previous time period.

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)



If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running EVPN than previously, looking for changes in the topology, and so forth.

### View Devices with the Most EVPN-related Alarms

Switches experiencing a large number of EVPN alarms may indicate a configuration or performance issue that needs further investigation. You can view the switches sorted by the number of BGP alarms and then use the Switches card workflow or the Alarms card workflow to gather more information about possible causes for the alarms.

To view switches with the most EVPN alarms:

1. Open the large EVPN Service card.
2. Hover over the header and click

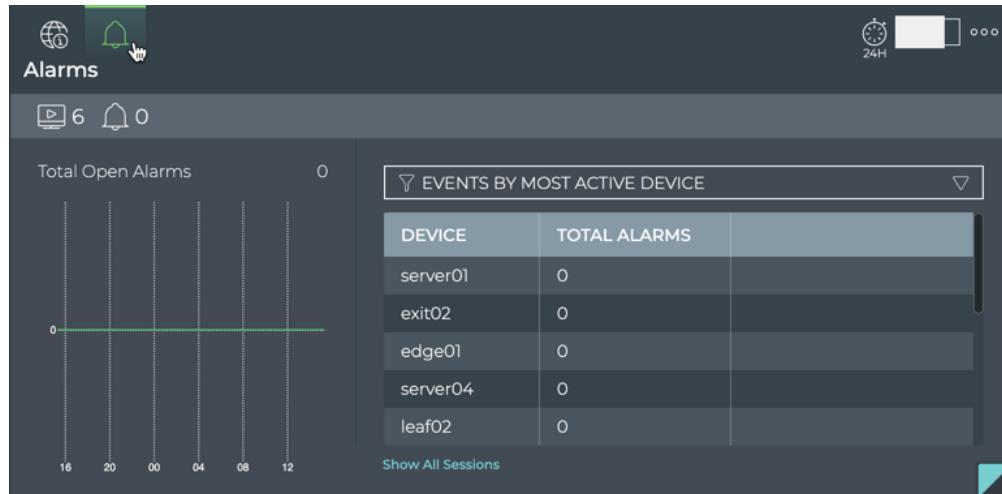


## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

3. Select **Events by Most Active Device** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most EVPN alarms at the top. Scroll down to view those with the fewest alarms.



Where to go next depends on what data you see, but a few options include:

- Hover over the Total Alarms chart to focus on the switches exhibiting alarms during that smaller time slice.  
The table content changes to match the hovered content. Click on the chart to persist the table changes.
- Change the time period for the data to compare with a prior time. If the same switches are consistently indicating the most alarms, you might want to look more carefully at those switches using the Switches card workflow.
- Click **Show All Sessions** to investigate all EVPN sessions network-wide in the full screen card.

### View All EVPN Events

The EVPN Service card workflow enables you to view all of the EVPN events in the designated time period.

To view all EVPN events:

1. Open the full screen EVPN Service card.

## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

2. Click **All Alarms** tab in the navigation panel. By default, events are sorted by Time, with most recent events listed first.

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
exit01	VNI 104001 state changed from up to down	evpn	critical	9/10/19 3:28 PM

Where to go next depends on what data you see, but a few options include:

- Open one of the other full screen tabs in this flow to focus on devices or sessions.
- Sort by the **Message** or **Severity** to narrow your focus.
- Export the data for use in another analytics tool, by selecting all or some of the events and clicking **Export**.
- Click  at the top right to return to your workbench.

## View Details for All Devices Running EVPN

You can view all stored attributes of all switches running EVPN in your network in the full screen card.

To view all switch and host details, open the full screen EVPN Service card, and click the **All Switches** tab.

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...
exit01	8/28/19 3:21 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/28/19 3:21 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/28/19 3:20 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

To return to your workbench, click .

at the top right.

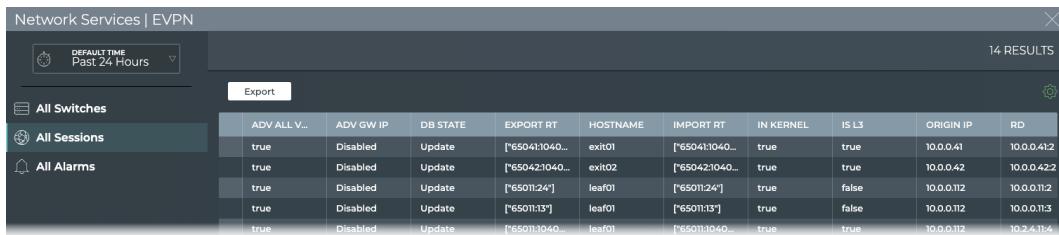
## Monitor the EVPN Service

## Monitor the EVPN Service (All Sessions)

### View Details for All EVPN Sessions

You can view all stored attributes of all EVPN sessions in your network in the full screen card.

To view all session details, open the full screen EVPN Service card, and click the **All Sessions** tab.



The screenshot shows the Network Services | EVPN card with the 'All Sessions' tab selected. The card displays a table with 14 results, each row representing an EVPN session. The columns include ADV ALL V..., ADV GW IP, DB STATE, EXPORT RT, HOSTNAME, IMPORT RT, IN KERNEL, IS L3, ORIGIN IP, and RD. The data shows various session types (e.g., exit01, leaf01) and their corresponding attributes like RD values (10.0.0.41, 10.0.0.42, etc.).

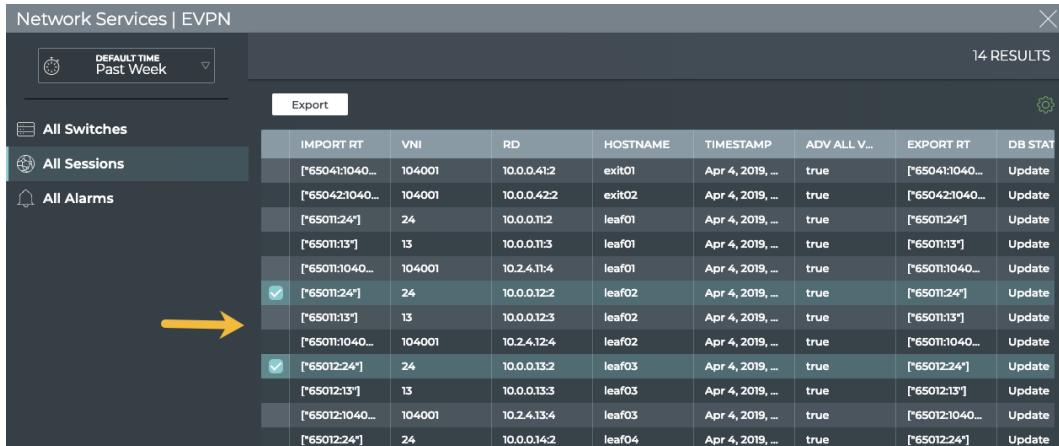
ADV ALL V...	ADV GW IP	DB STATE	EXPORT RT	HOSTNAME	IMPORT RT	IN KERNEL	IS L3	ORIGIN IP	RD
true	Disabled	Update	[*65041:1040...]	exit01	[*65041:1040...]	true	true	10.0.0.41	10.0.0.41:2
true	Disabled	Update	[*65042:1040...]	exit02	[*65042:1040...]	true	true	10.0.0.42	10.0.0.42:2
true	Disabled	Update	[*65011:24*]	leaf01	[*65011:24*]	true	false	10.0.0.112	10.0.0.112
true	Disabled	Update	[*65011:13*]	leaf01	[*65011:13*]	true	false	10.0.0.112	10.0.0.112
true	Disabled	Update	[*65011:1040...]	leaf01	[*65011:1040...]	true	true	10.0.0.112	10.2.4.1:4

To return to your workbench, click  at the top right.

### Take Actions on Data Displayed in Results List

In the full screen EVPN Service card, you can determine which results are displayed in the results list, and which are exported.

To take actions on the data, click in the blank column at the very left of a row. A checkbox appears, selecting that switch, session, or alarm, and an edit menu is shown at the bottom of the card (shown enlarged here).

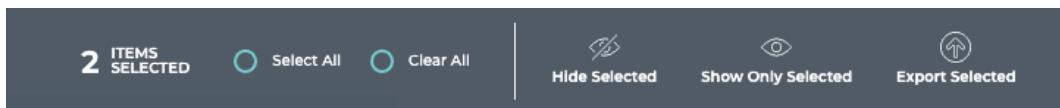


The screenshot shows the Network Services | EVPN card with the 'All Sessions' tab selected. A yellow arrow points to a row where the first column contains a checked checkbox. The card displays a table with 14 results, each row representing an EVPN session. The columns include IMPORT RT, VNI, RD, HOSTNAME, TIMESTAMP, ADV ALL V..., EXPORT RT, and DB STAT. The data shows various session types (e.g., leaf01, leaf02, leaf03) and their corresponding attributes like RD values (10.0.0.41, 10.0.0.42, etc.).

IMPORT RT	VNI	RD	HOSTNAME	TIMESTAMP	ADV ALL V...	EXPORT RT	DB STAT
[*65041:1040...]	104001	10.0.0.41:2	exit01	Apr 4, 2019, ...	true	[*65041:1040...]	Update
[*65042:1040...]	104001	10.0.0.42:2	exit02	Apr 4, 2019, ...	true	[*65042:1040...]	Update
[*65011:24*]	24	10.0.0.112	leaf01	Apr 4, 2019, ...	true	[*65011:24*]	Update
[*65011:13*]	13	10.0.0.113	leaf01	Apr 4, 2019, ...	true	[*65011:13*]	Update
[*65011:1040...]	104001	10.2.4.1:4	leaf01	Apr 4, 2019, ...	true	[*65011:1040...]	Update
<input checked="" type="checkbox"/> [*65011:24*]	24	10.0.0.12:2	leaf02	Apr 4, 2019, ...	true	[*65011:24*]	Update
[*65011:13*]	13	10.0.0.123	leaf02	Apr 4, 2019, ...	true	[*65011:13*]	Update
[*65011:1040...]	104001	10.2.4.12:4	leaf02	Apr 4, 2019, ...	true	[*65011:1040...]	Update
<input checked="" type="checkbox"/> [*65012:24*]	24	10.0.0.13:2	leaf03	Apr 4, 2019, ...	true	[*65012:24*]	Update
[*65012:13*]	13	10.0.0.13:3	leaf03	Apr 4, 2019, ...	true	[*65012:13*]	Update
[*65012:1040...]	104001	10.2.4.13:4	leaf03	Apr 4, 2019, ...	true	[*65012:1040...]	Update
[*65012:24*]	24	10.0.0.14:2	leaf04	Apr 4, 2019, ...	true	[*65012:24*]	Update

## Monitor the EVPN Service

## Monitor a Single EVPN Session



You can perform the following actions on the results list:

Option	Action or Behavior on Click
Select All	Selects all items in the results list
Clear All	Clears all existing selections of items in the results list. This also hides the edit menu.
Open Cards	Open the corresponding validation or trace result card.
Hide Selected	Hide selected items (switches, sessions, alarms, and so forth) from the results list.
Show Only Selected	Hide unselected items (switches, sessions, alarms, and so forth) from the results list.
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the <b>Export</b> button.

To return to original display of results, click the associated tab.

## Monitor a Single EVPN Session

With NetQ, you can monitor the performance of a single EVPN session, including the number of associated VNI, VTEPs and type. For an overview and how to configure EVPN in your data center network, refer to [Ethernet Virtual Private Network - EVPN](#).

**NOTE**

To access the single session cards, you must open the full screen EVPN Service, click the All Sessions tab, select the desired session, then click  (Open Cards).

### EVPN Session Card Workflow Summary

The small EVPN Session card displays:

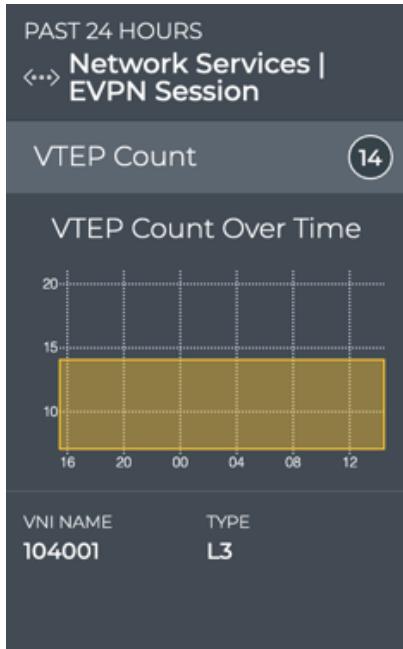


Item	Description
<::>	Indicates data is for an EVPN session
Title	EVPN Session
VNI Name	Name of the VNI (virtual network instance) used for this EVPN session
Current VNI Nodes	Total number of VNI nodes participating in the EVPN session currently

The medium EVPN Session card displays:

## Monitor the EVPN Service

## Monitor a Single EVPN Session

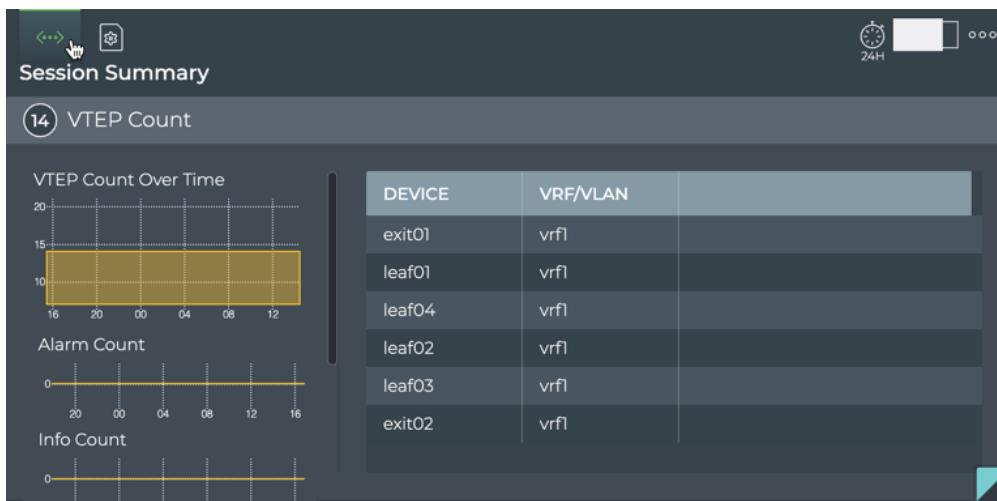


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
<::>	Indicates data is for an EVPN session
Title	Network Services   EVPN Session
Summary bar	VTEP (VXLAN Tunnel EndPoint) Count: Total number of VNI nodes participating in the EVPN session currently
VTEP Count Over Time chart	Distribution of VTEP counts during the designated time period
VNI Name	Name of the VNI used for this EVPN session

Item	Description
Type	Indicates whether the session is established as part of a layer 2 or layer 3 overlay network

The large EVPN Session card contains two tabs.

The *Session Summary* tab displays:



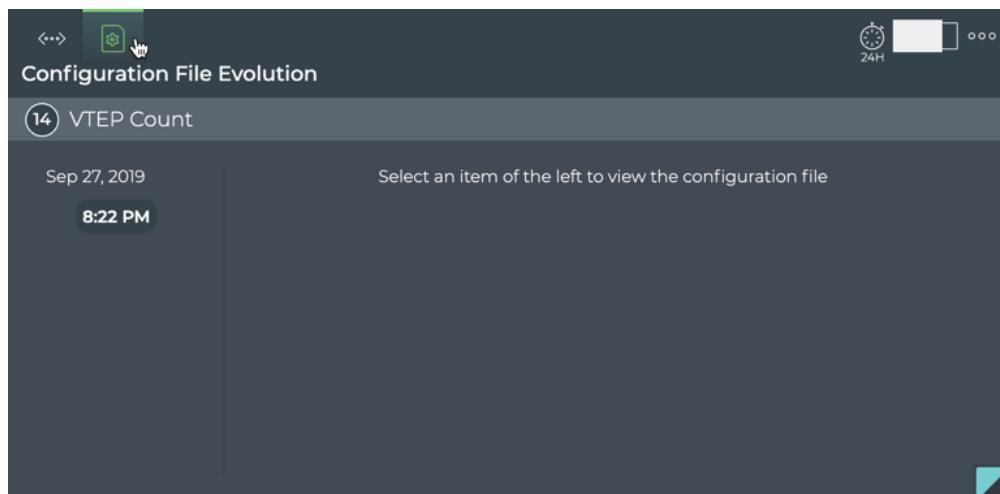
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
↔	Indicates data is for an EVPN session
Title	Session Summary (Network Services   EVPN Session)
Summary bar	VTEP (VXLAN Tunnel EndPoint) Count: Total number of VNI devices participating in the EVPN session currently

## Monitor the EVPN Service

## Monitor a Single EVPN Session

Item	Description
VTEP Count Over Time chart	Distribution of VTEPs during the designated time period
Alarm Count chart	Distribution of alarms during the designated time period
Info Count chart	Distribution of info events during the designated time period
Table	VRF (for layer 3) or VLAN (for layer 2) identifiers by device

The *Configuration File Evolution* tab displays:



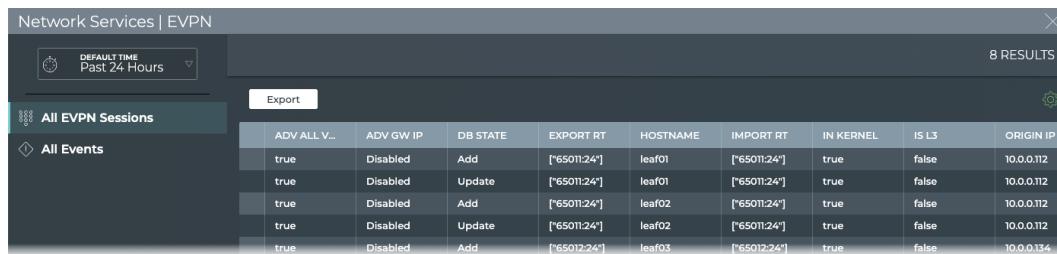
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes

## Monitor the EVPN Service

## Monitor a Single EVPN Session

Item	Description
	Indicates configuration file information for a single session of a Network Service or Protocol
Title	(Network Services   EVPN Session) Configuration File Evolution
	VTEP count (currently)
Timestamps	When changes to the configuration file have occurred, the date and time are indicated. Click the time to see the changed file.
Configuration File	<p>When <b>File</b> is selected, the configuration file as it was at the selected time is shown.</p> <p>When <b>Diff</b> is selected, the configuration file at the selected time is shown on the left and the configuration file at the previous timestamp is shown on the right. Differences are highlighted.</p> <p><b>Note:</b> If no configuration file changes have been made, only the original file date is shown.</p>

The full screen EVPN Session card provides tabs for all EVPN sessions and all events.



The screenshot shows a card titled "Network Services | EVPN". At the top, there is a dropdown menu set to "Past 24 Hours". Below the title, there are two tabs: "All EVPN Sessions" (selected) and "All Events". The main area displays a table with 8 results. The columns are: ADV ALL V..., ADV GW IP, DB STATE, EXPORT RT, HOSTNAME, IMPORT RT, IN KERNEL, IS L3, and ORIGIN IP. The data in the table is as follows:

ADV ALL V...	ADV GW IP	DB STATE	EXPORT RT	HOSTNAME	IMPORT RT	IN KERNEL	IS L3	ORIGIN IP
true	Disabled	Add	[*65011:24*]	leaf01	[*65011:24*]	true	false	10.0.0.112
true	Disabled	Update	[*65011:24*]	leaf01	[*65011:24*]	true	false	10.0.0.112
true	Disabled	Add	[*65011:24*]	leaf02	[*65011:24*]	true	false	10.0.0.112
true	Disabled	Update	[*65011:24*]	leaf02	[*65011:24*]	true	false	10.0.0.112
true	Disabled	Add	[*65012:24*]	leaf03	[*65012:24*]	true	false	10.0.0.134

Item	Description
Title	Network Services   EVPN

Item	Description
X	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab
All EVPN Sessions tab	<p>Displays all EVPN sessions network-wide. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"> <li>• <b>Adv All Vni:</b> Indicates whether the VNI state is advertising all VNIs (true) or not (false)</li> <li>• <b>Adv Gw Ip:</b> Indicates whether the host device is advertising the gateway IP address (true) or not (false)</li> <li>• <b>DB State:</b> Session state of the DB</li> <li>• <b>Export RT:</b> IP address and port of the export route target used in the filtering mechanism for BGP route exchange</li> <li>• <b>Import RT:</b> IP address and port of the import route target used in the filtering mechanism for BGP route exchange</li> <li>• <b>In Kernel:</b> Indicates whether the associated VNI is in the kernel (in kernel) or not (not in kernel)</li> <li>• <b>Is L3:</b> Indicates whether the session is part of a layer 3 configuration (true) or not (false)</li> <li>• <b>Origin Ip:</b> Host device's local VXLAN tunnel IP address for the EVPN instance</li> <li>• <b>OPID:</b> LLDP service identifier</li> <li>• <b>Rd:</b> Route distinguisher used in the filtering mechanism for BGP route exchange</li> <li>• <b>Timestamp:</b> Date and time the session was started, deleted, updated or marked as dead (device is down)</li> <li>• <b>Vni:</b> Name of the VNI where session is running</li> </ul>

Item	Description
All Events tab	<p>Displays all events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of a EVPN-related event. Example: VNI 3 kernel state changed from down to up</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of <i>evpn</i> in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Session Status Summary

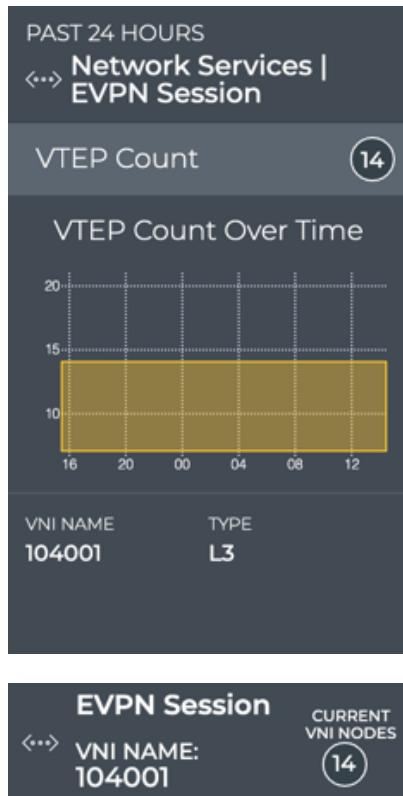
A summary of the EVPN session is available from the EVPN Session card workflow, showing the node and its peer and current status.

To view the summary:

1. Add the Network Services | All EVPN Sessions card.
2. Switch to the full screen card.
3. Click the **All Sessions** tab.
4. Double-click the session of interest. The full screen card closes automatically.
5. Optionally, switch to the small EVPN Session card.

## Monitor the EVPN Service

## Monitor a Single EVPN Session



For more detail, select a different size EVPN Session card.

### View VTEP Count

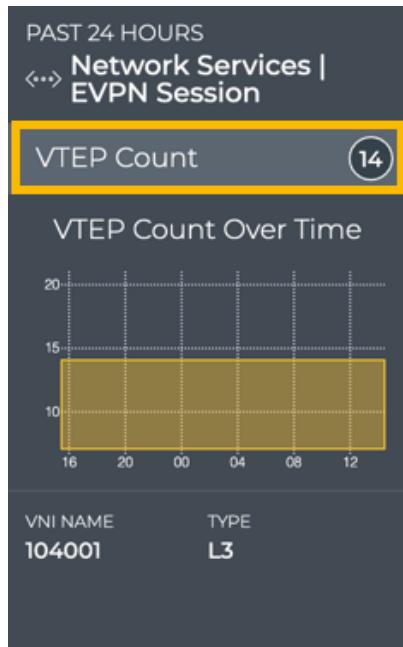
You can view the count of VTEPs for a given EVPN session from the medium and large EVPN Session cards.

To view the count for a given EVPN session, on the *medium* EVPN Session card:

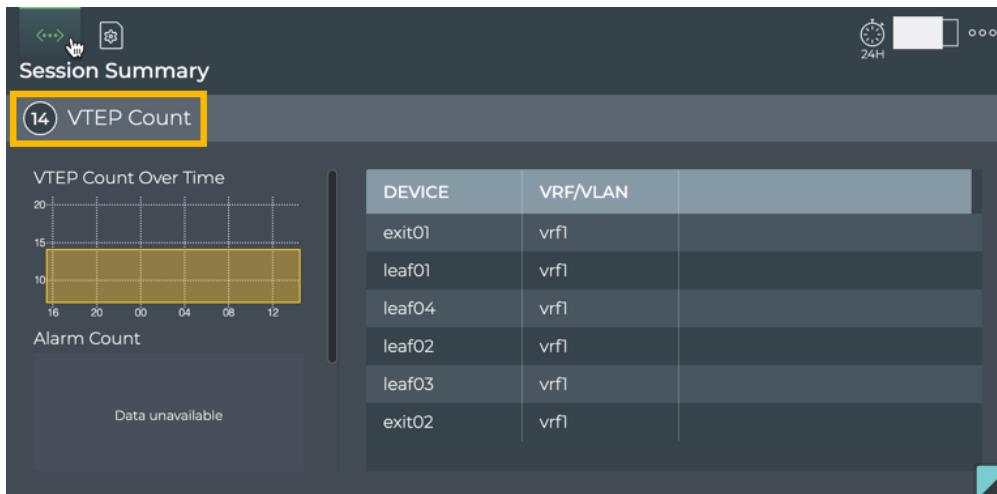
1. Add the Network Services | All EVPN Sessions card.
2. Switch to the full screen card.
3. Click the **All Sessions** tab.
4. Double-click the session of interest. The full screen card closes automatically.

## Monitor the EVPN Service

## Monitor a Single EVPN Session



To view the count for a given EVPN session on the *large* EVPN Session card, follow the same steps as for the medium card and then switch to the large card.



## View All EVPN Session Details

You can view all stored attributes of all of the EVPN sessions running network-wide.

To view all session details, open the full screen EVPN Session card and click the **All EVPN Sessions** tab.

## Monitor the EVPN Service

## Monitor a Single EVPN Session

The screenshot shows a card titled "Network Services | EVPN". At the top left is a time filter set to "Past 24 Hours". On the right, it says "8 RESULTS". Below the title is a section titled "All EVPN Sessions" with a sub-section "All Events". A table follows, with columns: ADV ALL V..., ADV GW IP, DB STATE, EXPORT RT, HOSTNAME, IMPORT RT, IN KERNEL, IS L3, and ORIGIN IP. The data in the table is as follows:

ADV ALL V...	ADV GW IP	DB STATE	EXPORT RT	HOSTNAME	IMPORT RT	IN KERNEL	IS L3	ORIGIN IP
true	Disabled	Add	[“65011:24”]	leaf01	[“65011:24”]	true	false	10.0.0.112
true	Disabled	Update	[“65011:24”]	leaf01	[“65011:24”]	true	false	10.0.0.112
true	Disabled	Add	[“65011:24”]	leaf02	[“65011:24”]	true	false	10.0.0.112
true	Disabled	Update	[“65011:24”]	leaf02	[“65011:24”]	true	false	10.0.0.112
true	Disabled	Add	[“65012:24”]	leaf03	[“65012:24”]	true	false	10.0.0.134

To return to your workbench, click



in the top right of the card.

### View All Events

You can view all of the alarm and info events occurring network wide.

To view all events, open the full screen EVPN Session card and click the **All Events** tab.

The screenshot shows a card titled "Network Services | EVPN". At the top left is a time filter set to "Past 24 Hours". On the right, it says "34 RESULTS". Below the title is a section titled "All EVPN Sessions" with a sub-section "All Events". A table follows, with columns: SOURCE, TIME, TYPE, MESSAGE, and SEVERITY. The data in the table is as follows:

SOURCE	TIME	TYPE	MESSAGE	SEVERITY
server04	Apr 4, 2019, 5:49 pm	services	Service syslog status changed from active to inactive	critical
server02	Apr 4, 2019, 5:35 pm	services	Service syslog status changed from active to inactive	critical
server02	Apr 4, 2019, 4:16 pm	link	HostName server02 changed state from up to down Interface:eth2	critical
server02	Apr 4, 2019, 4:16 pm	link	HostName server02 changed state from up to down Interface:eth1	critical
server01	Apr 4, 2019, 4:16 pm	link	HostName server01 changed state from up to down Interface:eth2	critical
server04	Apr 4, 2019, 4:16 pm	link	HostName server04 changed state from up to down Interface:eth2	critical
server01	Apr 4, 2019, 4:16 pm	link	HostName server01 changed state from up to down Interface:eth1	critical
server04	Apr 4, 2019, 4:16 pm	link	HostName server04 changed state from up to down Interface:eth1	critical

Where to go next depends on what data you see, but a few options include:

- Open one of the other full screen tabs in this flow to focus on sessions.
- Sort by the **Message** or **Severity** to narrow your focus.
- Export the data for use in another analytics tool, by selecting all or some of the events and clicking **Export**.
- Click



at the top right to return to your workbench.

# Monitor the LLDP Service

The Cumulus NetQ UI enables operators to view the health of the LLDP service on a network-wide and a per session basis, giving greater insight into all aspects of the service. This is accomplished through two card workflows, one for the service and one for the session. They are described separately here.

## Monitor the LLDP Service (All Sessions)

With NetQ, you can monitor the number of nodes running the LLDP service, view nodes with the most LLDP neighbor nodes, those nodes with the least neighbor nodes, and view alarms triggered by the LLDP service. For an overview and how to configure LLDP in your data center network, refer to [Link Layer Discovery Protocol](#).

### LLDP Service Card Workflow Summary

The small LLDP Service card displays:



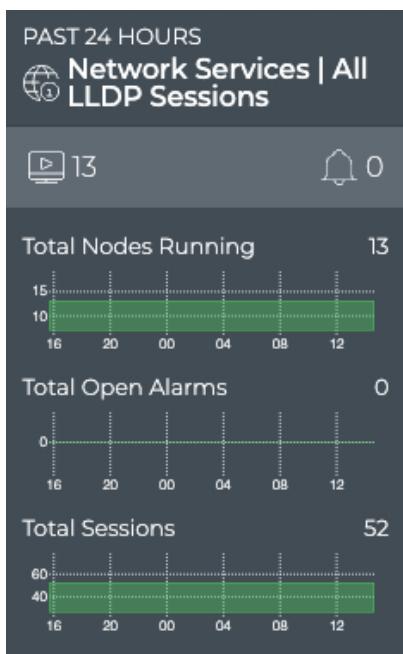
Item	Description
	Indicates data is for all sessions of a Network Service or Protocol
Title	LLDP: All LLDP Sessions, or the LLDP Service

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

Item	Description
	Total number of switches with the LLDP service enabled during the designated time period
	Total number of LLDP-related alarms received during the designated time period
Chart	Distribution of LLDP-related alarms received during the designated time period

The medium LLDP Service card displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

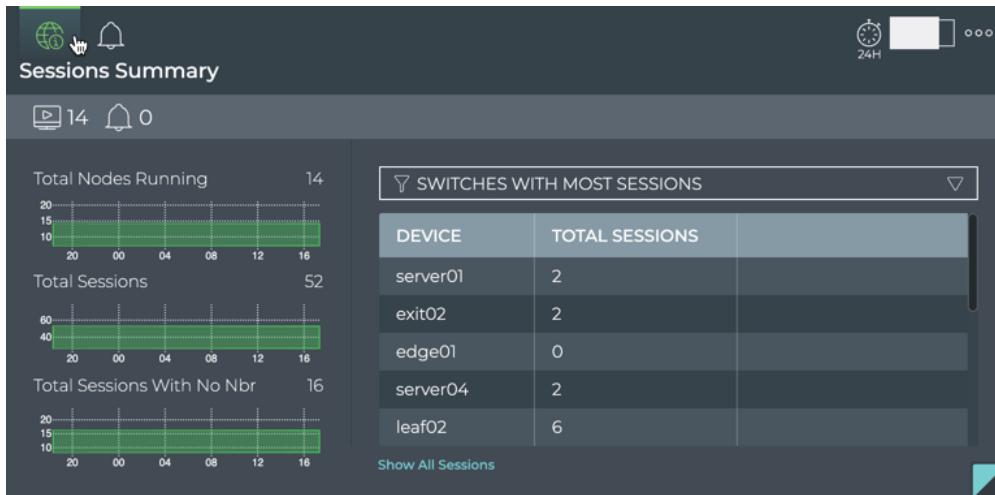
Item	Description
Title	LLDP: All LLDP Sessions, or the LLDP Service
	Total number of switches with the LLDP service enabled during the designated time period
	Total number of LLDP-related alarms received during the designated time period
Total Nodes Running chart	<p>Distribution of switches and hosts with the LLDP service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running LLDP last week or last month might be more or less than the number of nodes running LLDP currently.</p>
Total Open Alarms chart	<p>Distribution of LLDP-related alarms received during the designated time period, and the total number of current LLDP-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Total Sessions chart	Distribution of LLDP sessions running during the designated time period, and the total number of sessions running on the network currently.

The large LLDP service card contains two tabs.

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

The *Sessions Summary* tab which displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	Sessions Summary (Network Services   All LLDP Sessions)
	Total number of switches with the LLDP service enabled during the designated time period
	Total number of LLDP-related alarms received during the designated time period

## Monitor the LLDP Service

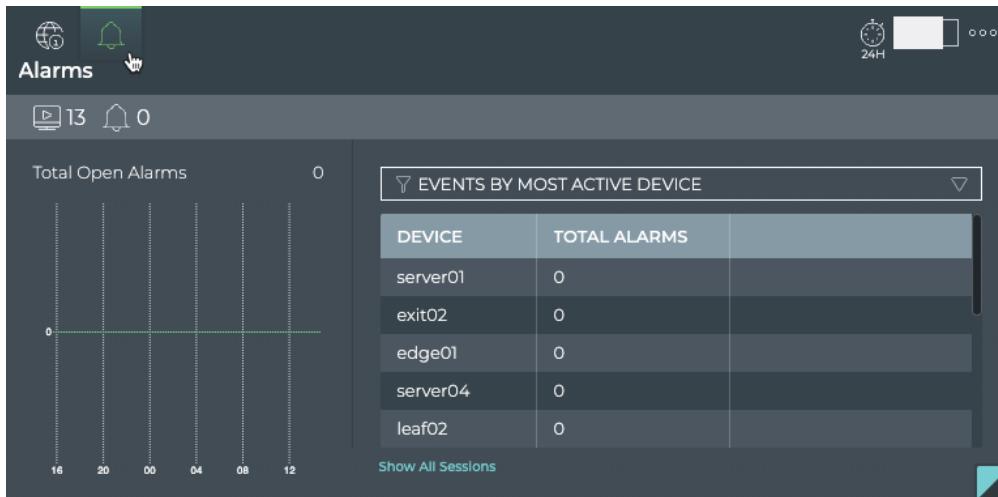
## Monitor the LLDP Service (All Sessions)

Item	Description
Total Nodes Running chart	<p>Distribution of switches and hosts with the LLDP service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running LLDP last week or last month might be more or less than the number of nodes running LLDP currently.</p>
Total Sessions chart	Distribution of LLDP sessions running during the designated time period, and the total number of sessions running on the network currently
Total Sessions with No Nbr chart	Distribution of LLDP sessions missing neighbor information during the designated time period, and the total number of session missing neighbors in the network currently
Table/Filter options	<p>When the <b>Switches with Most Sessions</b> filter is selected, the table displays switches running LLDP sessions in decreasing order of session count—devices with the largest number of sessions are listed first</p> <p>When the <b>Switches with Most Unestablished Sessions</b> filter is selected, the table displays switches running LLDP sessions in decreasing order of unestablished session count—devices with the largest number of unestablished sessions are listed first</p>
Show All Sessions	Link to view all LLDP sessions in the full screen card

The *Alarms* tab which displays:

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
(in header)	Indicates data is all alarms for all LLDP sessions
Title	Alarms (visible when you hover over card)
	Total number of switches with the LLDP service enabled during the designated time period
(in summary bar)	Total number of LLDP-related alarms received during the designated time period

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

Item	Description
Total Alarms chart	<p>Distribution of LLDP-related alarms received during the designated time period, and the total number of current LLDP-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Table/Filter options	<p>When the <b>Events by Most Active Device</b> filter is selected, the table displays switches running LLDP sessions in decreasing order of alarm count—devices with the largest number of sessions are listed first</p>
Show All Sessions	<p>Link to view all LLDP sessions in the full screen card</p>

The full screen LLDP Service card provides tabs for all switches, all sessions, and all alarms.

The screenshot shows a table titled "Network Services | LLDP" with 8 results. The table has columns: HOSTNAME, TIME, ASIC MOD., AGENT VERSI..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., and PLATFOR... . The data rows are:

HOSTNAME	TIME	ASIC MOD.	AGENT VERSI...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...
exit01	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

Item	Description
Title	Network Services   LLDP

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

Item	Description
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

All Switches tab	<p>Displays all switches and hosts running the EVPN service. By default, the device list is sorted by <b>hostname</b>. This tab provides the following additional data about each device:</p> <ul style="list-style-type: none"><li>• <b>Agent</b><ul style="list-style-type: none"><li>◦ State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).</li><li>◦ Version: Software version number of the NetQ Agent on a given device. This should match the version number of the NetQ software loaded on your server or appliance; for example, 2.1.0.</li></ul></li><li>• <b>ASIC</b><ul style="list-style-type: none"><li>◦ Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.</li><li>◦ Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.</li><li>◦ Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.</li><li>◦ Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.</li><li>◦ Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.</li></ul></li><li>• <b>CPU</b><ul style="list-style-type: none"><li>◦ Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.</li><li>◦ Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.</li><li>◦ Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.</li><li>◦ Nos: Number of cores. Example values include 2, 4, and 8.</li></ul></li><li>• <b>Disk Total Size:</b> Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.</li><li>• <b>License State:</b> Indicator of validity. Values include ok and bad.</li><li>• <b>Memory Size:</b> Total amount of local RAM. Example values include 8192 MB and 2048 MB.</li><li>• <b>OS</b></li></ul>
------------------------	---

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

Item	Description
All Sessions tab	<p>Displays all EVPN sessions network-wide. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"><li>• <b>Adv All Vni:</b> Indicates whether the VNI state is advertising all VNIs (true) or not (false)</li><li>• <b>Adv Gw Ip:</b> Indicates whether the host device is advertising the gateway IP address (true) or not (false)</li><li>• <b>DB State:</b> Session state of the DB</li><li>• <b>Export RT:</b> IP address and port of the export route target used in the filtering mechanism for BGP route exchange</li><li>• <b>Import RT:</b> IP address and port of the import route target used in the filtering mechanism for BGP route exchange</li><li>• <b>In Kernel:</b> Indicates whether the associated VNI is in the kernel (in kernel) or not (not in kernel)</li><li>• <b>Is L3:</b> Indicates whether the session is part of a layer 3 configuration (true) or not (false)</li><li>• <b>Origin Ip:</b> Host device's local VXLAN tunnel IP address for the EVPN instance</li><li>• <b>OPID:</b> LLDP service identifier</li><li>• <b>Rd:</b> Route distinguisher used in the filtering mechanism for BGP route exchange</li><li>• <b>Timestamp:</b> Date and time the session was started, deleted, updated or marked as dead (device is down)</li><li>• <b>Vni:</b> Name of the VNI where session is running</li></ul>

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

Item	Description
All Sessions tab	<p>Displays all LLDP sessions network-wide. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"><li>• <b>DB State:</b> Session state of the DB.</li><li>• <b>Ifname:</b> Name of the host interface where LLDP session is running</li><li>• <b>LLDP Peer:</b><ul style="list-style-type: none"><li>◦ Os: Operating system (OS) used by peer device. Values include Cumulus Linux, RedHat, Ubuntu, and CentOS.</li><li>◦ Osv: Version of the OS used by peer device. Example values include 3.7.3, 2.5.x, 16.04, 7.1.</li><li>◦ Bridge: Indicates whether the peer device is a bridge (true) or not (false)</li><li>◦ Router: Indicates whether the peer device is a router (true) or not (false)</li><li>◦ Station: Indicates whether the peer device is a station (true) or not (false)</li></ul></li><li>• <b>OPID:</b> LLDP service identifier</li><li>• <b>Peer:</b><ul style="list-style-type: none"><li>◦ Hostname: User-defined name for the peer device</li><li>◦ Ifname: Name of the peer interface where the session is running</li></ul></li><li>• <b>Timestamp:</b> Date and time that the session was started, deleted, updated, or marked dead (device is down)</li></ul>

Item	Description
All Alarms tab	<p>Displays all LLDP events network-wide. By default, the event list is sorted by time, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li><b>Message:</b> Text description of a LLDP-related event. Example: LLDP Session with host leaf02 swp6 modified fields leaf06 swp21</li> <li><b>Source:</b> Hostname of network device that generated the event</li> <li><b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li><b>Type:</b> Network protocol or service generating the event. This always has a value of <i>lldp</i> in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Service Status Summary

A summary of the LLDP service is available from the Network Services card workflow, including the number of nodes running the service, the number of LLDP-related alarms, and a distribution of those alarms.

To view the summary, open the small LLDP Service card.



In this example, there are no LLDP alarms present on the network of 14 devices.

For more detail, select a different size LLDP Network Services card.

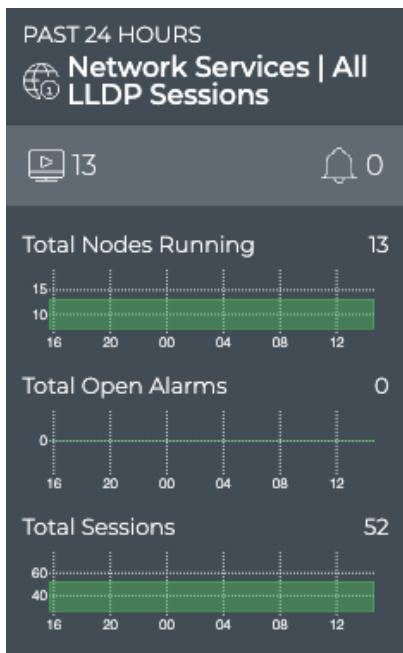
## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

### View the Distribution of Nodes, Alarms, and Sessions

It is useful to know the number of network nodes running the LLDP protocol over a period of time, as it gives you insight into nodes that might be misconfigured or experiencing communication issues. Additionally, if there are a large number of alarms, it is worth investigating either the service or particular devices.

To view the distribution, open the medium LLDP Service card.



In this example, we see that 13 nodes are running the LLDP protocol, that there are 52 sessions established, and that no LLDP-related alarms have occurred in the last 24 hours.

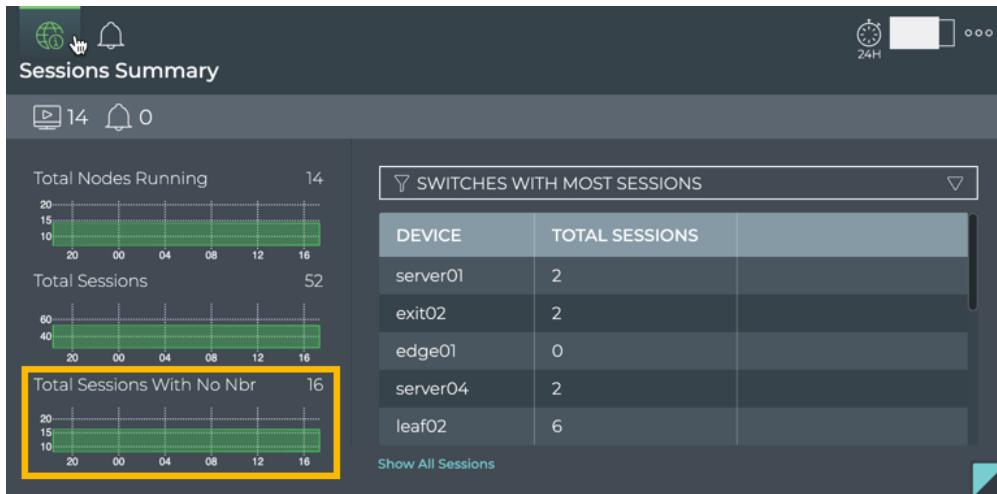
### View the Distribution of Missing Neighbors

You can view the number of missing neighbors in any given time period and how that number has changed over time. This is a good indicator of link communication issues.

To view the distribution, open the large LLDP Service card and view the bottom chart on the left, **Total Sessions with No Nbr**.

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)



In this example, we see that 16 of the 52 sessions are missing the neighbor (peer) device.

### View Devices with the Most LLDP Sessions

You can view the load from LLDP on your switches using the large LLDP Service card.

This data enables you to see which switches are handling the most LLDP traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

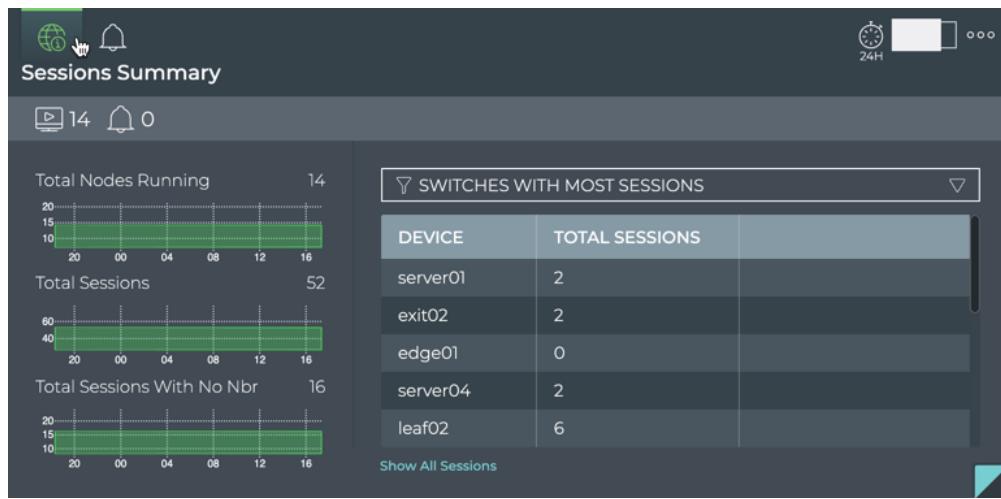
To view switches and hosts with the most LLDP sessions:

1. Open the large LLDP Service card.
2. Select **Switches with Most Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most LLDP sessions at the top. Scroll down to view those with the fewest sessions.

## Monitor the LLDP Service

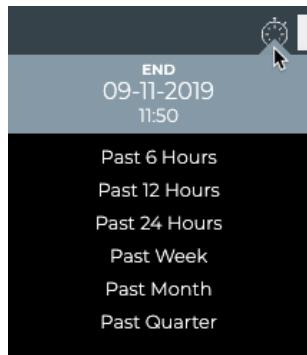
## Monitor the LLDP Service (All Sessions)



To compare this data with the same data at a previous time:

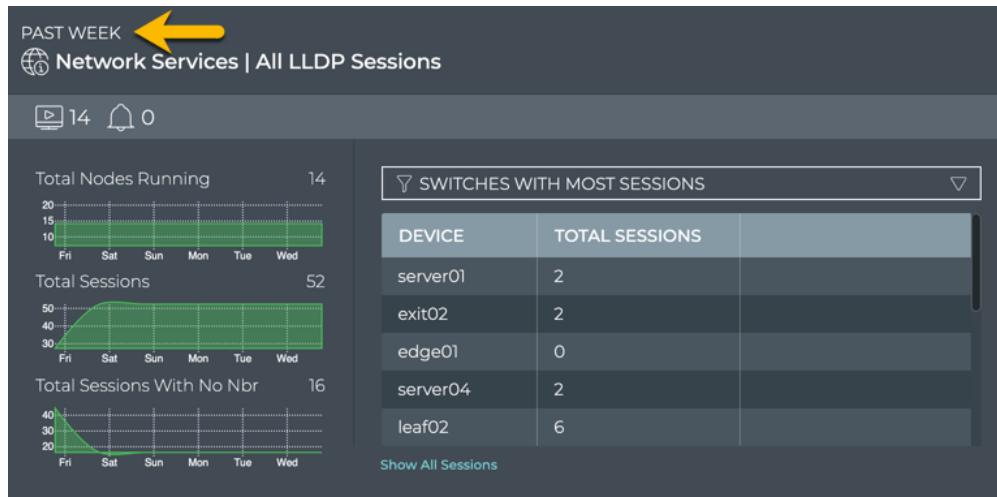
1. Open another large LLDP Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking
4. Select the time period that you want to compare with the current time.

You can now see whether there are significant differences between this time period and the previous time period.



## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)



In this case, notice that the alarms have reduced significantly in the last week. If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running LLDP than previously, looking for changes in the topology, and so forth.

### View Devices with the Most Unestablished LLDP Sessions

You can identify switches that are experiencing difficulties establishing LLDP sessions; both currently and in the past.

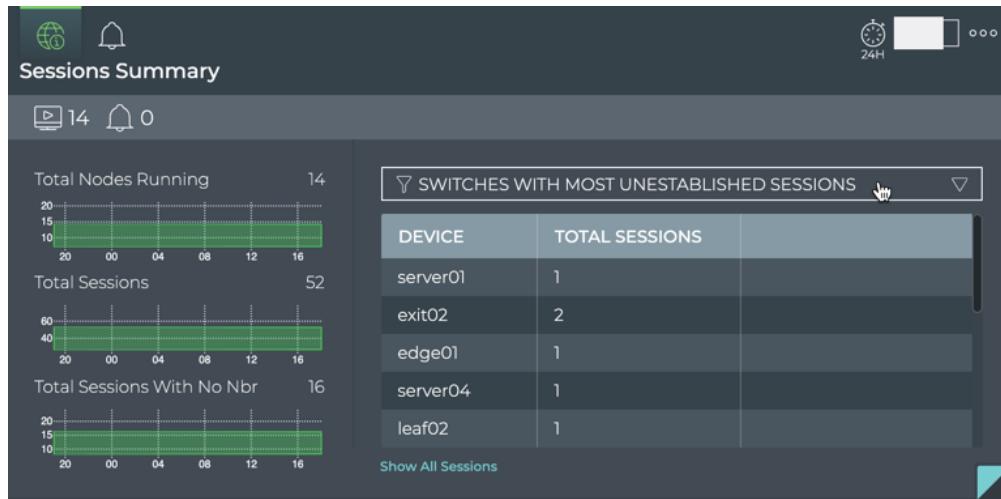
To view switches with the most unestablished LLDP sessions:

1. Open the large LLDP Service card.
2. Select **Switches with Most Unestablished Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most unestablished CLAG sessions at the top. Scroll down to view those with the fewest unestablished sessions.

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)



Where to go next depends on what data you see, but a few options include:

- Change the time period for the data to compare with a prior time.

If the same switches are consistently indicating the most unestablished sessions, you might want to look more carefully at those switches using the Switches card workflow to determine probable causes. Refer to [Monitor Switches](#).

- Click **Show All Sessions** to investigate all LLDP sessions with events in the full screen card.

### View Switches with the Most LLDP-related Alarms

Switches experiencing a large number of LLDP alarms may indicate a configuration or performance issue that needs further investigation. You can view the switches sorted by the number of LLDP alarms and then use the Switches card workflow or the Alarms card workflow to gather more information about possible causes for the alarms.

To view switches with most LLDP alarms:

1. Open the large LLDP Service card.
2. Hover over the header and click

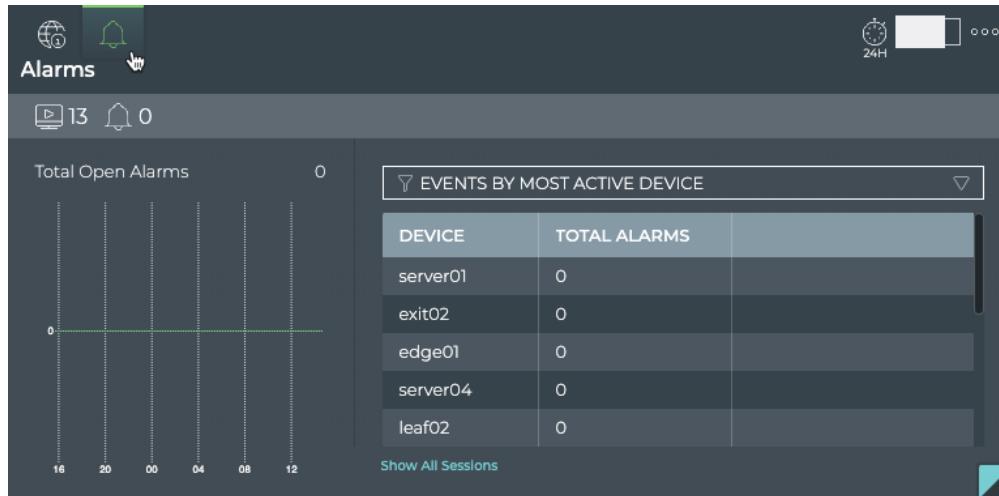


## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

3. Select **Events by Most Active Device** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most BGP alarms at the top. Scroll down to view those with the fewest alarms.



Where to go next depends on what data you see, but a few options include:

- Hover over the Total Alarms chart to focus on the switches exhibiting alarms during that smaller time slice.  
The table content changes to match the hovered content. Click on the chart to persist the table changes.
- Change the time period for the data to compare with a prior time. If the same switches are consistently indicating the most alarms, you might want to look more carefully at those switches using the Switches card workflow.
- Click **Show All Sessions** to investigate all switches running LLDP sessions in the full screen card.

### View All LLDP Events

The LLDP Network Services card workflow enables you to view all of the LLDP events in the designated time period.

To view all LLDP events:

1. Open the full screen LLDP Service card.

## Monitor the LLDP Service

## Monitor the LLDP Service (All Sessions)

2. Click the **All Alarms** tab.

SOURCE	TIME	TYPE	MESSAGE	SEVERITY
roc-se	Mar 3, 2019, ...	lldp	LLDP Session...	info
roc-se	Mar 3, 2019, ...	lldp	LLDP Session...	info
roc-se	Mar 3, 2019, ...	lldp	LLDP Session...	info
roc-se	Mar 3, 2019, ...	lldp	LLDP Session...	info
spine-1	Mar 3, 2019, ...	lldp	LLDP Session...	info
spine-1	Mar 3, 2019, ...	lldp	LLDP Session...	info
spine-1	Mar 3, 2019, ...	lldp	LLDP Session...	info

Where to go next depends on what data you see, but a few options include:

- Open the **All Switches** or **All Sessions** tabs to look more closely at the alarms from the switch or session perspective.
- Sort on other parameters:
  - by **Message** to determine the frequency of particular events
  - by **Severity** to determine the most critical events
  - by **Time** to find events that may have occurred at a particular time to try to correlate them with other system events
- Export data to a file
- Return to your workbench by clicking in the top right corner

### View Details About All Switches Running LLDP

You can view all stored attributes of all switches running LLDP in your network in the full screen card.

To view all switch details, open the LLDP Service card, and click the **All Switches** tab.

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...
exit01	8/28/19 3:21 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/28/19 3:21 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/28/19 3:20 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 ...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

## Monitor the LLDP Service

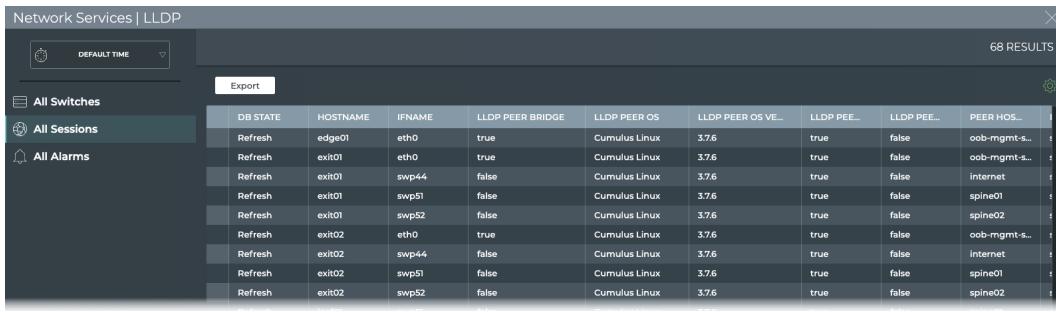
## Monitor the LLDP Service (All Sessions)

Return to your workbench by clicking  in the top right corner.

### View Detailed Information About All LLDP Sessions

You can view all stored attributes of all LLDP sessions in your network in the full screen card.

To view all session details, open the LLDP Service card, and click the **All Sessions** tab.



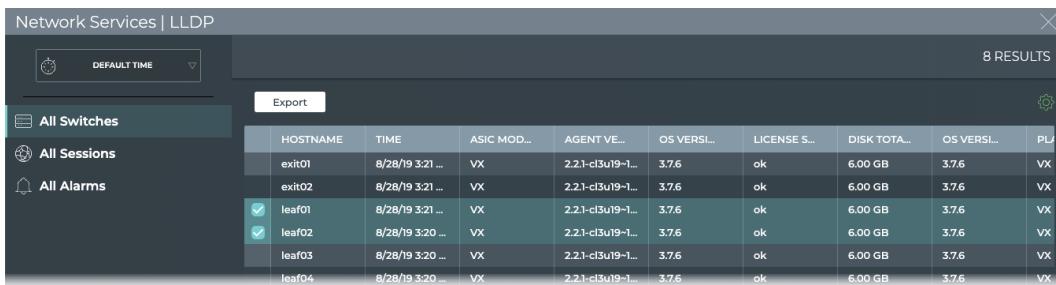
DB STATE	HOSTNAME	IFNAME	LLDP PEER BRIDGE	LLDP PEER OS	LLDP PEER OS VE...	LLDP PEE...	LLDP PEE...	PEER HOS...
Refresh	edge01	eth0	true	Cumulus Linux	3.7.6	true	false	oob-mgmt-s...
Refresh	exit01	eth0	true	Cumulus Linux	3.7.6	true	false	oob-mgmt-s...
Refresh	exit01	swp44	false	Cumulus Linux	3.7.6	true	false	internet
Refresh	exit01	swp51	false	Cumulus Linux	3.7.6	true	false	spine01
Refresh	exit01	swp52	false	Cumulus Linux	3.7.6	true	false	spine02
Refresh	exit02	eth0	true	Cumulus Linux	3.7.6	true	false	oob-mgmt-s...
Refresh	exit02	swp44	false	Cumulus Linux	3.7.6	true	false	internet
Refresh	exit02	swp51	false	Cumulus Linux	3.7.6	true	false	spine01
Refresh	exit02	swp52	false	Cumulus Linux	3.7.6	true	false	spine02

Return to your workbench by clicking  in the top right corner.

### Take Actions on Data Displayed in Results List

In the full screen LLDP Service card, you can determine which results are displayed in the results list, and which are exported.

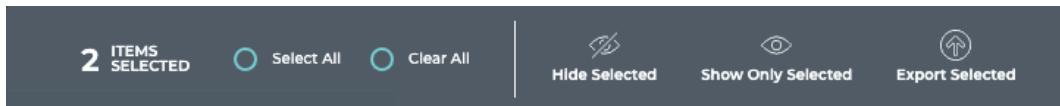
To take actions on the data, click in the blank column at the very left of a row. A checkbox appears, selecting that switch, session, or alarm, and an edit menu is shown at the bottom of the card (shown enlarged here).



HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLA...
exit01	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
<input checked="" type="checkbox"/> leaf01	8/28/19 3:21 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
<input checked="" type="checkbox"/> leaf02	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf04	8/28/19 3:20 ...	VX	2.2.1-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX

## Monitor the LLDP Service

## Monitor a Single LLDP Session



You can perform the following actions on the results list:

Option	Action or Behavior on Click
Select All	Selects all items in the results list
Clear All	Clears all existing selections of items in the results list. This also hides the edit menu.
Open Cards	Open the corresponding validation or trace result card.
Hide Selected	Hide selected items (switches, sessions, alarms, and so forth) from the results list.
Show Only Selected	Hide unselected items (switches, sessions, alarms, and so forth) from the results list.
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the <b>Export</b> button.

To return to original display of results, click the associated tab.

## Monitor a Single LLDP Session

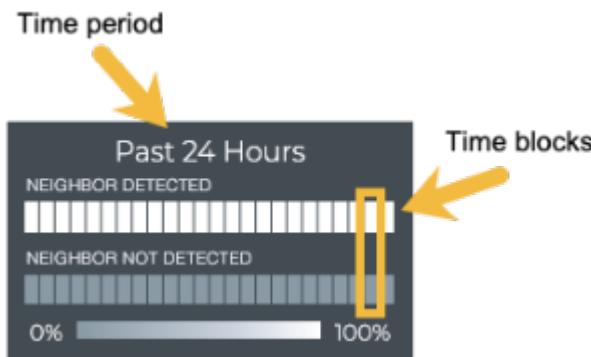
With NetQ, you can monitor the number of nodes running the LLDP service, view neighbor state changes, and compare with events occurring at the same time, as well as monitor the running LLDP configuration and changes to the configuration file. For an overview and how to configure LLDP in your data center network, refer to [Link Layer Discovery Protocol](#).

**NOTE**

To access the single session cards, you must open the full screen LLDP Service card, click the All Sessions tab, select the desired session, then click  (Open Cards).

**Granularity of Data Shown Based on Time Period**

On the medium and large single LLDP session cards, the status of the neighboring peers is represented in heat maps stacked vertically; one for peers that are reachable (neighbor detected), and one for peers that are unreachable (neighbor not detected). Depending on the time period of data on the card, the number of smaller time blocks used to indicate the status varies. A vertical stack of time blocks, one from each map, includes the results from all checks during that time. The results are shown by how saturated the color is for each block. If all peers during that time period were detected for the entire time block, then the top block is 100% saturated (white) and the neighbor not detected block is zero percent saturated (gray). As peers become reachable, the neighbor detected block increases in saturation, the peers that are unreachable (neighbor not detected) block is proportionally reduced in saturation. An example heat map for a time period of 24 hours is shown here with the most common time periods in the table showing the resulting time blocks.



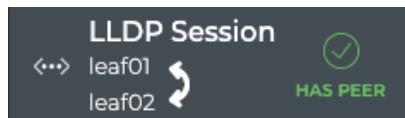
## Monitor the LLDP Service

## Monitor a Single LLDP Session

Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

### LLDP Session Card Workflow Summary

The small LLDP Session card displays:



Item	Description
↔	Indicates data is for a single session of a Network Service or Protocol
Title	LLDP Session
	Host and peer devices in session. Arrow points from host to peer.
✓ ✗	Indicates whether the host sees the peer or not; ✓ has a peer, ✗ no peer

## Monitor the LLDP Service

## Monitor a Single LLDP Session

The medium LLDP Session card displays:



Item	Description
Time period	Range of time in which the displayed data was collected
↔	Indicates data is for a single session of a Network Service or Protocol
Title	LLDP Session
	Host and peer devices in session. Arrow points from host to peer.
✓ ✗	Indicates whether the host sees the peer or not; ✓ has a peer, ✗ no peer

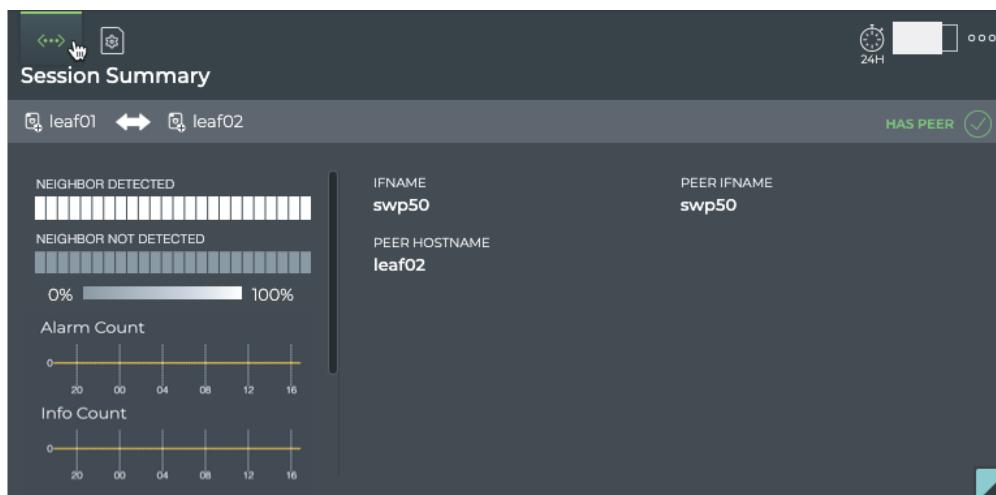
## Monitor the LLDP Service

## Monitor a Single LLDP Session

Item	Description
Time period	Range of time for the distribution chart
Heat map	Distribution of neighbor availability (detected or undetected) during this given time period
Hostname	User-defined name of the host device
Interface Name	Software interface on the host device where the session is running
Peer Hostname	User-defined name of the peer device
Peer Interface Name	Software interface on the peer where the session is running

The large LLDP Session card contains two tabs.

The *Session Summary* tab displays:



## Monitor the LLDP Service

## Monitor a Single LLDP Session

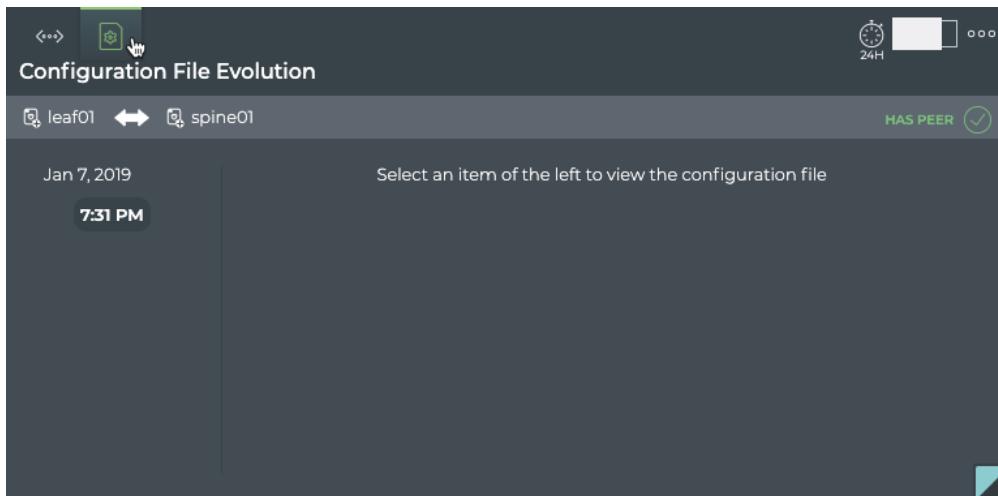
	<b>Description</b>
Time period	Range of time in which the displayed data was collected
↔↔↔	Indicates data is for a single session of a Network Service or Protocol
Title	Summary Session (Network Services   LLDP Session)
	Host and peer devices in session. Arrow points from host to peer.
✓ , ✗	Indicates whether the host sees the peer or not; ✓ has a peer, ✗ no peer
Heat map	Distribution of neighbor state (detected or undetected) during this given time period
Alarm Count chart	Distribution and count of LLDP alarm events during the given time period
Info Count chart	Distribution and count of LLDP info events during the given time period
Host Interface Name	Software interface on the host where the session is running
Peer Hostname	User-defined name of the peer device

## Monitor the LLDP Service

## Monitor a Single LLDP Session

	Description
Peer Interface Name	Software interface on the peer where the session is running

The *Configuration File Evolution* tab displays:



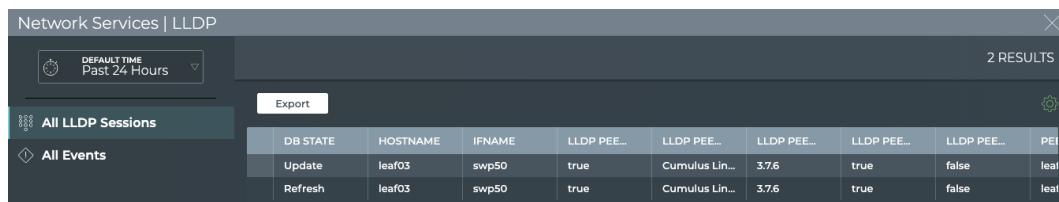
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates configuration file information for a single session of a Network Service or Protocol
Title	(Network Services   LLDP Session) Configuration File Evolution
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Click  to open associated device card.

## Monitor the LLDP Service

## Monitor a Single LLDP Session

Item	Description
<span style="font-size: 2em;">(✓)</span> <span style="font-size: 1.5em;">(✗)</span>	Indicates whether the host sees the peer or not; <span style="font-size: 1.5em;">(✓)</span> has a peer, <span style="font-size: 1.5em;">(✗)</span> no peer
Timestamps	When changes to the configuration file have occurred, the date and time are indicated. Click the time to see the changed file.
Configuration File	<p>When <b>File</b> is selected, the configuration file as it was at the selected time is shown. When <b>Diff</b> is selected, the configuration file at the selected time is shown on the left and the configuration file at the previous timestamp is shown on the right. Differences are highlighted.</p> <p><b>Note:</b> If no configuration file changes have been made, the card shows no results.</p>

The full screen LLDP Session card provides tabs for all LLDP sessions and all events.



DB STATE	HOSTNAME	IFNAME	LLDP PEE...	LLDP PEE...	LLDP PEE...	LLDP PEE...	PEE...	
Update	leaf03	swp50	true	Cumulus Lin...	3.76	true	false	leaf
Refresh	leaf03	swp50	true	Cumulus Lin...	3.76	true	false	leaf

Item	Description
Title	Network Services   LLDP
X	Closes full screen card and returns to workbench

## Monitor the LLDP Service

## Monitor a Single LLDP Session

Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab
All LLDP Sessions tab	<p>Displays all LLDP sessions on the host device. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"><li>• <b>DB State:</b> Session state of the DB.</li><li>• <b>Ifname:</b> Name of the host interface where LLDP session is running</li><li>• <b>LLDP Peer:</b><ul style="list-style-type: none"><li>◦ Os: Operating system (OS) used by peer device. Values include Cumulus Linux, RedHat, Ubuntu, and CentOS.</li><li>◦ Osv: Version of the OS used by peer device. Example values include 3.7.3, 2.5.x, 16.04, 7.1.</li><li>◦ Bridge: Indicates whether the peer device is a bridge (true) or not (false)</li><li>◦ Router: Indicates whether the peer device is a router (true) or not (false)</li><li>◦ Station: Indicates whether the peer device is a station (true) or not (false)</li></ul></li><li>• <b>OPID:</b> LLDP service identifier</li><li>• <b>Peer:</b><ul style="list-style-type: none"><li>◦ Hostname: User-defined name for the peer device</li><li>◦ Ifname: Name of the peer interface where the session is running</li></ul></li><li>• <b>Timestamp:</b> Date and time that the session was started, deleted, updated, or marked dead (device is down)</li></ul>

Item	Description
All Events tab	<p>Displays all events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of an event. Example: LLDP Session with host leaf02 swp6 modified fields leaf06 swp21</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of <i>lldp</i> in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Session Status Summary

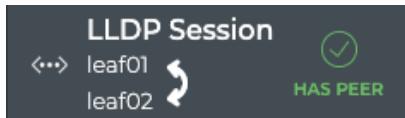
A summary of the LLDP session is available from the LLDP Session card workflow, showing the node and its peer and current status.

To view the summary:

1. Open the full screen LLDP Service card.
2. Double-click on a session. The full screen card closes automatically.
3. Locate the medium LLDP Session card.
4. Optionally, open the small LLDP Session card.

## Monitor the LLDP Service

## Monitor a Single LLDP Session



### View LLDP Session Neighbor State Changes

You can view the neighbor state for a given LLDP session from the medium and large LLDP Session cards. For a given time period, you can determine the stability of the LLDP session between two devices. If you experienced connectivity issues at a particular time, you can use these cards to help verify the state of the neighbor. If the neighbor was not alive more than it was alive, you can then investigate further into possible causes.

To view the neighbor availability for a given LLDP session on the medium card:

1. Open the full screen LLDP Service card.
2. Double-click on a session. The full screen card closes automatically.
3. Locate the medium LLDP Session card.

## Monitor the LLDP Service

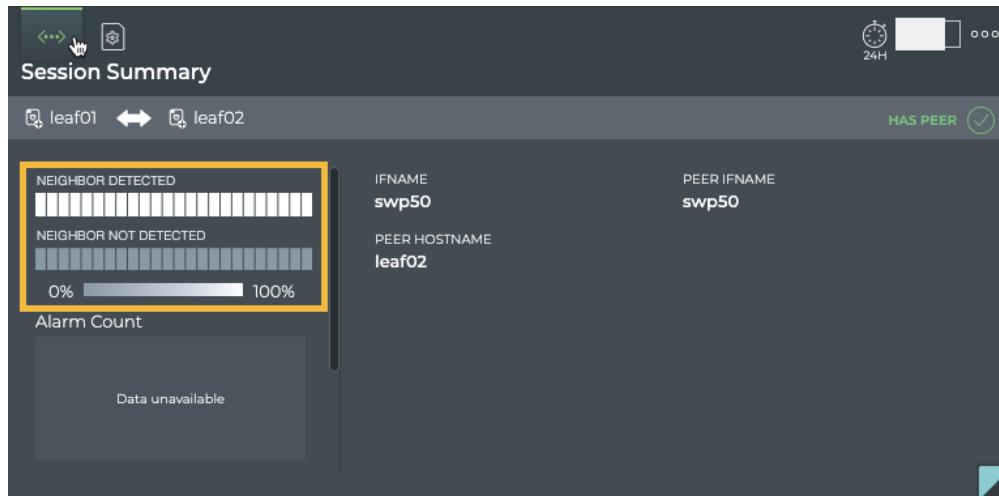
## Monitor a Single LLDP Session



In this example, the heat map tells us that this LLDP session has been able to detect a neighbor for the entire time period.

From this card, you can also view the host name and interface name, and the peer name and interface name.

To view the neighbor availability for a given LLDP session on the large LLDP Session card, open that card.



From this card, you can also view the alarm and info event counts, host interface name, peer hostname, and peer interface identifying the session in more detail.

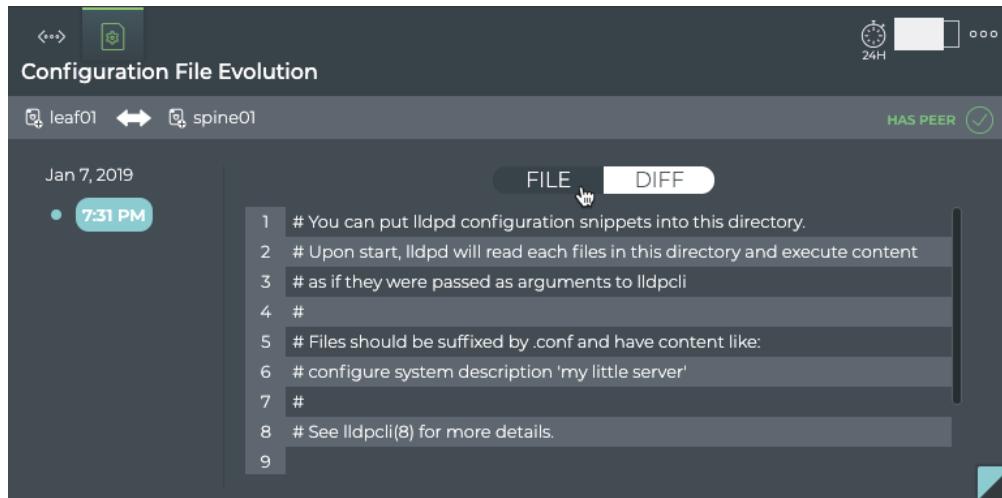
### View Changes to the LLDP Service Configuration File

Each time a change is made to the configuration file for the LLDP service, NetQ logs the change and enables you to compare it with the last version. This can be useful when you are troubleshooting potential causes for alarms or sessions losing their connections.

To view the configuration file changes:

1. Open the large LLDP Session card.
2. Hover over the card and click  to open the **LLDP Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.
4. Choose between the **File** view and the **Diff** view (selected option is dark; File by default).

The File view displays the content of the file for you to review.



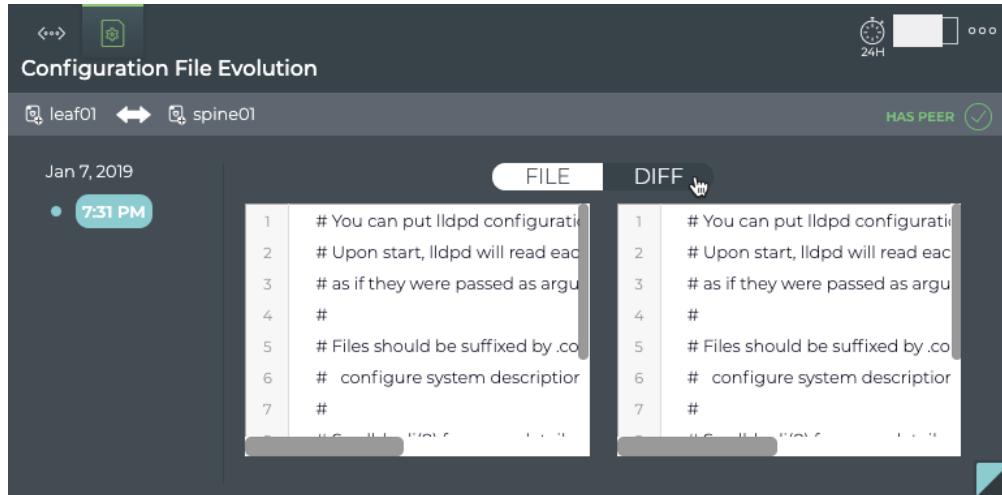
The screenshot shows the 'Configuration File Evolution' interface. At the top, there are two network cards: 'leaf01' and 'spine01'. To the right, there is a 'HAS PEER' status indicator with a green checkmark. Below the cards, the date 'Jan 7, 2019' and time '7:31 PM' are displayed. On the left, a vertical timeline shows a single event at 7:31 PM. On the right, there are two panes: 'FILE' (selected) and 'DIFF'. The 'FILE' pane displays the following configuration snippet:

```
1 # You can put llpd configuration snippets into this directory.  
2 # Upon start, llpd will read each files in this directory and execute content  
3 # as if they were passed as arguments to llpcli  
4 #  
5 # Files should be suffixed by .conf and have content like:  
6 # configure system description 'my little server'  
7 #  
8 # See llpcli(8) for more details.  
9
```

The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted in red and green. In this example, we don't have any changes to the file, so the same file is shown on both sides, and thus no highlighted lines.

## Monitor the LLDP Service

## Monitor a Single LLDP Session



The screenshot shows a comparison of configuration files for two devices: leaf01 and spine01. The interface has a dark theme with a header showing the devices and a timestamp of Jan 7, 2019, at 7:31 PM. A 'HAS PEER' status indicator is present. The left pane is labeled 'FILE' and the right pane is labeled 'DIFF'. The 'DIFF' pane highlights differences in the configuration files, specifically regarding the lldpd command and its arguments.

1	# You can put lldpd configurati	1	# You can put lldpd configurati
2	# Upon start, lldpd will read each	2	# Upon start, lldpd will read each
3	# as if they were passed as argu	3	# as if they were passed as argu
4	#	4	#
5	# Files should be suffixed by .co	5	# Files should be suffixed by .co
6	# configure system descriptor	6	# configure system descriptor
7	#	7	#

### View All LLDP Session Details

You can view all stored attributes of all of the LLDP sessions associated with the two devices on this card.

To view all session details, open the full screen LLDP Session card, and click the **All LLDP Sessions** tab.



The screenshot shows the 'Network Services | LLDP' card with the 'All LLDP Sessions' tab selected. It displays two results in a table format. The table includes columns for DB STATE, HOSTNAME, IFNAME, LLDP PEE..., LLDP PEE..., LLDP PEE..., LLDP PEE..., and PEI. The data shows two entries for 'leaf03' and 'leaf01'.

DB STATE	HOSTNAME	IFNAME	LLDP PEE...	LLDP PEE...	LLDP PEE...	LLDP PEE...	PEI
Update	leaf03	swp50	true	Cumulus Lin...	3.7.6	true	false
Refresh	leaf03	swp50	true	Cumulus Lin...	3.7.6	true	false

To return to your workbench, click



in the top right of the card.

### View All Events

You can view all of the alarm and info events in the network.

To view all events, open the full screen LLDP Session card, and click the **All Events** tab.

## Monitor the LLDP Service

## Monitor a Single LLDP Session

The screenshot shows a software interface titled "Network Services | LLDP". At the top, there is a search bar with a clock icon and the text "DEFAULT TIME Past 24 Hours". To the right, it says "481 RESULTS". Below the search bar, there are two tabs: "All LLDP Sessions" and "All Events", with "All Events" being the active tab. There is also an "Export" button and a gear icon. The main area displays a table with the following columns: SOURCE, TIME, TYPE, MESSAGE, and SEVERITY. The data in the table is as follows:

SOURCE	TIME	TYPE	MESSAGE	SEVERITY
server04	Apr 4, 2019, ...	services	Service rsysl...	critical
server02	Apr 4, 2019, ...	services	Service rsysl...	critical
server04	Apr 4, 2019, ...	agent	Agent state ...	critical
server01	Apr 4, 2019, ...	agent	Agent state ...	critical
server04	Apr 4, 2019, ...	agent	Agent state ...	critical
server03	Apr 4, 2019, ...	agent	Agent state ...	critical
server01	Apr 4, 2019, ...	agent	Agent state ...	critical
edge01	Apr 4, 2019, ...	agent	Agent state ...	critical

Where to go next depends on what data you see, but a few options include:

- Open the **All LLDP Sessions** tabs to look more closely at the details of the sessions between these two devices.
- Sort on other parameters:
  - by **Message** to determine the frequency of particular events
  - by **Severity** to determine the most critical events
  - by **Time** to find events that may have occurred at a particular time to try to correlate them with other system events
- Export data to a file
- Return to your workbench by clicking  in the top right corner

# Monitor the MLAG Service

The Cumulus NetQ UI enables operators to view the health of the MLAG service on a network-wide and a per session basis, giving greater insight into all aspects of the service. This is accomplished through two card workflows, one for the service and one for the session. They are described separately here.



## NOTE

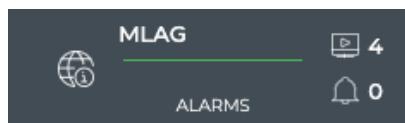
**MLAG or CLAG?** The Cumulus Linux implementation of MLAG is referred to by other vendors as MLAG, MC-LAG or VPC. The Cumulus NetQ UI uses the MLAG terminology predominantly.

## Monitor the MLAG Service (All Sessions)

With NetQ, you can monitor the number of nodes running the MLAG service, view sessions running, and view alarms triggered by the MLAG service. For an overview and how to configure MLAG in your data center network, refer to [Multi-Chassis Link Aggregation - MLAG](#).

### MLAG Service Card Workflow Summary

The small MLAG Service card displays:

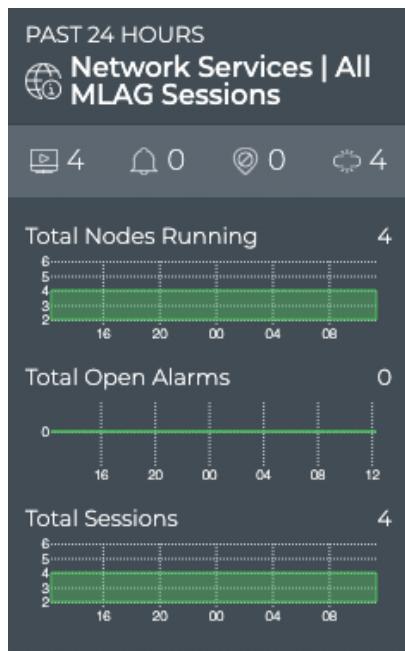


## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

Item	Description
	Indicates data is for all sessions of a Network Service or Protocol
Title	MLAG: All MLAG Sessions, or the MLAG Service
	Total number of switches with the MLAG service enabled during the designated time period
	Total number of MLAG-related alarms received during the designated time period
Chart	Distribution of MLAG-related alarms received during the designated time period

The medium MLAG Service card displays:



## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	Network Services   All MLAG Sessions
	Total number of switches with the MLAG service enabled during the designated time period
	Total number of MLAG-related alarms received during the designated time period
	Total number of sessions with an inactive backup IP address during the designated time period
	Total number of bonds with only a single connection during the designated time period
Total Nodes Running chart	<p>Distribution of switches and hosts with the MLAG service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running MLAG last week or last month might be more or less than the number of nodes running MLAG currently.</p>

## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

Item	Description
Total Open Alarms chart	<p>Distribution of MLAG-related alarms received during the designated time period, and the total number of current MLAG-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Total Sessions chart	Distribution of MLAG sessions running during the designated time period, and the total number of sessions running on the network currently

The large MLAG service card contains two tabs.

The *All MLAG Sessions Summary* tab which displays:



## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

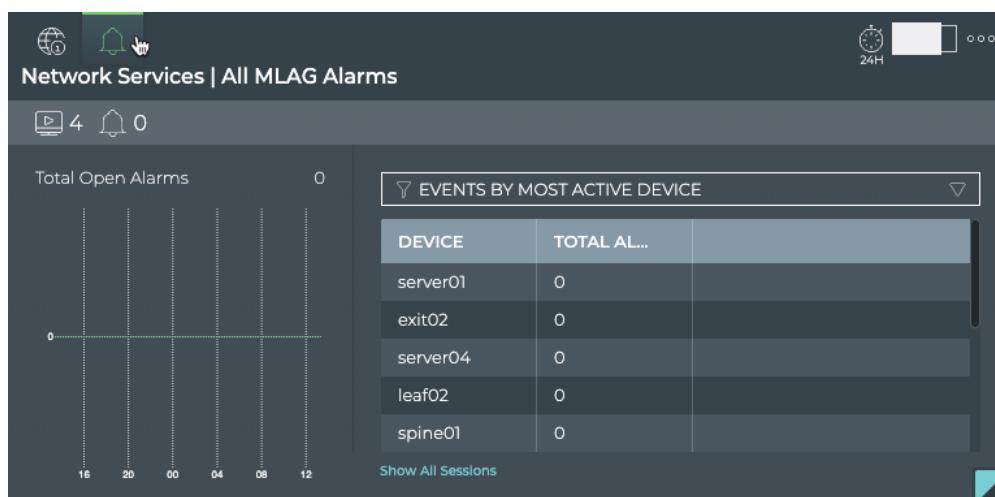
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	All MLAG Sessions Summary
	Total number of switches with the MLAG service enabled during the designated time period
	Total number of MLAG-related alarms received during the designated time period
Total Nodes Running chart	Distribution of switches and hosts with the MLAG service enabled during the designated time period, and a total number of nodes running the service currently.  <b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running MLAG last week or last month might be more or less than the number of nodes running MLAG currently.
Total Sessions chart	Distribution of MLAG sessions running during the designated time period, and the total number of sessions running on the network currently

## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

Item	Description
Total Sessions with Inactive-backup-ip chart	Distribution of sessions without an active backup IP defined during the designated time period, and the total number of these sessions running on the network currently
Table/Filter options	<p>When the <b>Switches with Most Sessions</b> filter is selected, the table displays switches running MLAG sessions in decreasing order of session count—devices with the largest number of sessions are listed first</p> <p>When the <b>Switches with Most Unestablished Sessions</b> filter is selected, the table displays switches running MLAG sessions in decreasing order of unestablished session count—devices with the largest number of unestablished sessions are listed first</p>
Show All Sessions	Link to view all MLAG sessions in the full screen card

The *All MLAG Alarms* tab which displays:



## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
 (in header)	Indicates alarm data for all MLAG sessions
Title	Network Services   All MLAG Alarms (visible when you hover over card)
	Total number of switches with the MLAG service enabled during the designated time period
 (in summary bar)	Total number of MLAG-related alarms received during the designated time period
Total Alarms chart	<p>Distribution of MLAG-related alarms received during the designated time period, and the total number of current MLAG-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Table/Filter options	When the <b>Events by Most Active Device</b> filter is selected, the table displays switches running MLAG sessions in decreasing order of alarm count—devices with the largest number of sessions are listed first

## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

Item	Description
Show All Sessions	Link to view all MLAG sessions in the full screen card

The full screen MLAG Service card provides tabs for all switches, all sessions, and all alarms.

The screenshot shows a table titled "Network Services | MLAG" with 8 results. The columns are: HOSTNAME, TIME, ASIC MOD., AGENT VE..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., PLATFOR..., and MEM. The data rows are:

HOSTNAME	TIME	ASIC MOD.	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	MEM
exit01	9/13/19 11:44 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
exit02	9/13/19 11:44 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
leaf01	9/13/19 11:46 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
leaf02	9/13/19 11:45 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
leaf03	9/13/19 11:45 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0

Item	Description
Title	Network Services   MLAG
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

All Switches tab	<p>Displays all switches and hosts running the MLAG service. By default, the device list is sorted by <b>hostname</b>. This tab provides the following additional data about each device:</p> <ul style="list-style-type: none"><li>• <b>Agent</b><ul style="list-style-type: none"><li>◦ State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).</li><li>◦ Version: Software version number of the NetQ Agent on a given device. This should match the version number of the NetQ software loaded on your server or appliance; for example, 2.1.0.</li></ul></li><li>• <b>ASIC</b><ul style="list-style-type: none"><li>◦ Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.</li><li>◦ Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.</li><li>◦ Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.</li><li>◦ Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.</li><li>◦ Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.</li></ul></li><li>• <b>CPU</b><ul style="list-style-type: none"><li>◦ Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.</li><li>◦ Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.</li><li>◦ Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.</li><li>◦ Nos: Number of cores. Example values include 2, 4, and 8.</li></ul></li><li>• <b>Disk Total Size:</b> Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.</li><li>• <b>License State:</b> Indicator of validity. Values include ok and bad.</li><li>• <b>Memory Size:</b> Total amount of local RAM. Example values include 8192 MB and 2048 MB</li></ul>
------------------	--

Item	Description
All Sessions tab	<p>Displays all MLAG sessions network-wide. By default, the session list is sorted by hostname. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"> <li>• <b>Backup Ip:</b> IP address of the interface to use if the peerlink (or bond) goes down</li> <li>• <b>Backup Ip Active:</b> Indicates whether the backup IP address has been specified and is active (true) or not (false)</li> <li>• <b>Bonds</b> <ul style="list-style-type: none"> <li>◦ Conflicted: Identifies the set of interfaces in a bond that do not match on each end of the bond</li> <li>◦ Single: Identifies a set of interfaces connecting to only one of the two switches</li> <li>◦ Dual: Identifies a set of interfaces connecting to both switches</li> <li>◦ Proto Down: Interface on the switch brought down by the clagd service. Value is blank if no interfaces are down due to clagd service.</li> </ul> </li> <li>• <b>Clag Sysmac:</b> Unique MAC address for each bond interface pair. <b>Note:</b> Must be a value between 44:38:39:ff:00:00 and 44:38:39:ff:ff:ff.</li> <li>• <b>DB State:</b> Session state of the DB.</li> <li>• <b>OPID:</b> MLAG service identifier</li> <li>• <b>Peer:</b> <ul style="list-style-type: none"> <li>◦ If: Name of the peer interface</li> <li>◦ Role: Role of the peer device. Values include primary and secondary.</li> <li>◦ State: Indicates if peer device is up (true) or down (false)</li> </ul> </li> <li>• <b>Role:</b> Role of the host device. Values include primary and secondary.</li> <li>• <b>Timestamp:</b> Date and time the CLAG session was started, deleted, updated, or marked dead (device went down)</li> <li>• <b>Vxlan Anycast:</b> Anycast IP address used for VXLAN termination</li> </ul>

Item	Description
All Alarms tab	<p>Displays all CLAG events network-wide. By default, the event list is sorted by time, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li><b>Message:</b> Text description of a BGP-related event. Example: Clag conflicted bond changed from swp7 swp8 to swp9 swp10</li> <li><b>Source:</b> Hostname of network device that generated the event</li> <li><b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li><b>Type:</b> Network protocol or service generating the event. This always has a value of <i>clag</i> in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Service Status Summary

A summary of the MLAG service is available from the MLAG Service card workflow, including the number of nodes running the service, the number of MLAG-related alarms, and a distribution of those alarms.

To view the summary, open the small MLAG Service card.



For more detail, select a different size MLAG Service card.

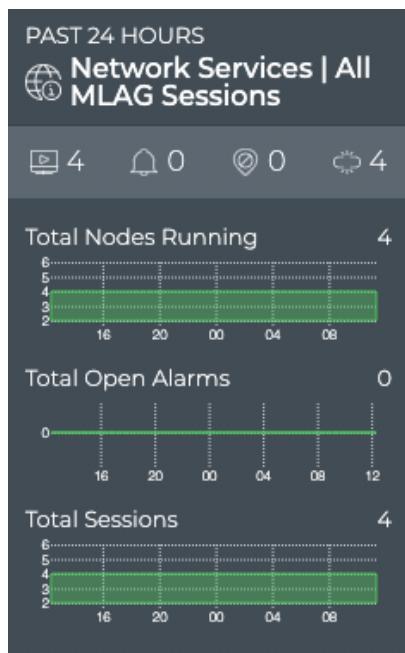
## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

### View the Distribution of Sessions and Alarms

It is useful to know the number of network nodes running the MLAG protocol over a period of time, as it gives you insight into the amount of traffic associated with and breadth of use of the protocol. It is also useful to compare the number of nodes running MLAG with the alarms present at the same time to determine if there is any correlation between the issues and the ability to establish a MLAG session.

To view these distributions, open the medium MLAG Service card.



If a visual correlation is apparent, you can dig a little deeper with the large MLAG Service card tabs.

### View Devices with the Most CLAG Sessions

You can view the load from MLAG on your switches using the large MLAG Service card. This data enables you to see which switches are handling the most MLAG traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

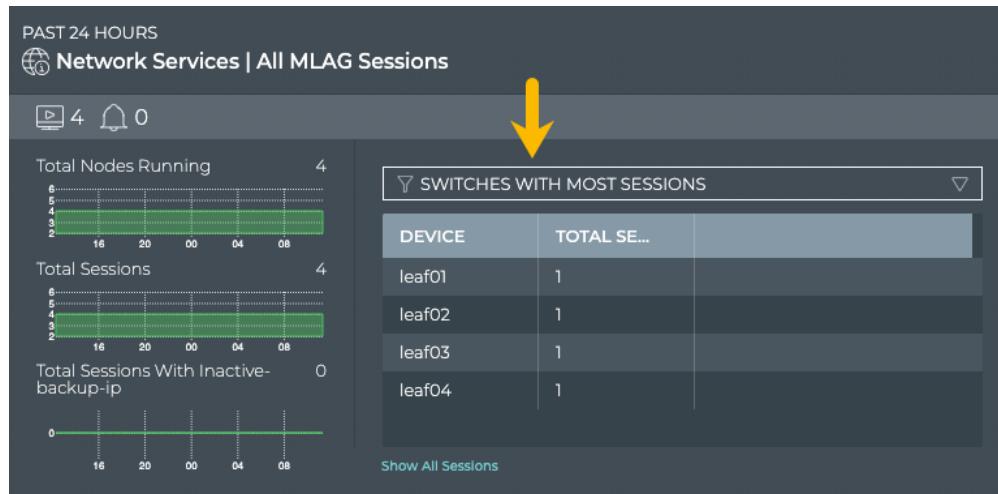
## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

To view switches and hosts with the most MLAG sessions:

1. Open the large MLAG Service card.
2. Select **Switches with Most Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most MLAG sessions at the top. Scroll down to view those with the fewest sessions.



To compare this data with the same data at a previous time:

1. Open another large MLAG Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking

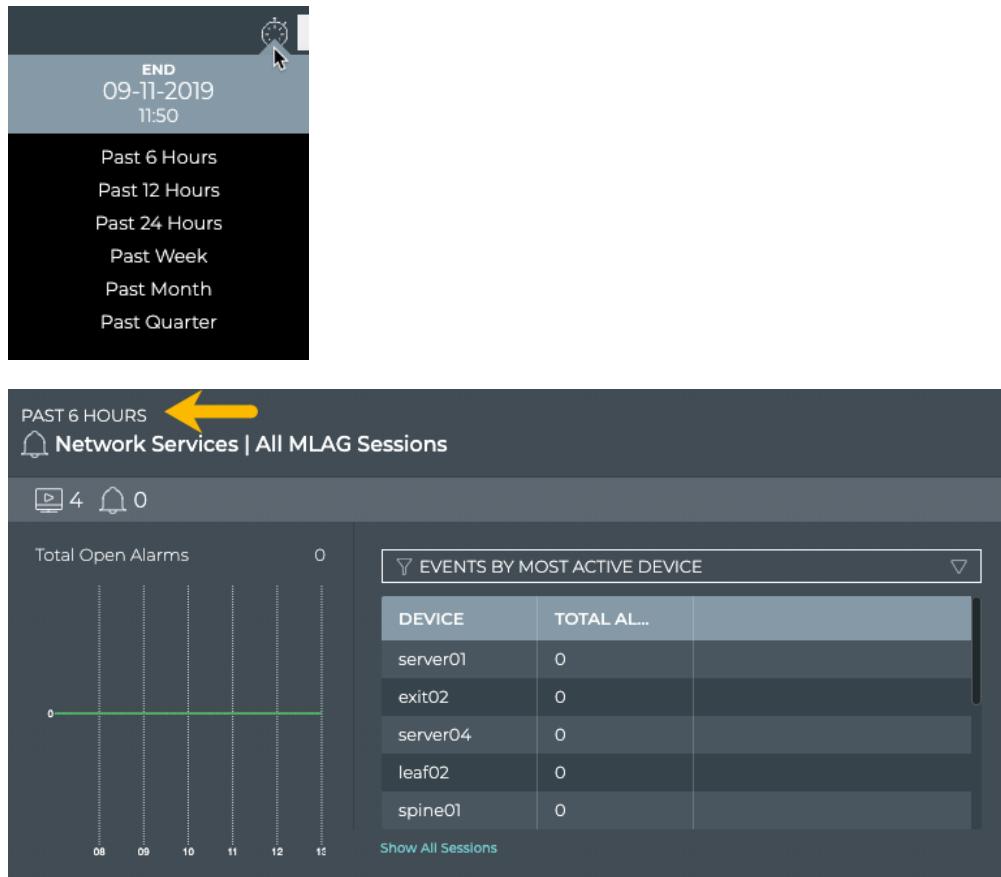


4. Select the time period that you want to compare with the current time.

You can now see whether there are significant differences between this time period and the previous time period.

## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)



If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running MLAG than previously, looking for changes in the topology, and so forth.

### View Devices with the Most Unestablished MLAG Sessions

You can identify switches that are experiencing difficulties establishing MLAG sessions; both currently and in the past.

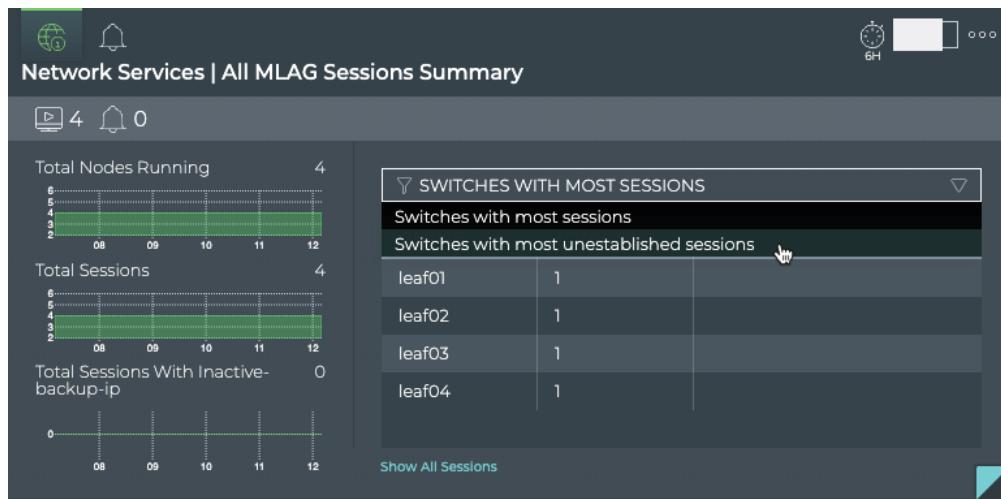
To view switches with the most unestablished MLAG sessions:

1. Open the large MLAG Service card.
2. Select **Switches with Most Unestablished Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most unestablished MLAG sessions at the top. Scroll down to view those with the fewest unestablished sessions.

## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)



Where to go next depends on what data you see, but a few options include:

- Change the time period for the data to compare with a prior time.

If the same switches are consistently indicating the most unestablished sessions, you might want to look more carefully at those switches using the Switches card workflow to determine probable causes. Refer to [Monitor Switches](#).

- Click **Show All Sessions** to investigate all MLAG sessions with events in the full screen card.

### View Switches with the Most MLAG-related Alarms

Switches experiencing a large number of MLAG alarms may indicate a configuration or performance issue that needs further investigation. You can view the switches sorted by the number of MLAG alarms and then use the Switches card workflow or the Alarms card workflow to gather more information about possible causes for the alarms.

To view switches with most MLAG alarms:

1. Open the large MLAG Service card.
2. Hover over the header and click

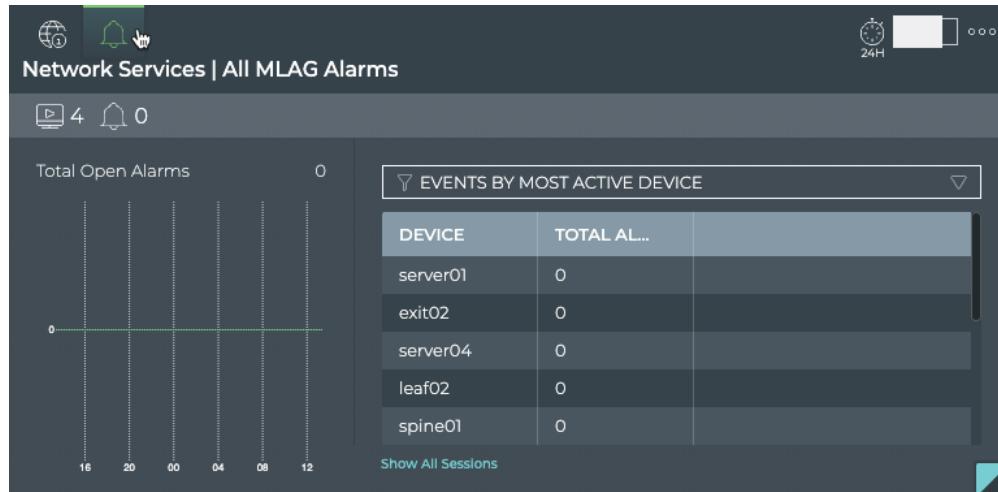


## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

3. Select **Events by Most Active Device** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most MLAG alarms at the top. Scroll down to view those with the fewest alarms.



Where to go next depends on what data you see, but a few options include:

- Change the time period for the data to compare with a prior time. If the same switches are consistently indicating the most alarms, you might want to look more carefully at those switches using the Switches card workflow.
- Click **Show All Sessions** to investigate all MLAG sessions with alarms in the full screen card.

### View All MLAG Events

The MLAG Service card workflow enables you to view all of the MLAG events in the designated time period.

To view all MLAG events:

1. Open the full screen MLAG Service card.
2. Click **All Alarms** tab.

## Monitor the MLAG Service

## Monitor the MLAG Service (All Sessions)

The screenshot shows a table titled "Network Services | MLAG" with 9 results. The table has columns: SOURCE, MESSAGE, TYPE, SEVERITY, and TIME. The data is as follows:

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
leaf02	Peer state changed to down	clag	critical	9/12/19 7:46 PM
leaf04	Peer state changed to down	clag	critical	9/12/19 7:45 PM
leaf03	Peer state changed to down	clag	critical	9/12/19 7:45 PM
leaf01	Peer state changed to down	clag	critical	9/12/19 7:45 PM
leaf02	Peer state changed to down	clag	critical	8/2/19 4:05 PM

Where to go next depends on what data you see, but a few options include:

- Open the **All Switches** or **All Sessions** tabs to look more closely at the alarms from the switch or session perspective.
- Sort on other parameters:
  - by **Message** to determine the frequency of particular events
  - by **Severity** to determine the most critical events
  - by **Time** to find events that may have occurred at a particular time to try to correlate them with other system events
- Export the data to a file by clicking **Export** or selecting a subset and clicking **Export Selected** in edit menu
- Return to your workbench by clicking in the top right corner

## View Details About All Switches Running MLAG

You can view all stored attributes of all switches running MLAG in your network in the full-screen card.

To view all switch details, open the full screen MLAG Service card, and click the **All Switches** tab.

The screenshot shows a table titled "Network Services | MLAG" with 8 results. The table has columns: HOSTNAME, TIME, ASIC MOD..., AGENT VE..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., PLATFOR..., and MEM. The data is as follows:

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	MEM
exit01	9/13/19 11:44 ...	VX	2.3.0-cl3u2!~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
exit02	9/13/19 11:44 ...	VX	2.3.0-cl3u2!~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
leaf01	9/13/19 11:46 ...	VX	2.3.0-cl3u2!~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
leaf02	9/13/19 11:49 ...	VX	2.3.0-cl3u2!~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0
leaf03	9/13/19 11:49 ...	VX	2.3.0-cl3u2!~...	3.7.8	ok	6.00 GB	3.7.8	VX	768.0

## Monitor the MLAG Service

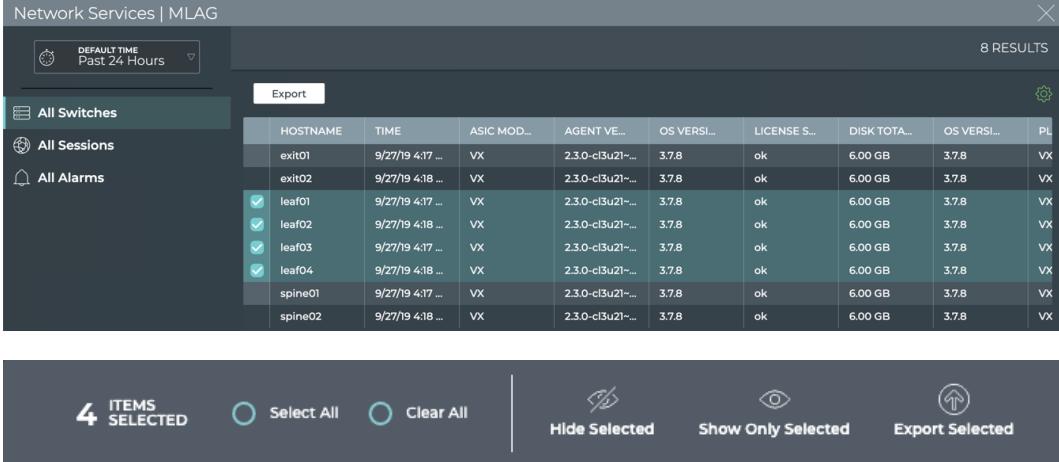
## Monitor the MLAG Service (All Sessions)

To return to your workbench, click  in the top right corner.

### Take Actions on Data Displayed in Results List

In the full screen MLAG Service card, you can determine which results are displayed in the results list, and which are exported.

To take actions on the data, click in the blank column at the very left of a row. A checkbox appears, selecting that switch, session, or alarm, and an edit menu is shown at the bottom of the card (shown enlarged here).



	HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PL...
	exit01	9/27/19 4:17 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
	exit02	9/27/19 4:18 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
<input checked="" type="checkbox"/>	leaf01	9/27/19 4:17 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
<input checked="" type="checkbox"/>	leaf02	9/27/19 4:18 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
<input checked="" type="checkbox"/>	leaf03	9/27/19 4:17 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
<input checked="" type="checkbox"/>	leaf04	9/27/19 4:18 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
	spine01	9/27/19 4:17 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX
	spine02	9/27/19 4:18 ...	VX	2.3.0-cl3u2l~...	3.7.8	ok	6.00 GB	3.7.8	VX

You can perform the following actions on the results list:

Option	Action or Behavior on Click
Select All	Selects all items in the results list
Clear All	Clears all existing selections of items in the results list. This also hides the edit menu.
Open Cards	Open the corresponding validation or trace result card.
Hide Selected	Hide selected items (switches, sessions, alarms, and so forth) from the results list.

Option	Action or Behavior on Click
Show Only Selected	Hide unselected items (switches, sessions, alarms, and so forth) from the results list.
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the <b>Export</b> button.

To return to original display of results, click the associated tab.

## Monitor a Single MLAG Session

With NetQ, you can monitor the number of nodes running the MLAG service, view switches with the most peers alive and not alive, and view alarms triggered by the MLAG service. For an overview and how to configure MLAG in your data center network, refer to [Multi-Chassis Link Aggregation - MLAG](#).

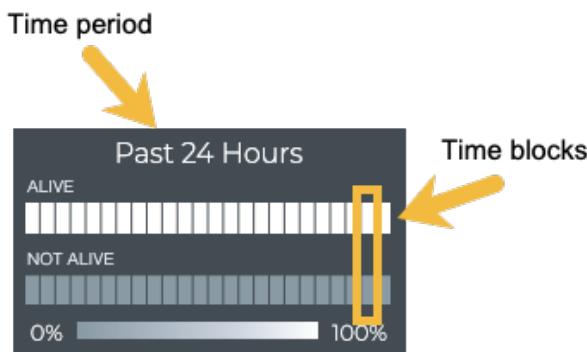
 NOTE

To access the single session cards, you must open the full screen MLAG Service, click the All Sessions tab, select the desired session, then click  (Open Cards).

### Granularity of Data Shown Based on Time Period

On the medium and large single MLAG session cards, the status of the peers is represented in heat maps stacked vertically; one for peers that are reachable (alive), and one for peers that are unreachable (not alive). Depending on the time period of data on the card, the number of smaller time blocks used to indicate the status varies. A vertical stack of time blocks, one from each map, includes the results from all checks during that time. The results are shown by how saturated the color is for each block. If

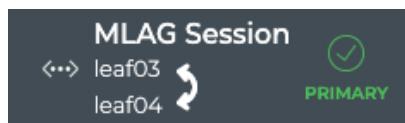
all peers during that time period were alive for the entire time block, then the top block is 100% saturated (white) and the not alive block is zero percent saturated (gray). As peers that are not alive increase in saturation, the peers that are alive block is proportionally reduced in saturation. An example heat map for a time period of 24 hours is shown here with the most common time periods in the table showing the resulting time blocks.



Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

### MLAG Session Card Workflow Summary

The small MLAG Session card displays:



## Monitor the MLAG Service

## Monitor a Single MLAG Session

Item	Description
<code>&lt;--&gt;</code>	Indicates data is for a single session of a Network Service or Protocol
Title	CLAG Session
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session.
,	Indication of host role, primary or secondary 

The medium MLAG Session card displays:



## Monitor the MLAG Service

## Monitor a Single MLAG Session

Item	Description
Time period (in header)	Range of time in which the displayed data was collected; applies to all card sizes
↔↔↔	Indicates data is for a single session of a Network Service or Protocol
Title	Network Services   MLAG Session
◊	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Arrow points from the host to the peer. Click ◊ to open associated device card.
✓ ,✗	Indication of host role, primary ✓ or secondary ✗
Time period (above chart)	Range of time for data displayed in peer status chart
Peer Status chart	Distribution of peer availability, alive or not alive, during the designated time period. The number of time segments in a time period varies according to the length of the time period.
Role	Role that host device is playing. Values include primary and secondary.

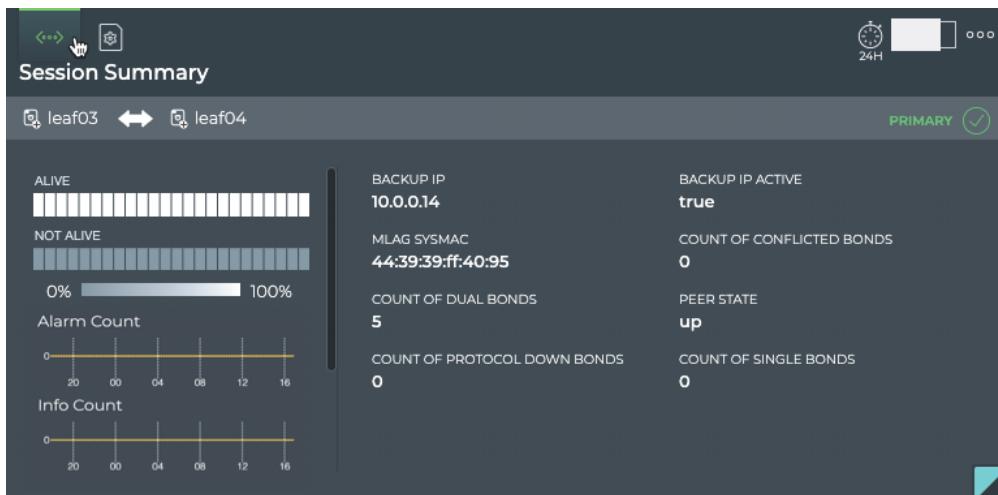
## Monitor the MLAG Service

## Monitor a Single MLAG Session

Item	Description
CLAG sysmac	System MAC address of the MLAG session
Peer Role	Role that peer device is playing. Values include primary and secondary.
Peer State	Operational state of the peer, up (true) or down (false)

The large MLAG Session card contains two tabs.

The *Session Summary* tab displays:

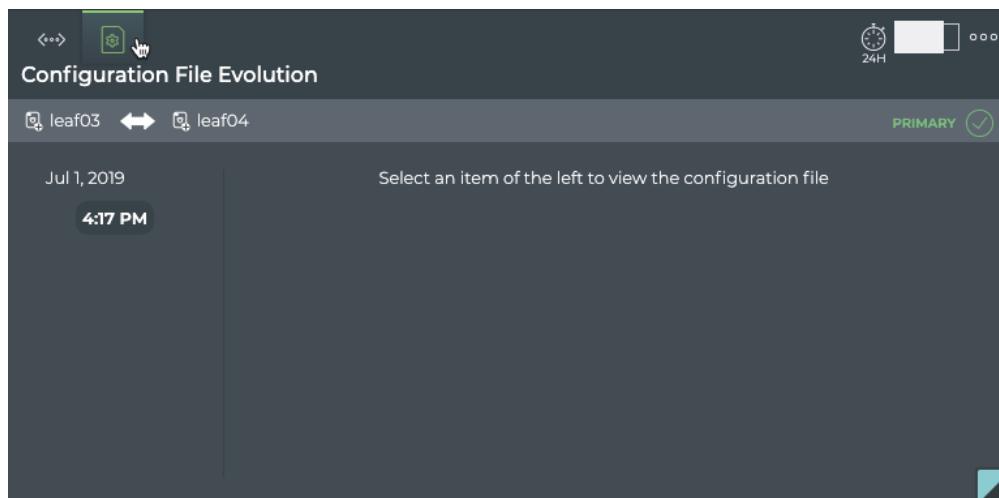


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
<::>	Indicates data is for a single session of a Network Service or Protocol

Item	Description
Title	(Network Services   MLAG Session) Session Summary
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Arrow points from the host to the peer. Click  to open associated device card.
  	Indication of host role, primary  or secondary 
Alarm Count Chart	Distribution and count of CLAG alarm events over the given time period.
Info Count Chart	Distribution and count of CLAG info events over the given time period.
Peer Status chart	Distribution of peer availability, alive or not alive, during the designated time period. The number of time segments in a time period varies according to the length of the time period.
Backup IP	IP address of the interface to use if the peerlink (or bond) goes down
Backup IP Active	Indicates whether the backup IP address is configured
CLAG SysMAC	System MAC address of the MLAG session

Item	Description
Peer State	Operational state of the peer, up (true) or down (false)
Count of Dual Bonds	Number of bonds connecting to both switches.
Count of Single Bonds	Number of bonds connecting to only one switch.
Count of Protocol Down Bonds	Number of bonds with interfaces that were brought down by the clagd service.
Count of Conflicted Bonds	Number of bonds which have a set of interfaces that are not the same on both switches

The *Configuration File Evolution* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates configuration file information for a single session of a Network Service or Protocol
Title	(Network Services   MLAG Session) Configuration File Evolution
	<p>Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Arrow points from the host to the peer. Click  to open associated device card.</p>
	<p>Indication of host role, primary            or secondary  </p>
Timestamps	When changes to the configuration file have occurred, the date and time are indicated. Click the time to see the changed file.
Configuration File	<p>When <b>File</b> is selected, the configuration file as it was at the selected time is shown.</p> <p>When <b>Diff</b> is selected, the configuration file at the selected time is shown on the left and the configuration file at the previous timestamp is shown on the right. Differences are highlighted.</p>

The full screen MLAG Session card provides tabs for all MLAG sessions and all events.

## Monitor the MLAG Service

## Monitor a Single MLAG Session

Network Services   MLAG								
DEFAULT TIME Past 24 Hours		2 RESULTS						
		Export						
All MLAG Sessions		All Events						
HOSTNAME	TIMESTAMP	DUAL BONDS	ROLE	DB STATE	PEER IF	BACKUP I...	PROTO DO...	LAST UPD...
leaf03	9/23/19 12:47 AM	{bond03:bond03,bond04:...	primary	Refresh	peerlink.4094	true		
leaf03	9/24/19 12:05 AM	{bond03:bond03,bond04:...	primary	Update	peerlink.4094	true		

Item	Description
Title	Network Services   MLAG
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

Item	Description
All MLAG Sessions tab	<p>Displays all MLAG sessions for the given session. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"> <li>• <b>Backup Ip:</b> IP address of the interface to use if the peerlink (or bond) goes down</li> <li>• <b>Backup Ip Active:</b> Indicates whether the backup IP address has been specified and is active (true) or not (false)</li> <li>• <b>Bonds</b> <ul style="list-style-type: none"> <li>◦ Conflicted: Identifies the set of interfaces in a bond that do not match on each end of the bond</li> <li>◦ Single: Identifies a set of interfaces connecting to only one of the two switches</li> <li>◦ Dual: Identifies a set of interfaces connecting to both switches</li> <li>◦ Proto Down: Interface on the switch brought down by the clagd service. Value is blank if no interfaces are down due to clagd service.</li> </ul> </li> <li>• <b>Mlag Sysmac:</b> Unique MAC address for each bond interface pair. <b>Note:</b> Must be a value between 44:38:39:ff:00:00 and 44:38:39:ff:ff:ff.</li> <li>• <b>DB State:</b> Session state of the DB.</li> <li>• <b>OPID:</b> MLAG service identifier</li> <li>• <b>Peer:</b> <ul style="list-style-type: none"> <li>◦ If: Name of the peer interface</li> <li>◦ Role: Role of the peer device. Values include primary and secondary.</li> <li>◦ State: Indicates if peer device is up (true) or down (false)</li> </ul> </li> <li>• <b>Role:</b> Role of the host device. Values include primary and secondary.</li> <li>• <b>Timestamp:</b> Date and time the MLAG session was started, deleted, updated, or marked dead (device went down)</li> <li>• <b>Vxlan Anycast:</b> Anycast IP address used for VXLAN termination</li> </ul>

Item	Description
All Events tab	<p>Displays all events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of an event. Example: Clag conflicted bond changed from swp7 swp8 to swp9 swp10</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of <i>clag</i> in this card workflow.</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Session Status Summary

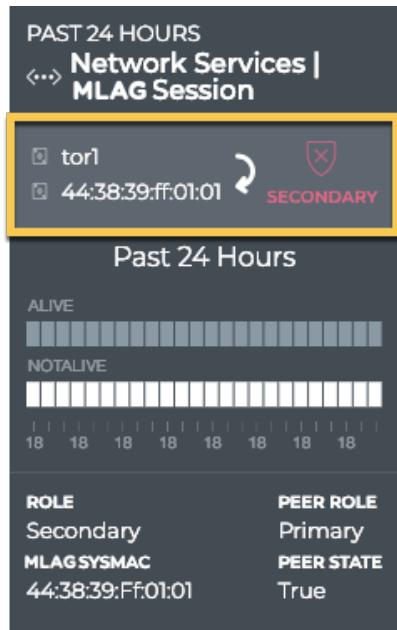
A summary of the MLAG session is available from the MLAG Session card workflow, showing the node and its peer and current status.

To view the summary:

1. Open the full screen MLAG Service card.
2. Select a session from the listing to view.
3. Close the full screen card to view the medium MLAG Session card.

## Monitor the MLAG Service

## Monitor a Single MLAG Session



In the left example, we see that the tor1 switch plays the secondary role in this session with the switch at 44:38:39:ff:01:01. In the right example, we see that the leaf03 switch plays the primary role in this session with leaf04.

## View MLAG Session Peering State Changes

You can view the peering state for a given MLAG session from the medium and large MLAG Session cards. For a given time period, you can determine the stability of the MLAG session between two devices. If you experienced connectivity issues at a

particular time, you can use these cards to help verify the state of the peer. If the peer was not alive more than it was alive, you can then investigate further into possible causes.

To view the state transitions for a given MLAG session:

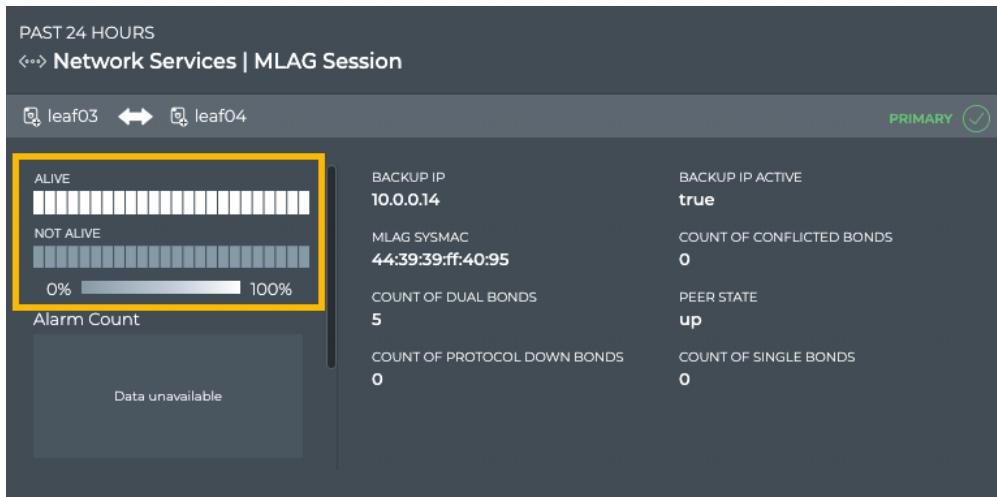
1. Open the full screen MLAG Service card.
2. Select a session from the listing to view.
3. Close the full screen card to view the medium MLAG Session card.



In this example, the peer switch has been alive for the entire 24-hour period.

From this card, you can also view the node role, peer role and state, and MLAG system MAC address which identify the session in more detail.

To view the peering state transitions for a given MLAG session on the large MLAG Session card, open that card.



From this card, you can also view the alarm and info event counts, node role, peer role, state, and interface, MLAG system MAC address, active backup IP address, single, dual, conflicted, and protocol down bonds, and the VXLAN anycast address identifying the session in more detail.

#### [View Changes to the MLAG Service Configuration File](#)

Each time a change is made to the configuration file for the MLAG service, NetQ logs the change and enables you to compare it with the last version. This can be useful when you are troubleshooting potential causes for alarms or sessions losing their connections.

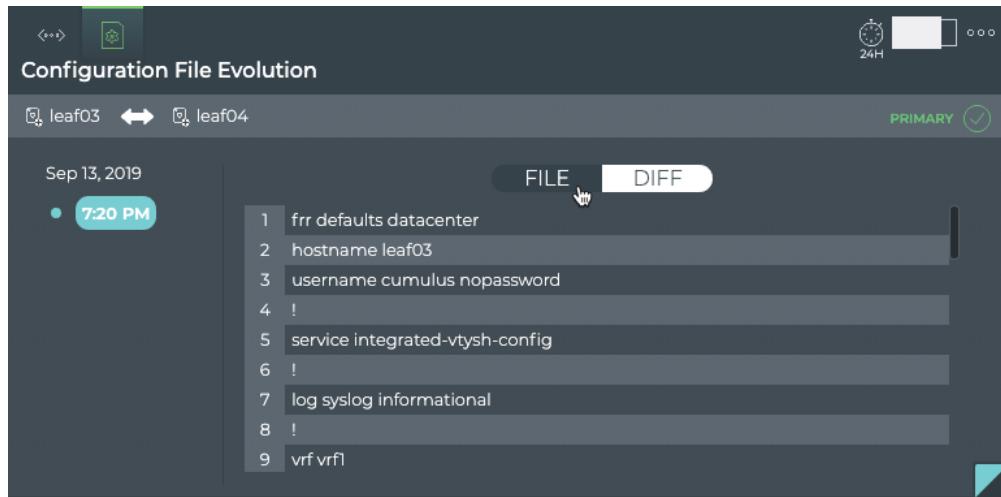
To view the configuration file changes:

1. Open the large MLAG Session card.
2. Hover over the card and click  to open the **Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.
4. Choose between the **File** view and the **Diff** view (selected option is dark; File by default).

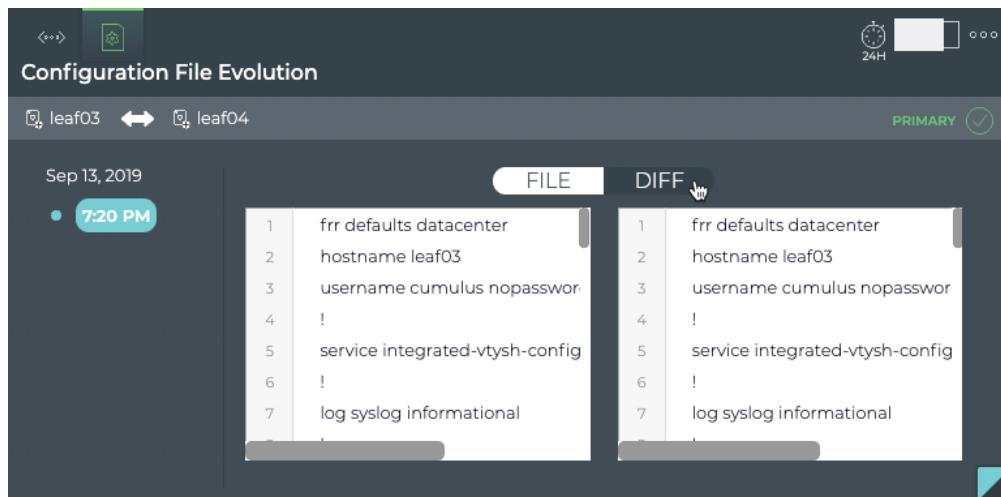
The File view displays the content of the file for you to review.

## Monitor the MLAG Service

## Monitor a Single MLAG Session



The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted in red and green. In this example, we don't have any changes after this first creation, so the same file is shown on both sides and no highlighting is present.



## All MLAG Session Details

You can view all stored attributes of all of the MLAG sessions associated with the two devices on this card.

To view all session details, open the full screen MLAG Session card, and click the **All MLAG Sessions** tab.

## Monitor the MLAG Service

## Monitor a Single MLAG Session

The screenshot shows a table titled 'All MLAG Sessions' with two rows of data. The columns are HOSTNAME, TIMESTAMP, DUAL BONDS, ROLE, DB STATE, PEER IF, BACKUP I., and PROTO DO... . The first row is for leaf03 on 9/23/19 at 12:47 AM, with dual bonds {bond03,bond03,bond04,...} and role primary. The second row is for leaf03 on 9/24/19 at 12:05 AM, with dual bonds {bond03,bond03,bond04,...} and role primary. The table has an 'Export' button at the top.

HOSTNAME	TIMESTAMP	DUAL BONDS	ROLE	DB STATE	PEER IF	BACKUP I.	PROTO DO...
leaf03	9/23/19 12:47 AM	{bond03,bond03,bond04,...}	primary	Refresh	peerlink.4094	true	
leaf03	9/24/19 12:05 AM	{bond03,bond03,bond04,...}	primary	Update	peerlink.4094	true	

Where to go next depends on what data you see, but a few options include:

- Open the **All Events** tabs to look more closely at the alarm and info events from the network.
- Sort on other parameters:
  - by **Single Bonds** to determine which interface sets are only connected to one of the switches
  - by **Backup IP and Backup IP Active** to determine if the correct backup IP address is specified for the service
- Export the data to a file by clicking **Export** or selecting a subset and clicking **Export Selected** in edit menu
- Return to your workbench by clicking in the top right corner

### View All MLAG Session Events

You can view all of the alarm and info events for the two devices on this card.

To view all events, open the full screen MLAG Session card, and click the **All Events** tab.

The screenshot shows a table titled 'All Events' with seven rows of data. The columns are SOURCE, MESSAGE, TYPE, SEVERITY, and TIME. The events listed are: server01 Sync state changed from yes to no for server01 (ntp, critical, 9/24/19 12:20 AM); server01 Sync state changed from yes to no for server01 (ntp, critical, 9/23/19 2:40 PM); server03 Sync state changed from yes to no for server03 (ntp, critical, 9/23/19 2:24 PM); and oob-mgmt-s... Service netd status changed from active to inactive (services, critical, 9/23/19 8:19 PM). The table has an 'Export' button at the top.

SOURCE	MESSAGE	TYPE	SEVERITY	TIME
server01	Sync state changed from yes to no for server01	ntp	critical	9/24/19 12:20 AM
server01	Sync state changed from yes to no for server01	ntp	critical	9/23/19 2:40 PM
server03	Sync state changed from yes to no for server03	ntp	critical	9/23/19 2:24 PM
oob-mgmt-s...	Service netd status changed from active to inactive	services	critical	9/23/19 8:19 PM

Where to go next depends on what data you see, but a few options include:

- Open the **All MLAG Sessions** tabs to look more closely at the individual sessions.

## Monitor the MLAG Service

## Monitor a Single MLAG Session

- Sort on other parameters:
  - by **Message** to determine the frequency of particular events
  - by **Severity** to determine the most critical events
  - by **Time** to find events that may have occurred at a particular time to try to correlate them with other system events
- Export the data to a file by clicking **Export** or selecting a subset and clicking **Export Selected** in edit menu
- Return to your workbench by clicking  in the top right corner

# Monitor the OSPF Service

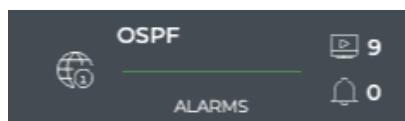
The Cumulus NetQ UI enables operators to view the health of the OSPF service on a network-wide and a per session basis, giving greater insight into all aspects of the service. This is accomplished through two card workflows, one for the service and one for the session. They are described separately here.

## Monitor the OSPF Service (All Sessions)

With NetQ, you can monitor the number of nodes running the OSPF service, view switches with the most full and unestablished OSPF sessions, and view alarms triggered by the OSPF service. For an overview and how to configure OSPF to run in your data center network, refer to [Open Shortest Path First - OSPF](#) or [Open Shortest Path First v3 - OSPFv3](#).

### OSPF Service Card Workflow

The small OSPF Service card displays:



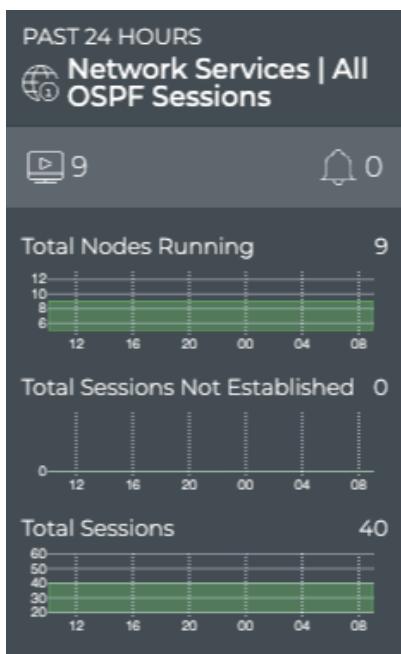
Item	Description
	Indicates data is for all sessions of a Network Service or Protocol
Title	OSPF: All OSPF Sessions, or the OSPF Service

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)

Item	Description
	Total number of switches and hosts with the OSPF service enabled during the designated time period
	Total number of OSPF-related alarms received during the designated time period
Chart	Distribution of OSPF-related alarms received during the designated time period

The medium OSPF Service card displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)

Item	Description
Title	Network Services   All OSPF Sessions
	Total number of switches and hosts with the OSPF service enabled during the designated time period
	Total number of OSPF-related alarms received during the designated time period
Total Nodes Running chart	Distribution of switches and hosts with the OSPF service enabled during the designated time period, and a total number of nodes running the service currently.  <b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running OSPF last week or last month might be more or less than the number of nodes running OSPF currently.
Total Sessions Not Established chart	Distribution of unestablished OSPF sessions during the designated time period, and the total number of unestablished sessions in the network currently.  <b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of unestablished session last week or last month might be more or less than the number of nodes with unestablished sessions currently.
Total Sessions chart	Distribution of OSPF sessions during the designated time period, and the total number of sessions running on the network currently.

The large OSPF service card contains two tabs.

The *Sessions Summary* tab displays:

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)



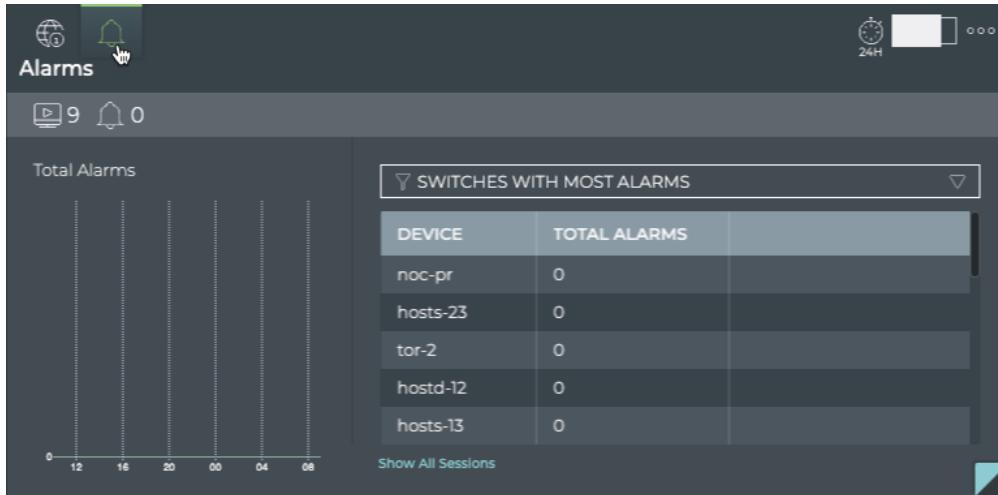
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	Sessions Summary (visible when you hover over card)
	Total number of switches and hosts with the OSPF service enabled during the designated time period
	Total number of OSPF-related alarms received during the designated time period
Total Nodes Running chart	<p>Distribution of switches and hosts with the OSPF service enabled during the designated time period, and a total number of nodes running the service currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of nodes running OSPF last week or last month might be more or less than the number of nodes running OSPF currently.</p>

Item	Description
Total Sessions chart	Distribution of OSPF sessions during the designated time period, and the total number of sessions running on the network currently.
Total Sessions Not Established chart	<p>Distribution of unestablished OSPF sessions during the designated time period, and the total number of unestablished sessions in the network currently.</p> <p><b>Note:</b> The node count here may be different than the count in the summary bar. For example, the number of unestablished session last week or last month might be more or less than the number of nodes with unestablished sessions currently.</p>
Table/Filter options	<p>When the <b>Switches with Most Sessions</b> filter option is selected, the table displays the switches and hosts running OSPF sessions in decreasing order of session count—devices with the largest number of sessions are listed first</p> <p>When the <b>Switches with Most Unestablished Sessions</b> filter option is selected, the table switches and hosts running OSPF sessions in decreasing order of unestablished sessions—devices with the largest number of unestablished sessions are listed first</p>
Show All Sessions	Link to view data for all OSPF sessions in the full screen card

The *Alarms* tab displays:

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
(in header)	Indicates data is all alarms for all OSPF sessions
Title	Alarms (visible when you hover over card)
	Total number of switches and hosts with the OSPF service enabled during the designated time period
(in summary bar)	Total number of OSPF-related alarms received during the designated time period

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)

Item	Description
Total Alarms chart	<p>Distribution of OSPF-related alarms received during the designated time period, and the total number of current OSPF-related alarms in the network.</p> <p><b>Note:</b> The alarm count here may be different than the count in the summary bar. For example, the number of new alarms received in this time period does not take into account alarms that have already been received and are still active. You might have no new alarms, but still have a total number of alarms present on the network of 10.</p>
Table/Filter options	<p>When the selected filter option is <b>Switches with Most Alarms</b>, the table displays switches and hosts running OSPF in decreasing order of the count of alarms—devices with the largest number of OSPF alarms are listed first</p>
Show All Sessions	<p>Link to view data for all OSPF sessions in the full screen card</p>

The full screen OSPF Service card provides tabs for all switches, all sessions, and all alarms.

The screenshot shows a table titled "Network Services | OSPF" with 11 results. The table has columns: HOSTNAME, TIME, ASIC MOD., AGENT VERSI..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., and PLAT. The data is as follows:

HOSTNAME	TIME	ASIC MOD.	AGENT VERSI...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLAT
noc-pr	Aug 5, 2019, ...	C-Z	2.2.2-cl3u20...	C.2.0	N/A	30 GB	C.2.0	C.\
noc-se	Aug 5, 2019, ...	C-Z	2.2.2-cl3u20...	C.2.0	N/A	30 GB	C.2.0	C.\
spine-1	Aug 5, 2019, ...	B-Z	2.2.2-cl3u20...	B.2.0	bad	20 GB	B.2.0	B.\
spine-2	Aug 5, 2019, ...	F-Z	2.2.2-cl3u20...	F.2.0	bad	10 GB	F.2.0	F.\
spine-3	Aug 5, 2019, ...	H-Z	2.2.2-cl3u20...	H.2.0	missing	10 GB	H.2.0	H.\

Item	Description
Title	Network Services   OSPF

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)

Item	Description
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

All Switches tab	<p>Displays all switches and hosts running the OSPF service. By default, the device list is sorted by <b>hostname</b>. This tab provides the following additional data about each device:</p> <ul style="list-style-type: none"><li>• <b>Agent</b><ul style="list-style-type: none"><li>◦ State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).</li><li>◦ Version: Software version number of the NetQ Agent on a given device. This should match the version number of the NetQ software loaded on your server or appliance; for example, 2.1.0.</li></ul></li><li>• <b>ASIC</b><ul style="list-style-type: none"><li>◦ Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.</li><li>◦ Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.</li><li>◦ Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.</li><li>◦ Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.</li><li>◦ Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.</li></ul></li><li>• <b>CPU</b><ul style="list-style-type: none"><li>◦ Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.</li><li>◦ Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.</li><li>◦ Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.</li><li>◦ Nos: Number of cores. Example values include 2, 4, and 8.</li></ul></li><li>• <b>Disk Total Size:</b> Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.</li><li>• <b>License State:</b> Indicator of validity. Values include ok and bad.</li><li>• <b>Memory Size:</b> Total amount of local RAM. Example values include 8192 MB and 2048 MB</li></ul>
------------------	--

Item	Description
All Sessions tab	<p>Displays all OSPF sessions network-wide. By default, the session list is sorted by <b>hostname</b>. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"> <li>• <b>Area:</b> Routing domain for this host device. Example values include 0.0.0.1, 0.0.0.23.</li> <li>• <b>DB State:</b> Session state of DB</li> <li>• <b>Ifname:</b> Name of the interface on host device where session resides. Example values include swp5, peerlink-1.</li> <li>• <b>Is IPv6:</b> Indicates whether the address of the host device is IPv6 (true) or IPv4 (false)</li> <li>• <b>Peer</b> <ul style="list-style-type: none"> <li>◦ Address: IPv4 or IPv6 address of the peer device</li> <li>◦ Hostname: User-defined name for peer device</li> <li>◦ ID: Network subnet address of router with access to the peer device</li> </ul> </li> <li>• <b>State:</b> Current state of OSPF. Values include Full, 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.</li> <li>• <b>Timestamp:</b> Date and time session was started, deleted, updated or marked dead (device is down)</li> </ul>
All Alarms tab	<p>Displays all OSPF events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of a OSPF-related event. Example: swp4 area ID mismatch with peer leaf02</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of <i>OSPF</i> in this card workflow.</li> </ul>

## Monitor the OSPF Service

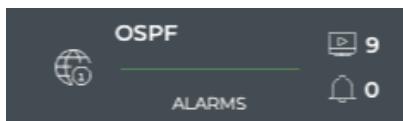
## Monitor the OSPF Service (All Sessions)

Item	Description
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Service Status Summary

A summary of the OSPF service is available from the Network Services card workflow, including the number of nodes running the service, the number of OSPF-related alarms, and a distribution of those alarms.

To view the summary, open the small OSPF Service card.



For more detail, select a different size OSPF Service card.

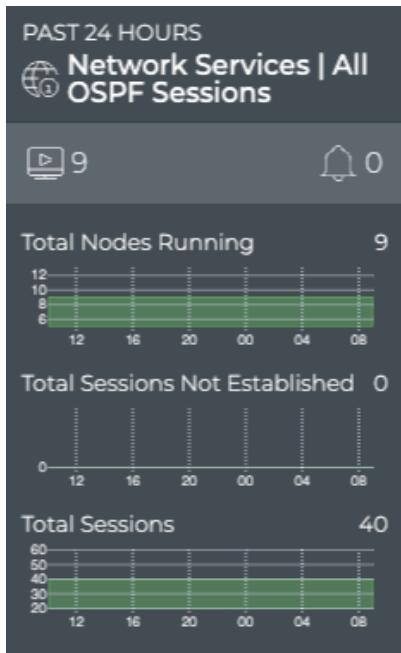
### View the Distribution of Sessions

It is useful to know the number of network nodes running the OSPF protocol over a period of time, as it gives you insight into the amount of traffic associated with and breadth of use of the protocol. It is also useful to view the health of the sessions.

To view these distributions, open the medium OSPF Service card.

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)



You can dig a little deeper with the large OSPF Service card tabs.

### View Devices with the Most OSPF Sessions

You can view the load from OSPF on your switches and hosts using the large Network Services card. This data enables you to see which switches are handling the most OSPF traffic currently, validate that is what is expected based on your network design, and compare that with data from an earlier time to look for any differences.

To view switches and hosts with the most OSPF sessions:

1. Open the large OSPF Service card.
2. Select **Switches with Most Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes running the most OSPF sessions at the top. Scroll down to view those with the fewest sessions.

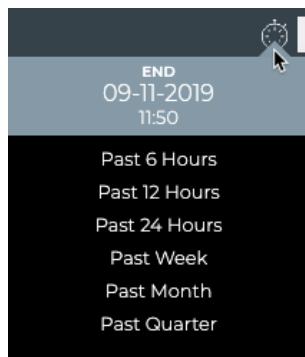
## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)



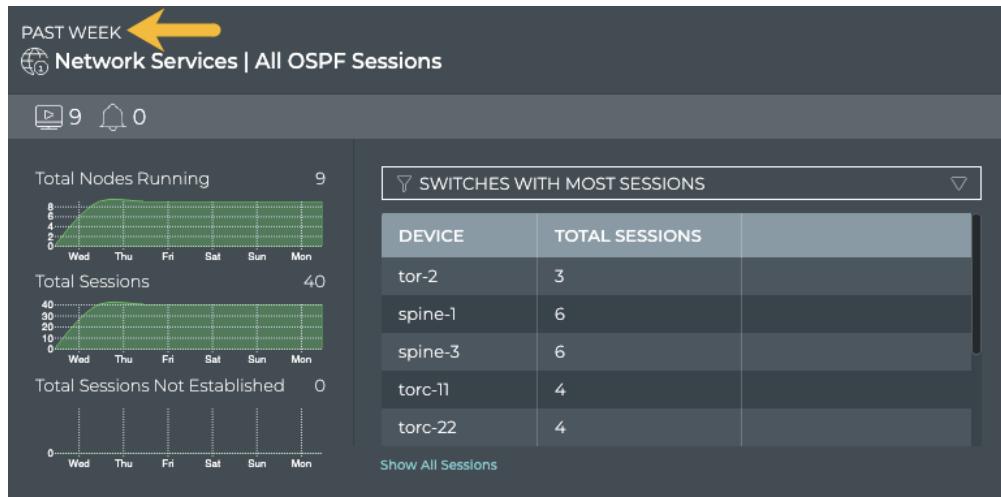
To compare this data with the same data at a previous time:

1. Open another large OSPF Service card.
2. Move the new card next to the original card if needed.
3. Change the time period for the data on the new card by hovering over the card and clicking
4. Select the time period that you want to compare with the original time. We chose *Past Week* for this example.



## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)



You can now see whether there are significant differences between this time and the original time. If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running OSPF than previously, looking for changes in the topology, and so forth.

### View Devices with the Most Unestablished OSPF Sessions

You can identify switches and hosts that are experiencing difficulties establishing OSPF sessions; both currently and in the past.

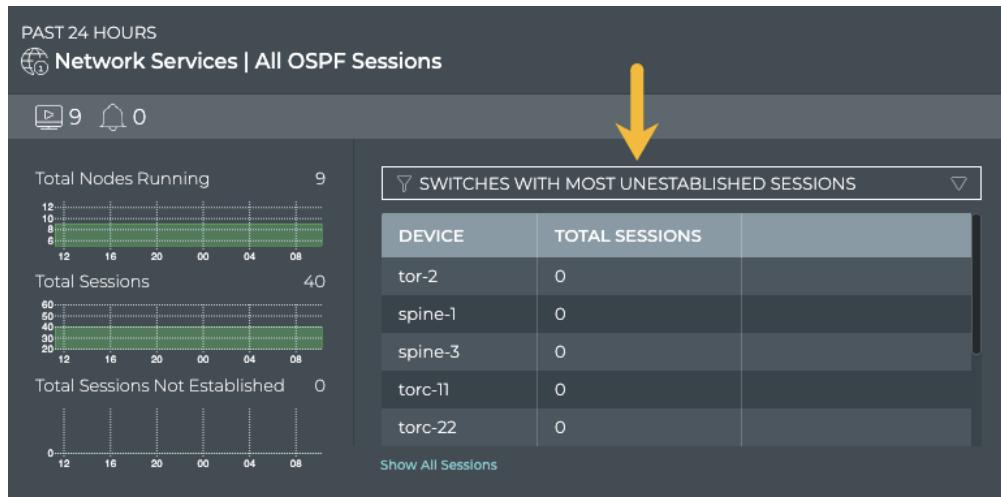
To view switches with the most unestablished OSPF sessions:

1. Open the large OSPF Service card.
2. Select **Switches with Most Unestablished Sessions** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most unestablished OSPF sessions at the top. Scroll down to view those with the fewest unestablished sessions.

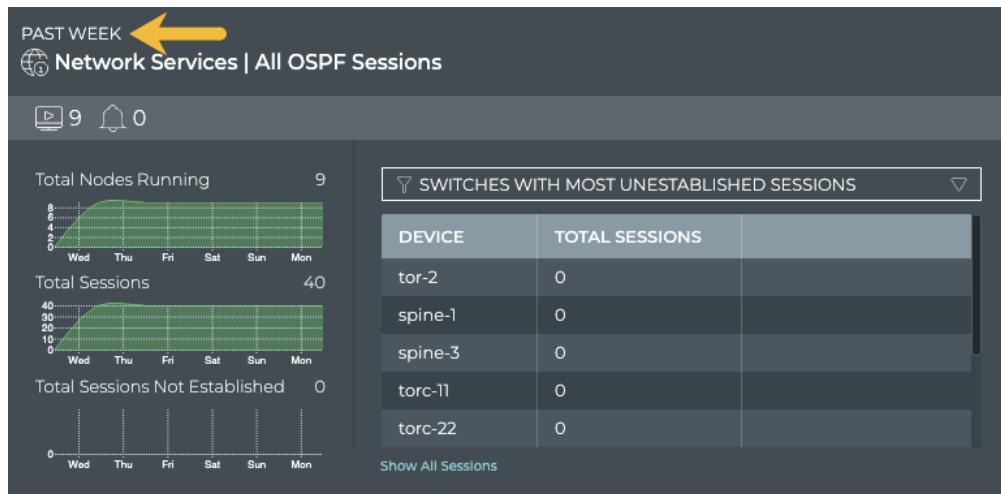
## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)



Where to go next depends on what data you see, but a couple of options include:

- Change the time period for the data to compare with a prior time.



If the same switches are consistently indicating the most unestablished sessions, you might want to look more carefully at those switches using the Switches card workflow to determine probable causes. Refer to [Monitor Switches](#).

- Click **Show All Sessions** to investigate all OSPF sessions with events in the full screen card.

## View Devices with the Most OSPF-related Alarms

Switches or hosts experiencing a large number of OSPF alarms may indicate a configuration or performance issue that needs further investigation. You can view the

devices sorted by the number of OSPF alarms and then use the Switches card workflow or the Alarms card workflow to gather more information about possible causes for the alarms. compare the number of nodes running OSPF with unestablished sessions with the alarms present at the same time to determine if there is any correlation between the issues and the ability to establish a OSPF session.

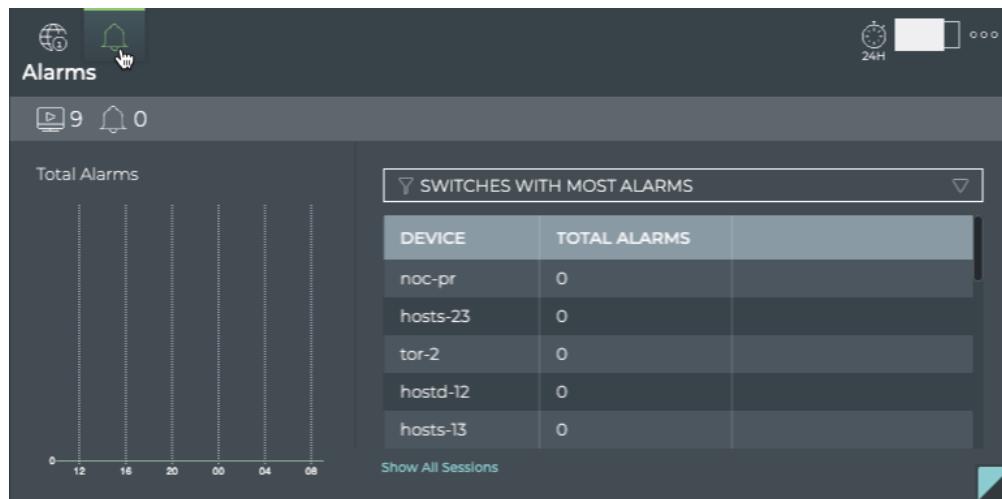
To view switches with the most OSPF alarms:

1. Open the large OSPF Service card.
2. Hover over the header and click



3. Select **Switches with Most Alarms** from the filter above the table.

The table content is sorted by this characteristic, listing nodes with the most OSPF alarms at the top. Scroll down to view those with the fewest alarms.



Where to go next depends on what data you see, but a few options include:

- Change the time period for the data to compare with a prior time. If the same switches are consistently indicating the most alarms, you might want to look more carefully at those switches using the Switches card workflow.
- Click **Show All Sessions** to investigate all OSPF sessions with events in the full screen card.

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)

### View All OSPF Events

The OSPF Network Services card workflow enables you to view all of the OSPF events in the designated time period.

To view all OSPF events:

1. Open the full screen OSPF Service card.
2. Click **All Alarms** tab in the navigation panel.

By default, events are listed in most recent to least recent order.

Where to go next depends on what data you see, but a couple of options include:

- Open one of the other full screen tabs in this flow to focus on devices or sessions.
- Export the data for use in another analytics tool, by clicking **Export** and providing a name for the data file.

### View Details for All Devices Running OSPF

You can view all stored attributes of all switches and hosts running OSPF in your network in the full screen card.

To view all device details, open the full screen OSPF Service card and click the **All Switches** tab.

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PU...
noc-pr	Aug 5, 2019, ...	C-Z	2.2.2-cl3u20...	C.2.0	N/A	30 GB	C.2.0	C.\
noc-se	Aug 5, 2019, ...	C-Z	2.2.2-cl3u20...	C.2.0	N/A	30 GB	C.2.0	C.\
spine-1	Aug 5, 2019, ...	B-Z	2.2.2-cl3u20...	B.2.0	bad	20 GB	B.2.0	B.\
spine-2	Aug 5, 2019, ...	F-Z	2.2.2-cl3u20...	F.2.0	bad	10 GB	F.2.0	F.\
spine-3	Aug 5, 2019, ...	H-Z	2.2.2-cl3u20...	H.2.0	missing	10 GB	H.2.0	H.\

To return to your workbench, click



in the top right corner.

## Monitor the OSPF Service

## Monitor the OSPF Service (All Sessions)

### View Details for All OSPF Sessions

You can view all stored attributes of all OSPF sessions in your network in the full-screen card.

To view all session details, open the full screen OSPF Service card and click the **All Sessions** tab.

The screenshot shows the Network Services | OSPF card with the All Sessions tab selected. The card has a header with a search bar, a time filter set to 'Past 24 Hours', and an 'Export' button. Below the header is a table with 40 results. The columns are: AREA, HOSTNAME, TIMESTAMP, STATE, PEER ADD., DB STATE, IFNAME, PEER HOS..., and PEER IP. The data shows multiple entries for 'spine-1' in area 0.0.0.0.

AREA	HOSTNAME	TIMESTAMP	STATE	PEER ADD...	DB STATE	IFNAME	PEER HOS...	PEER IP
0.0.0.0	spine-1	Aug 7, 2019, ...	Full	27.0.0.18	Refresh	swp7	tor-1	0.0.0.1
0.0.0.0	spine-1	Aug 7, 2019, ...	Full	27.0.0.22	Refresh	swp5	torc-21	0.0.0.1
0.0.0.0	spine-1	Aug 7, 2019, ...	Full	27.0.0.23	Refresh	swp6	torc-22	0.0.0.1
0.0.0.0	spine-1	Aug 7, 2019, ...	Full	27.0.0.19	Refresh	swp8	tor-2	0.0.0.1
0.0.0.0	spine-1	Aug 7, 2019, ...	Full	27.0.0.20	Refresh	swp3	torc-11	0.0.0.1
0.0.0.0	spine-1	Aug 7, 2019, ...	Full	27.0.0.21	Refresh	swp4	torc-12	0.0.0.1

To return to your workbench, click



in the top right corner.

### Take Actions on Data Displayed in Results List

In the full screen OSPF Service card, you can determine which results are displayed in the results list, and which are exported.

To take actions on the data, click in the blank column at the very left of a row. A checkbox appears, selecting that switch, session, or alarm, and an edit menu is shown at the bottom of the card (shown enlarged here).

The screenshot shows the Network Services | OSPF card with the All Sessions tab selected. The card has a header with a search bar, a time filter set to 'Past 24 Hours', and an 'Export' button. Below the header is a table with 11 results. The columns are: HOSTNAME, TIME, ASIC MOD..., AGENT VE..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., and PL. The data shows multiple entries for 'spine-1' and 'spine-2'. At the bottom of the card, there is an edit menu with buttons for 'Select All', 'Clear All', 'Hide Selected', 'Show Only Selected', and 'Export Selected'. A yellow arrow points to the 'spine-1' and 'spine-2' rows in the table.

HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PL
noc-pr	Aug 5, 2019, ...	C-Z	2.2.2-cl3u20...	C.2.0	N/A	30 GB	C.2.0	C.\
noc-se	Aug 5, 2019, ...	C-Z	2.2.2-cl3u20...	C.2.0	N/A	30 GB	C.2.0	C.\
<input checked="" type="checkbox"/> spine-1	Aug 5, 2019, ...	B-Z	2.2.2-cl3u20...	B.2.0	bad	20 GB	B.2.0	B.\
<input checked="" type="checkbox"/> spine-2	Aug 5, 2019, ...	F-Z	2.2.2-cl3u20...	F.2.0	bad	10 GB	F.2.0	F.\
spine-3	Aug 5, 2019, ...	H-Z	2.2.2-cl3u20...	H.2.0	missing	10 GB	H.2.0	H.\
tor-1	Aug 5, 2019, ...	D-Z	2.2.2-cl3u20...	D.2.0	missing	33 GB	D.2.0	D.\

2 ITEMS SELECTED     Select All     Clear All     Hide Selected     Show Only Selected     Export Selected

You can perform the following actions on the results list:

Option	Action or Behavior on Click
Select All	Selects all items in the results list
Clear All	Clears all existing selections of items in the results list. This also hides the edit menu.
Open Cards	Open the corresponding validation or trace result card.
Hide Selected	Hide selected items (switches, sessions, alarms, and so forth) from the results list.
Show Only Selected	Hide unselected items (switches, sessions, alarms, and so forth) from the results list.
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the <b>Export</b> button.

To return to original display of results, click the associated tab.

## Monitor a Single OSPF Session

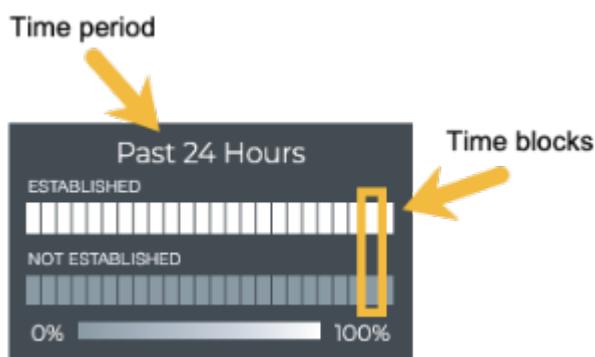
With NetQ, you can monitor a single session of the OSPF service, view session state changes, and compare with alarms occurring at the same time, as well as monitor the running OSPF configuration and changes to the configuration file. For an overview and how to configure OSPF to run in your data center network, refer to [Open Shortest Path First - OSPF](#) or [Open Shortest Path First v3 - OSPFv3](#).

**NOTE**

To access the single session cards, you must open the full screen OSPF Service, click the All Sessions tab, select the desired session, then click  (Open Cards).

**Granularity of Data Shown Based on Time Period**

On the medium and large single OSPF session cards, the status of the sessions is represented in heat maps stacked vertically; one for established sessions, and one for unestablished sessions. Depending on the time period of data on the card, the number of smaller time blocks used to indicate the status varies. A vertical stack of time blocks, one from each map, includes the results from all checks during that time. The results are shown by how saturated the color is for each block. If all sessions during that time period were established for the entire time block, then the top block is 100% saturated (white) and the not established block is zero percent saturated (gray). As sessions that are not established increase in saturation, the sessions that are established block is proportionally reduced in saturation. An example heat map for a time period of 24 hours is shown here with the most common time periods in the table showing the resulting time blocks.



6 hours

18

6

1 hour

## Monitor the OSPF Service

## Monitor a Single OSPF Session

Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

### OSPF Session Card Workflow Summary

The small OSPF Session card displays:



Item	Description
<::>	Indicates data is for a single session of a Network Service or Protocol
Title	OSPF Session
	Hostnames of the two devices in a session. Arrow points from the host to the peer.
(✓) ,(✗)	<p>Current state of OSPF.</p> <p>(✓) Full or (✗) 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.</p>

## Monitor the OSPF Service

## Monitor a Single OSPF Session

The medium OSPF Session card displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
↔	Indicates data is for a single session of a Network Service or Protocol
Title	Network Services   OSPF Session
	Hostnames of the two devices in a session. Arrow points in the direction of the session.

## Monitor the OSPF Service

## Monitor a Single OSPF Session

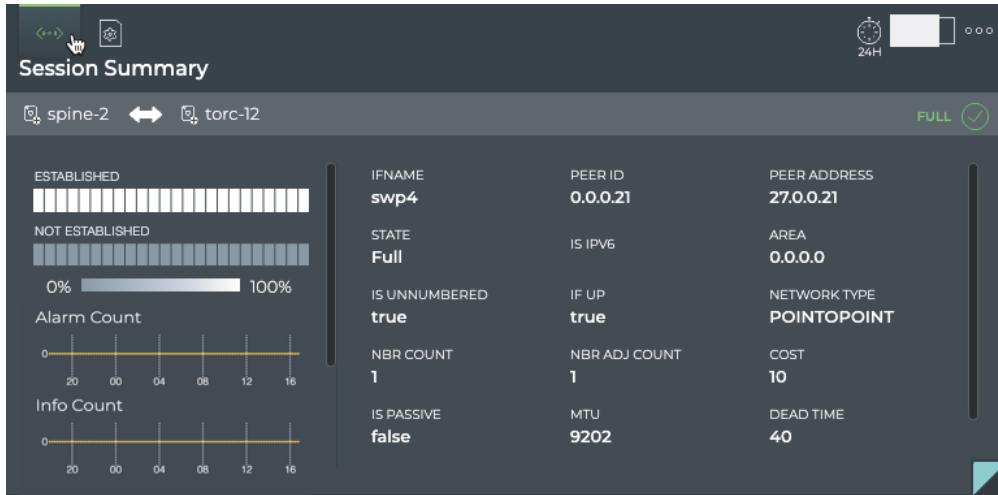
Item	Description
<input checked="" type="checkbox"/> <input type="checkbox"/>	Current state of OSPF.  Full or <input type="checkbox"/> 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.
Time period for chart	Time period for the chart data
Session State Changes Chart	Heat map of the state of the given session over the given time period. The status is sampled at a rate consistent with the time period. For example, for a 24 hour period, a status is collected every hour. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> .
Ifname	Interface name on or hostname for host device where session resides
Peer Address	IP address of the peer device
Peer ID	IP address of router with access to the peer device

The large OSPF Session card contains two tabs.

The *Session Summary* tab displays:

## Monitor the OSPF Service

## Monitor a Single OSPF Session



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
↔	Indicates data is for a single session of a Network Service or Protocol
Title	Session Summary (Network Services   OSPF Session)
Summary bar	Hostnames of the two devices in a session. Arrow points in the direction of the session.
	Current state of OSPF. ✓ Full or ✗ 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.
Session State Changes Chart	Heat map of the state of the given session over the given time period. The status is sampled at a rate consistent with the time period. For example, for a 24 hour period, a status is collected every hour. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> .
Alarm Count Chart	Distribution and count of OSPF alarm events over the given time period

## Monitor the OSPF Service

## Monitor a Single OSPF Session

Item	Description
Info Count Chart	Distribution and count of OSPF info events over the given time period
Ifname	Name of the interface on the host device where the session resides
State	Current state of OSPF. <input checked="" type="radio"/> Full or <input type="radio"/> 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.
Is Unnumbered	Indicates if the session is part of an unnumbered OSPF configuration (true) or part of a numbered OSPF configuration (false)
Nbr Count	Number of routers in the OSPF configuration
Is Passive	Indicates if the host is in a passive state (true) or active state (false).
Peer ID	IP address of router with access to the peer device
Is IPv6	Indicates if the IP address of the host device is IPv6 (true) or IPv4 (false)
If Up	Indicates if the interface on the host is up (true) or down (false)
Nbr Adj Count	Number of adjacent routers for this host
MTU	Maximum transmission unit (MTU) on shortest path between the host and peer
Peer Address	IP address of the peer device
Area	Routing domain of the host device

## Monitor the OSPF Service

## Monitor a Single OSPF Session

Item	Description
Network Type	Architectural design of the network. Values include Point-to-Point and Broadcast.
Cost	Shortest path through the network between the host and peer devices
Dead Time	Countdown timer, starting at 40 seconds, that is constantly reset as messages are heard from the neighbor. If the dead time gets to zero, the neighbor is presumed dead, the adjacency is torn down, and the link removed from SPF calculations in the OSPF database.

The *Configuration File Evolution* tab displays:

The screenshot shows the Configuration File Evolution interface. At the top, it displays two hosts: spine-2 and torc-12. Below the hosts, the date Jun 28, 2019 and time 7:52 AM are shown. On the right, there are buttons for FILE and DIFF, with DIFF being selected. The main area shows configuration differences between the two hosts. The configuration for spine-2 is as follows:

```
1 !
2 hostname spine-2
3 password cn321
4 enable password cn321
5 log timestamp precision 6
6 !
7 log file /var/log/frr/zebra.log
8
9 ip forwarding
```

Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates configuration file information for a single session of a Network Service or Protocol
Title	(Network Services   OSPF Session) Configuration File Evolution

## Monitor the OSPF Service

## Monitor a Single OSPF Session

Item	Description
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Arrow points from the host to the peer. Click  to open associated device card.
	Current state of OSPF.
	Full or 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.
Timestamps	When changes to the configuration file have occurred, the date and time are indicated. Click the time to see the changed file.
Configuration File	When <b>File</b> is selected, the configuration file as it was at the selected time is shown.  When <b>Diff</b> is selected, the configuration file at the selected time is shown on the left and the configuration file at the previous timestamp is shown on the right. Differences are highlighted.

The full screen OSPF Session card provides tabs for all OSPF sessions and all events.

AREA	HOSTNAME	TIMESTAMP	STATE	PEER ADD..	DB STATE	IFNAME	PEER HOS..	PEER ID	IS IPV6
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.23	Update	swp6	torc-22	0.0.0.23	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.19	Update	swp8	tor-2	0.0.0.19	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.20	Update	swp3	torc-11	0.0.0.20	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.21	Update	swp4	torc-12	0.0.0.21	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.22	Update	swp5	torc-21	0.0.0.22	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.18	Update	swp7	tor-1	0.0.0.18	
0.0.0	spine-2	7/2/19 4:01 AM	Full	27.0.0.22	Update	swp5	torc-21	0.0.0.22	

Item	Description
Title	Network Services   OSPF
X	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab
All OSPF Sessions tab	<p>Displays all OSPF sessions running on the host device. The session list is sorted by <b>hostname</b> by default. This tab provides the following additional data about each session:</p> <ul style="list-style-type: none"> <li>• <b>Area:</b> Routing domain for this host device. Example values include 0.0.0.1, 0.0.0.23.</li> <li>• <b>DB State:</b> Session state of DB</li> <li>• <b>Ifname:</b> Name of the interface on host device where session resides. Example values include swp5, peerlink-1.</li> <li>• <b>Is IPv6:</b> Indicates whether the address of the host device is IPv6 (true) or IPv4 (false)</li> <li>• <b>Peer</b> <ul style="list-style-type: none"> <li>◦ Address: IPv4 or IPv6 address of the peer device</li> <li>◦ Hostname: User-defined name for peer device</li> <li>◦ ID: Network subnet address of router with access to the peer device</li> </ul> </li> <li>• <b>State:</b> Current state of OSPF. Values include Full, 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.</li> <li>• <b>Timestamp:</b> Date and time session was started, deleted, updated or marked dead (device is down)</li> </ul>

Item	Description
All Events tab	<p>Displays all events network-wide. By default, the event list is sorted by <b>time</b>, with the most recent events listed first. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li>• <b>Message:</b> Text description of a OSPF-related event. Example: OSPF session with peer tor-1 swp7 vrf default state changed from failed to Established</li> <li>• <b>Source:</b> Hostname of network device that generated the event</li> <li>• <b>Severity:</b> Importance of the event. Values include critical, warning, info, and debug.</li> <li>• <b>Type:</b> Network protocol or service generating the event. This always has a value of OSPF in this card workflow.</li> </ul>
Export	<p>Enables export of all or selected items in a CSV or JSON formatted file</p>
	<p>Enables manipulation of table display; choose columns to display and reorder columns</p>

### View Session Status Summary

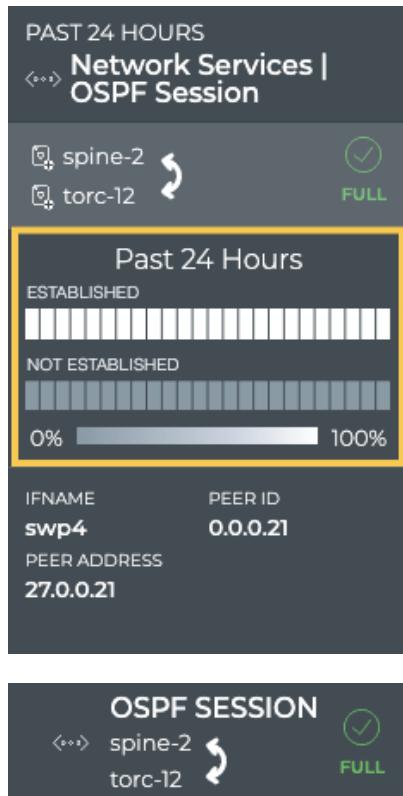
A summary of the OSPF session is available from the OSPF Session card workflow, showing the node and its peer and current status.

To view the summary:

1. Add the Network Services | All OSPF Sessions card.
2. Switch to the full screen card.
3. Click the **All Sessions** tab.
4. Double-click the session of interest. The full screen card closes automatically.
5. Optionally, switch to the small OSPF Session card.

## Monitor the OSPF Service

## Monitor a Single OSPF Session



### View OSPF Session State Changes

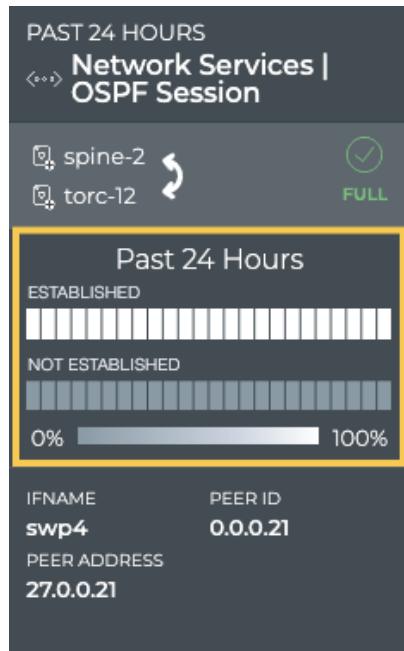
You can view the state of a given OSPF session from the medium and large OSPF Session Network Service cards. For a given time period, you can determine the stability of the OSPF session between two devices. If you experienced connectivity issues at a particular time, you can use these cards to help verify the state of the session. If it was not established more than it was established, you can then investigate further into possible causes.

To view the state transitions for a given OSPF session, on the *medium* OSPF Session card:

1. Add the Network Services | All OSPF Sessions card.
2. Switch to the full screen card.
3. Open the large OSPF Service card.
4. Click the **All Sessions** tab.
5. Double-click the session of interest. The full screen card closes automatically.

## Monitor the OSPF Service

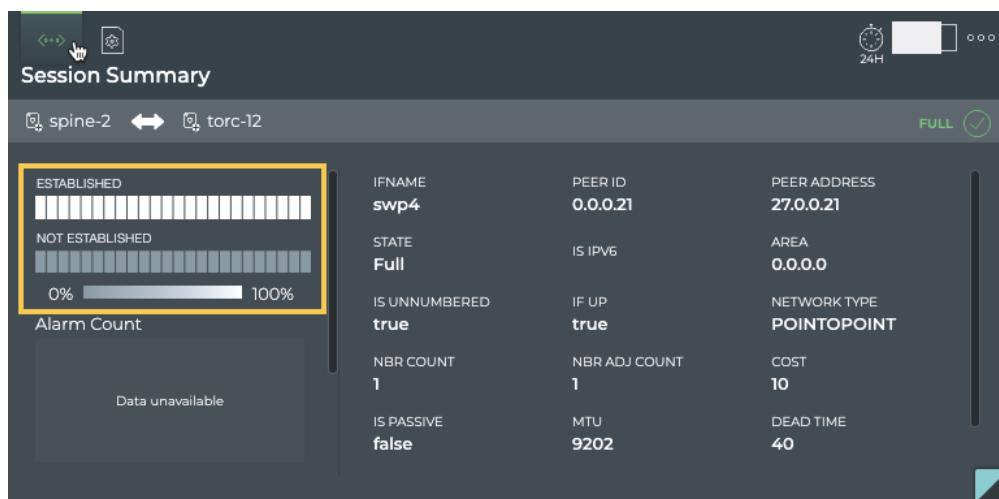
## Monitor a Single OSPF Session



The heat map indicates the status of the session over the designated time period. In this example, the session has been established for the entire time period.

From this card, you can also view the interface name, peer address, and peer id identifying the session in more detail.

To view the state transitions for a given OSPF session on the large OSPF Session card, follow the same steps to open the medium OSPF Session card and then switch to the large card.



From this card, you can view the alarm and info event counts, interface name, peer address and peer id, state, and several other parameters identifying the session in more detail.

### View Changes to the OSPF Service Configuration File

Each time a change is made to the configuration file for the OSPF service, NetQ logs the change and enables you to compare it with the last version. This can be useful when you are troubleshooting potential causes for alarms or sessions losing their connections.

To view the configuration file changes:

1. Open the large OSPF Session card.
2. Hover over the card and click  to open the **Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.
4. Choose between the **File** view and the **Diff** view (selected option is dark; File by default).

The File view displays the content of the file for you to review.



The screenshot shows the 'Configuration File Evolution' interface. At the top, there are icons for a network connection, a gear, and a hand cursor. On the right side of the header are a clock icon labeled '24H', a refresh icon, and three dots. Below the header, the title 'Configuration File Evolution' is displayed, followed by two session names: 'spine-2' and 'torc-12'. To the right of these names is a 'FULL' button with a checkmark. The main area has a dark background. On the left, a sidebar shows the date 'Jun 28, 2019' and a timestamp '7:52 AM' with a blue dot next to it. In the center, there are two tabs: 'FILE' (which is dark) and 'DIFF' (which is light). Below the tabs, a configuration file is listed with line numbers from 1 to 9. The configuration file content is as follows:

```
1 !
2 hostname spine-2
3 password cn321
4 enable password cn321
5 log timestamp precision 6
6 !
7 log file /var/log/frr/zebra.log
8
9 ip forwarding
```

## Monitor the OSPF Service

## Monitor a Single OSPF Session

The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted in red and green. In this example, we don't have a change to highlight, so it shows the same file on both sides.

PAST 24 HOURS  
Network Services | OSPF Session

spine-2 ↔ torc-12 FULL ✓

Jun 28, 2019 • 7:52 AM

FILE DIFF

1	!	1	!
2	hostname spine-2	2	hostname spine-2
3	password cn321	3	password cn321
4	enable password cn321	4	enable password cn321
5	log timestamp precision 6	5	log timestamp precision 6
6	!	6	!
7	log file /var/log/frr/zebra.log	7	log file /var/log/frr/zebra.log
8		8	

### View All OSPF Session Details

You can view all stored attributes of all of the OSPF sessions associated with the two devices on this card.

To view all session details, open the full screen OSPF Session card, and click the **All OSPF Sessions** tab.

Network Services | OSPF

DEFAULT TIME Past Week

All OSPF Sessions

All Events

Export

40 RESULTS

AREA	HOSTNAME	TIMESTAMP	STATE	PEER ADD...	DB STATE	IFNAME	PEER HOS...	PEER ID	IS IPV6
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.23	Update	swp6	torc-22	0.0.0.23	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.19	Update	swp8	tor-2	0.0.0.19	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.20	Update	swp3	torc-11	0.0.0.20	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.21	Update	swp4	torc-12	0.0.0.21	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.22	Update	swp5	torc-21	0.0.0.22	
0.0.0	spine-1	7/2/19 4:01 AM	Full	27.0.0.18	Update	swp7	tor-1	0.0.0.18	
0.0.0	spine-2	7/2/19 4:01 AM	Full	27.0.0.22	Update	swp5	torc-21	0.0.0.22	

To return to your workbench, click



in the top right corner.

### View All Events

You can view all of the alarm and info events for the two devices on this card.

## Monitor the OSPF Service

## Monitor a Single OSPF Session

To view all events, open the full screen OSPF Session card, and click the **All Events** tab.

To return to your workbench, click



in the top right corner.

# Monitor Network Connectivity

It is helpful to verify that communications are freely flowing between the various devices in your network. You can verify the connectivity between two devices in both an adhoc fashion and by defining connectivity checks to occur on a scheduled basis. There are three card workflows which enable you to view connectivity, the Trace Request, On-demand Trace Results, and Scheduled Trace Results.

## Create a Trace Request

Two types of connectivity checks can be run—an immediate (on-demand) trace and a scheduled trace. The Trace Request card workflow is used to configure and run both of these trace types.

### Trace Request Card Workflow Summary

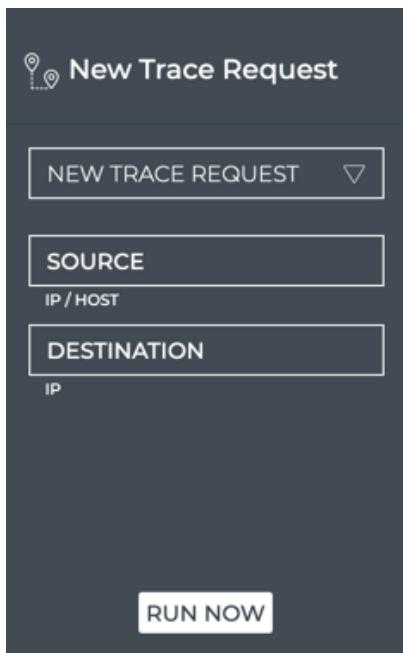
The small Trace Request card displays:



Item	Description
📍	Indicates a trace request
Select Trace list	Select a scheduled trace request from the list

Item	Description
Go	Click to start the trace now

The medium Trace Request card displays:



Item	Description
📍	Indicates a trace request
Title	New Trace Request
New Trace Request	Create a new layer 3 trace request. Use the large Trace Request card to create a new layer 2 or 3 request.
Source	(Required) Hostname or IP address of device where to begin the trace

Item	Description
Destination	(Required) IP address of device where to end the trace
Run Now	Start the trace now

The large Trace Request card displays:

New Trace Request

NEW TRACE REQUEST ▾

SOURCE  
IP / HOST

DESTINATION  
IP / MAC

SCHEDULE:  
Run every HOUR  
Starting DATE / TIME 9/10/19 15:42

Scheduled Traces Remaining 13 ( Limit : 15 )

RUN NOW UPDATE SAVE AS NEW

Item	Description
📍	Indicates a trace request
Title	New Trace Request
Trace selection	Leave <i>New Trace Request</i> selected to create a new request, or choose a scheduled request from the list.
Source	(Required) Hostname or IP address of device where to begin the trace.

Item	Description
Destination	(Required) Ending point for the trace. For layer 2 traces, value must be a MAC address. For layer 3 traces, value must be an IP address.
VRF	Optional for layer 3 traces. Virtual Route Forwarding interface to be used as part of the trace path.
VLAN ID	Required for layer 2 traces. Virtual LAN to be used as part of the trace path.
Schedule	Sets the frequency with which to run a new trace ( <b>Run every</b> ) and when to start the trace for the first time ( <b>Starting</b> ).
Run Now	Start the trace now
Update	<b>Update</b> is available when a scheduled trace request is selected from the dropdown list and you make a change to its configuration. Clicking <b>Update</b> saves the changes to the <i>existing</i> scheduled trace.
Save As New	<p><b>Save As New</b> is available in two instances:</p> <ul style="list-style-type: none"> <li>When you enter a source, destination, and schedule for a new trace. Clicking <b>Save As New</b> in this instance saves the new scheduled trace.</li> <li>When changes are made to a selected scheduled trace request. Clicking <b>Save As New</b> in this instance saves the modified scheduled trace <i>without</i> changing the original trace on which it was based.</li> </ul>

The full screen Trace Request card displays:

Trace Management						
DEFAULT TIME Past 24 Hours		3 RESULTS				
Schedule Preview		Export				
ACTION	FREQUENCY	ACTIVE	ID	START TIME	TRACE NAME	TRACE PARAMS
Add	30	true	c69c427...	7/2/19 2:30 PM	leaf01-00:03:00:33:33:01-vfl3-30min	(alert_on_failure:1;dst:0...
Update	30	true	798230...	7/2/19 2:05 PM	server02-10.1.3.103-30min	(alert_on_failure:1;dst:1...
delete	30	false	37cd0b...	1/18/70 16:36	test-trace-00(old)	(alert_on_failure:1;dst:0...

Item	Description
Title	Trace Request
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab
Schedule Preview tab	<p>Displays all scheduled trace requests for the given user. By default, the listing is sorted by <b>Start Time</b>, with the most recently started traces listed at the top. The tab provides the following additional data about each event:</p> <ul style="list-style-type: none"> <li><b>Action:</b> Indicates latest action taken on the trace job. Values include Add, Deleted, Update.</li> <li><b>Frequency:</b> How often the trace is scheduled to run</li> <li><b>Active:</b> Indicates if trace is actively running (true), or stopped from running (false)</li> <li><b>ID:</b> Internal system identifier for the trace job</li> <li><b>Trace Name:</b> User-defined name for a trace</li> <li><b>Trace Params:</b> Indicates source and destination, optional VLAN or VRF specified, and whether to alert on failure</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file

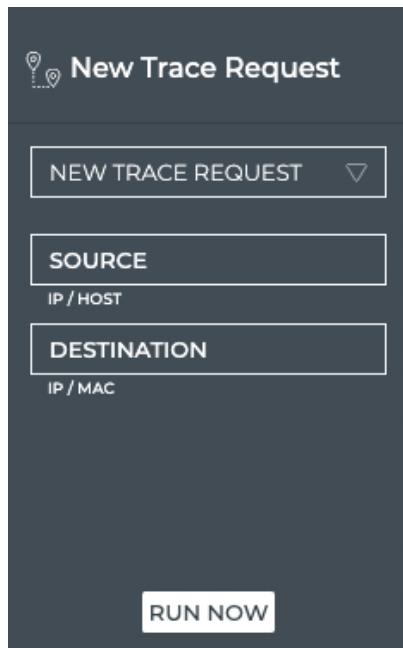
Item	Description
	Enables manipulation of table display; choose columns to display and reorder columns

### Create a Layer 3 On-demand Trace Request

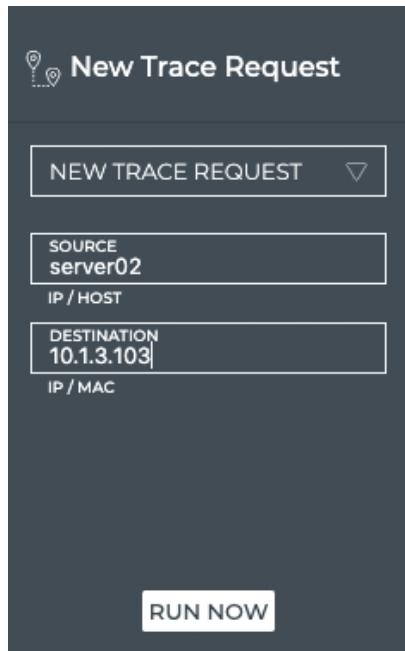
It is helpful to verify the connectivity between two devices when you suspect an issue is preventing proper communication between them. If you cannot find a path through a layer 3 path, you might also try checking connectivity through a layer 2 path.

To create a layer 3 trace request:

1. Open the medium Trace Request card.



2. In the **Source** field, enter the hostname or IP address of the device where you want to start the trace.
3. In the **Destination** field, enter the IP address of the device where you want to end the trace.



In this example, we are starting our trace at *server02* and ending it at *10.1.3.103*.

TIP

If you mistype an address, you must double-click it, or backspace over the error, and retype the address. You cannot select the address by dragging over it as this action attempts to move the card to another location.

4. Click **Run Now**. A corresponding Trace Results card is opened on your workbench.

Refer to [View Layer 3 Trace Results](#) for details.

#### Create a Layer 3 Trace Through a Given VRF

If you want to guide a trace through a particular VRF interface, you can do so using the large New Trace Request card.

To create the trace request:

1. Open the large Trace Request card.

2. In the **Source** field, enter the hostname or IP address of the device where you want to start the trace.
3. In the **Destination** field, enter the IP address of the device where you want to end the trace.
4. In the **VRF** field, enter the identifier for the VRF interface you want to use.

The screenshot shows the 'New Trace Request' card with the following details:

- SOURCE:** leaf01 (IP / HOST)
- DESTINATION:** 10.1.3.103 (IP / MAC)
- VRF:** vrf1
- SCHEDULE:**
  - Run every HOUR
  - Starting DATE / TIME: 9/11/19 18:08
- Scheduled Traces Remaining:** 13 (Limit: 15)
- Buttons:** RUN NOW, UPDATE, SAVE AS NEW

In this example, we are starting our trace at *leaf01* and ending it at *10.1.3.103* using VRF *vrf1*.

5. Click **Run Now**. A corresponding Trace Results card is opened on your workbench. Refer to [View Layer 3 Trace Results](#) for details.

### Create a Layer 2 Trace

It is helpful to verify the connectivity between two devices when you suspect an issue is preventing proper communication between them. If you cannot find a path through a layer 2 path, you might also try checking connectivity through a layer 3 path.

To create a layer 2 trace request:

1. Open the large Trace Request card.
2. In the **Source** field, enter the hostname or IP address of the device where you want to start the trace.
3. In the **Destination** field, enter the MAC address for where you want to end the trace.

4. In the **VLAN ID** field, enter the identifier for the VLAN you want to use.

The screenshot shows the 'New Trace Request' card with the following configuration:

- SOURCE:** leaf01 (IP / HOST)
- DESTINATION:** 00:03:00:33:33:01 (IP / MAC)
- VRF:** vrf1
- VLAN ID:** 13
- SCHEDULE:**
  - Run every: HOUR
  - Starting: DATE / TIME: 9/11/19 18:08
- Scheduled Traces Remaining:** 13 (Limit: 15)

At the bottom are three buttons: RUN NOW, UPDATE, and SAVE AS NEW.

In this example, we are starting our trace at *leaf01* and ending it at *00:03:00:33:33:01* using VLAN 13.

5. Click **Run Now**. A corresponding Trace Results card is opened on your workbench.

Refer to [View Layer 2 Trace Results](#) for details.

#### Create a Trace to Run on a Regular Basis (Scheduled Trace)

There may be paths through your network that you consider critical to your everyday or particularly important operations. In that case, it might be useful to create one or more traces to periodically confirm that at least one path is available between the relevant two devices. Scheduling a trace request can be performed from the large Trace Request card.

To schedule a trace:

1. Open the large Trace Request card.
2. In the **Source** field, enter the hostname or IP address of the device where you want to start the trace.
3. In the **Destination** field, enter the MAC address (layer 2) or IP address (layer 3) of the device where you want to end the trace.
4. Optionally, enter a VLAN ID (layer 2) or VRF interface (layer 3).

## Monitor Network Connectivity

## Create a Trace Request

The screenshot shows the 'New Trace Request' page. At the top, there's a header with a location pin icon and the text 'New Trace Request'. Below it, a dropdown menu says 'NEW TRACE REQUEST'. The form fields include:

- SOURCE:** leaf01 (IP / HOST)
- DESTINATION:** 00:03:00:33:33:01 (IP / HOST)
- VRF:** (empty field)
- VLAN ID:** 13
- SCHEDULE:**
  - Run every: HOUR (selected)
  - Starting: 8/5/19 11:43
- Scheduled Traces:** 2/15

At the bottom are three buttons: 'RUN NOW', 'UPDATE', and 'SAVE AS NEW'.

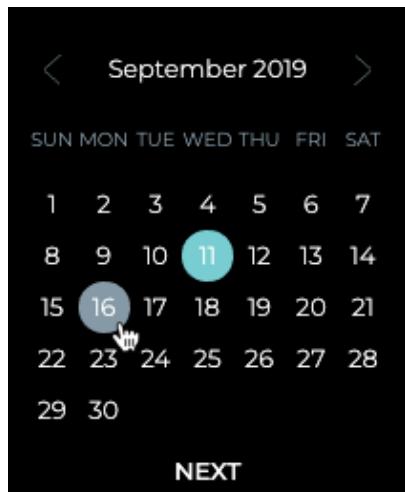
5. Select a timeframe under **Schedule** to specify how often you want to run the trace.

The screenshot shows the 'SCHEDULE:' dropdown menu. It includes:

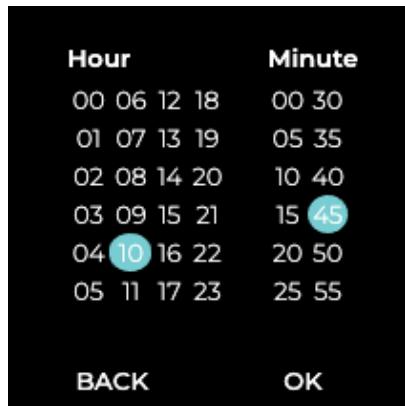
- Run every: HOUR (selected)
- Starting: 30 minutes, Hour, 3 Hours, 6 Hours, 12 Hours, Day
- Last Run: N/A

Below the dropdown are 'RUN NOW' and 'UPDATE' buttons.

6. Accept the default starting time, or click in the **Starting** field to specify the day you want the trace to run for the first time.



7. Click **Next**.
8. Click the time you want the trace to run for the first time.



9. Click **OK**.
10. Verify your entries are correct, then click **Save As New**.
11. Provide a name for the trace. **Note:** This name must be unique for a given user.



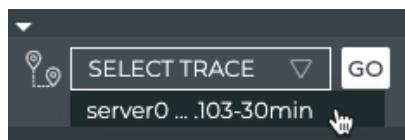
12. Click **Save**. You can now run this trace on demand by selecting it from the dropdown list, or wait for it to run on its defined schedule.

#### Run a Scheduled Trace on Demand

You may find that, although you have a schedule for a particular trace, you want to have visibility into the connectivity data now. You can run a scheduled trace on demand from the small, medium and large Trace Request cards.

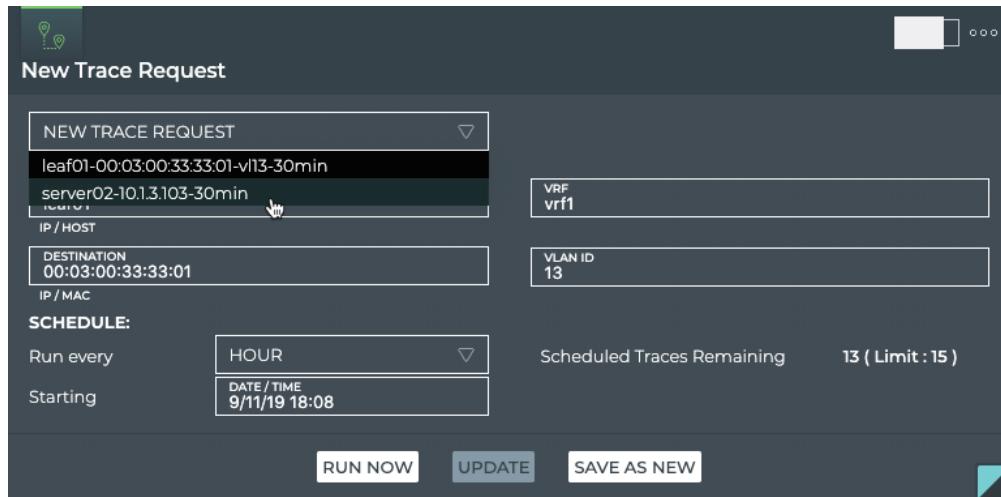
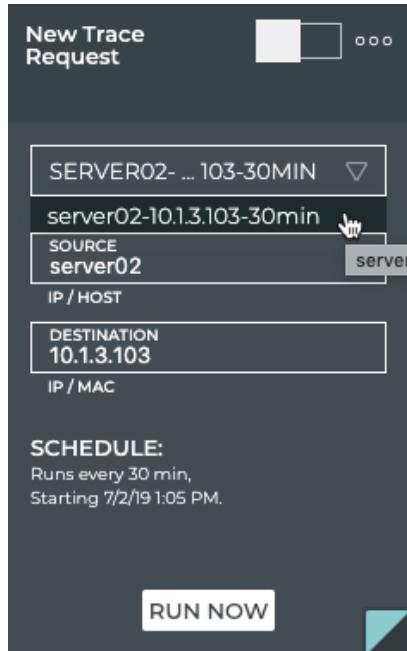
To run a scheduled trace now:

1. Open the small or medium or large Trace Request card.



## Monitor Network Connectivity

## Create a Trace Request



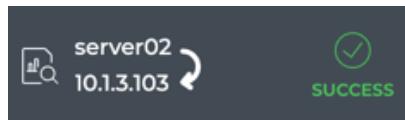
2. Select the scheduled trace from the **Select Trace or New Trace Request** list. **Note:** In the medium and large cards, the trace details are filled in on selection of the scheduled trace.
3. Click **Go** or **Run Now**. A corresponding Trace Results card is opened on your workbench.

## View On-demand Trace Results

Once you have started an on-demand trace, the results are displayed in the medium Trace Results card by default. You may view the results in more or less detail by switching to the large or small Trace Results card, respectively.

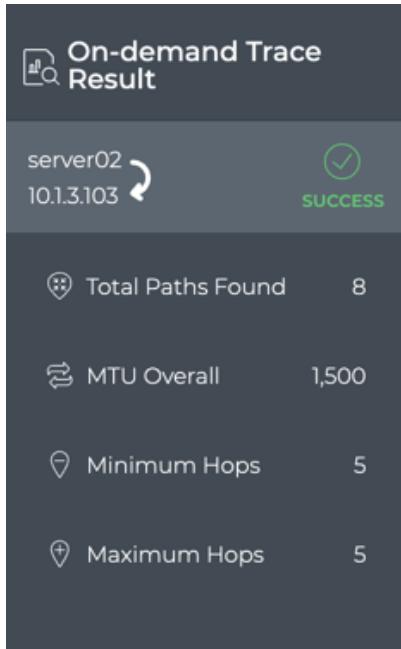
### On-demand Trace Results Card Workflow Summary

The small On-demand Trace Results card displays:



Item	Description
	Indicates an on-demand trace result
	Source and destination of the trace, identified by their address or hostname. Source is listed on top with arrow pointing to destination.
	Indicates success or failure of the trace request. A successful result implies all paths were successful without any warnings or failures. A failure result implies there was at least one path with warnings or errors.

The medium On-demand Trace Results card displays:

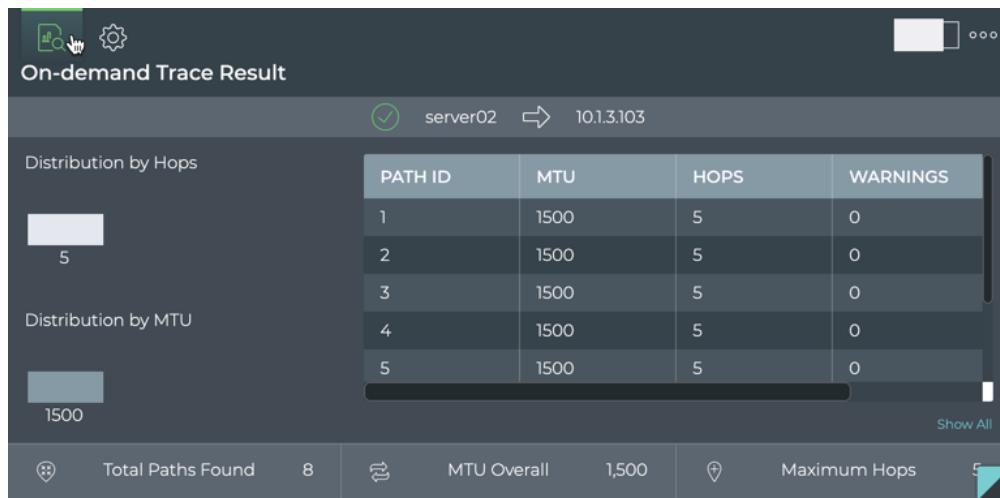


Item	Description
	Indicates an on-demand trace result
Title	On-demand Trace Result
	Source and destination of the trace, identified by their address or hostname. Source is listed on top with arrow pointing to destination.
,	Indicates success or failure of the trace request. A successful result implies all paths were successful without any warnings or failures. A failure result implies there was at least one path with warnings or errors.
Total Paths Found	Number of paths found between the two devices

Item	Description
MTU Overall	Average size of the maximum transmission unit for all paths
Minimum Hops	Smallest number of hops along a path between the devices
Maximum Hops	Largest number of hops along a path between the devices

The large On-demand Trace Results card contains two tabs.

The *On-demand Trace Result* tab displays:

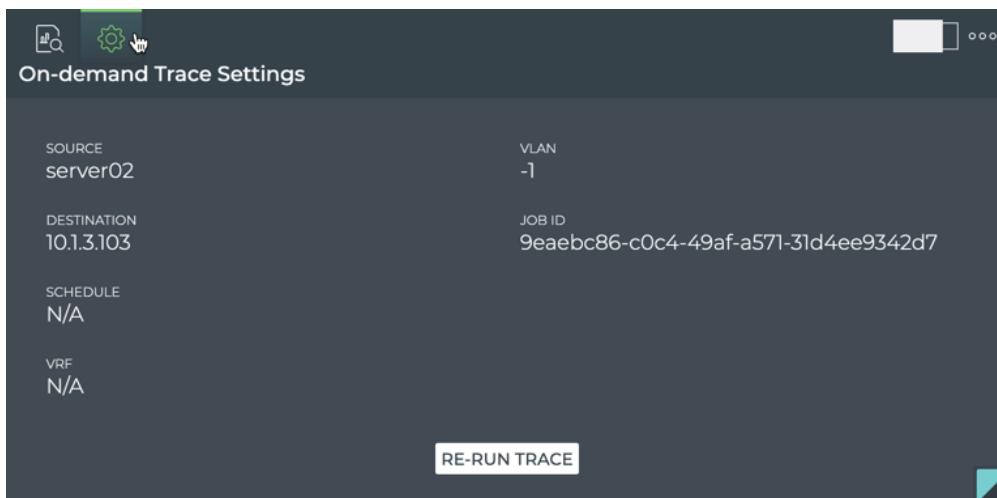


Item	Description
	Indicates an on-demand trace result
Title	On-demand Trace Result

Item	Description
 	Indicates success or failure of the trace request. A successful result implies all paths were successful without any warnings or failures. A failure result implies there was at least one path with warnings or errors.
	Source and destination of the trace, identified by their address or hostname. Source is listed on top with arrow pointing to destination.
Distribution by Hops chart	Displays the distributions of various hop counts for the available paths
Distribution by MTU chart	Displays the distribution of MTUs used on the interfaces used in the available paths
Table	<p>Provides detailed path information, sorted by the route identifier, including:</p> <ul style="list-style-type: none"> <li>• <b>Route ID:</b> Identifier of each path</li> <li>• <b>MTU:</b> Average speed of the interfaces used</li> <li>• <b>Hops:</b> Number of hops to get from the source to the destination device</li> <li>• <b>Warnings:</b> Number of warnings encountered during the trace on a given path</li> <li>• <b>Errors:</b> Number of errors encountered during the trace on a given path</li> </ul>
Total Paths Found	Number of paths found between the two devices

Item	Description
MTU Overall	Average size of the maximum transmission unit for all paths
Minimum Hops	Smallest number of hops along a path between the devices

The *On-demand Trace Settings* tab displays:



Item	Description
	Indicates an on-demand trace setting
Title	On-demand Trace Settings
Source	Starting point for the trace
Destination	Ending point for the trace
Schedule	Does not apply to on-demand traces

Item	Description
VRF	Associated virtual route forwarding interface, when used with layer 3 traces
VLAN	Associated virtual local area network, when used with layer 2 traces
Job ID	Identifier of the job; used internally
Re-run Trace	Clicking this button runs the trace again

The full screen On-demand Trace Results card displays:

The screenshot shows the 'Trace Management' card with the following details:

- Time Period:** DEFAULT TIME Past 24 Hours
- Results:** 1 RESULTS
- Schedule Preview:** (highlighted)
- Export:** (button)
- Settings:** (gear icon)

TRACE NA...	ACTION	FREQUEN...	ACTIVE	ID	START TIME	TRACE PA...
Server02	Add	60	true	44889ee8-5...	9/30/19 10:19 ...	[alert_on_fai...

Item	Description
Title	On-demand Trace Results
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

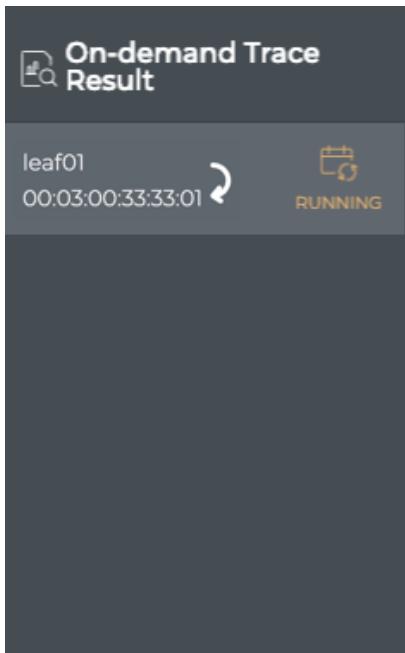
Item	Description
Trace Results tab	<p>Provides detailed path information, sorted by the <b>Resolution Time</b> (date and time results completed), including:</p> <ul style="list-style-type: none"><li>• <b>SCR.IP</b>: Source IP address</li><li>• <b>DST.IP</b>: Destination IP address</li><li>• <b>Max Hop Count</b>: Largest number of hops along a path between the devices</li><li>• <b>Min Hop Count</b>: Smallest number of hops along a path between the devices</li><li>• <b>Total Paths</b>: Number of paths found between the two devices</li><li>• <b>PMTU</b>: Average size of the maximum transmission unit for all interfaces along the paths</li><li>• <b>Errors</b>: Message provided for analysis when a trace fails</li></ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View Layer 2 Trace Results

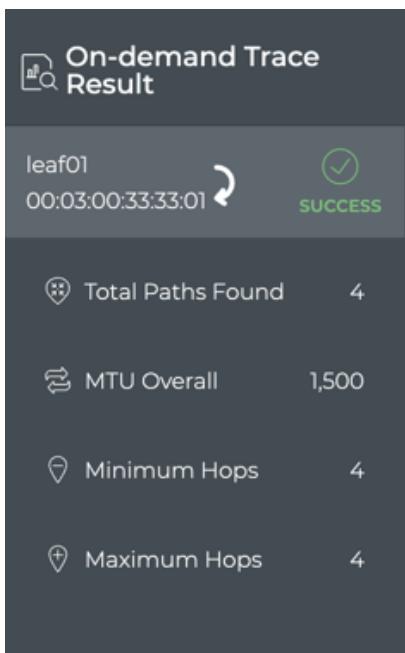
When you start the trace, the corresponding results card is opened on your workbench. While it is working on the trace, a notice is shown on the card indicating it is running.

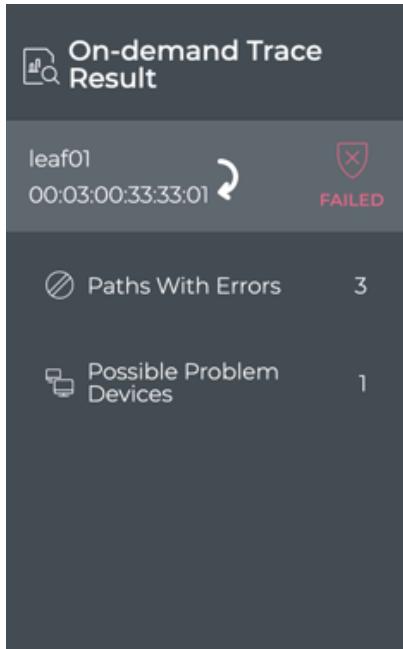
## Monitor Network Connectivity

[View On-demand Trace Results](#)



Once the job is completed, the results are displayed.





In this example, we see that the trace was successful. Four paths were found between the devices, each with four hops and with an overall MTU of 1500. If there was a difference between the minimum and maximum number of hops or other failures, viewing the results on the large card would provide additional information.

A large screenshot of the On-demand Trace Result interface. At the top, it shows the source 'server02' and destination '10.1.3.103'. Below this, there are two main sections: 'Distribution by Hops' and 'Distribution by MTU'.

PATH ID	MTU	HOPS	WARNINGS
1	1500	5	0
2	1500	5	0
3	1500	5	0
4	1500	5	0
5	1500	5	0

At the bottom, there are summary statistics: 'Total Paths Found' (8), 'MTU Overall' (1,500), and 'Maximum Hops' (5).

## Monitor Network Connectivity

## View On-demand Trace Results

The screenshot shows the 'On-demand Trace Result' card for a trace from 'leaf01' to 'leaf01' at '00:03:00:33:33:01'. It includes a distribution chart for hops (one hop) and a table for MTU values. A 'Show All' link is present. Below the card are summary metrics: 3 paths with errors and 1 possible problem device.

PATH ID	MTU	HOPS	WARNINGS
1	null	1	0
2	null	1	0

Distribution by MTU

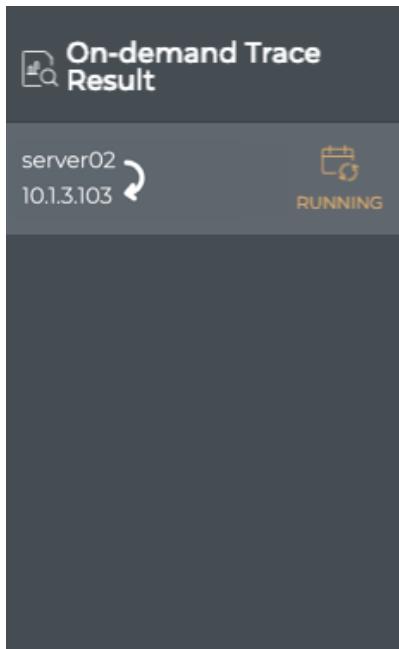
Show All

Paths With Errors 3 | Possible Problem Devices 1

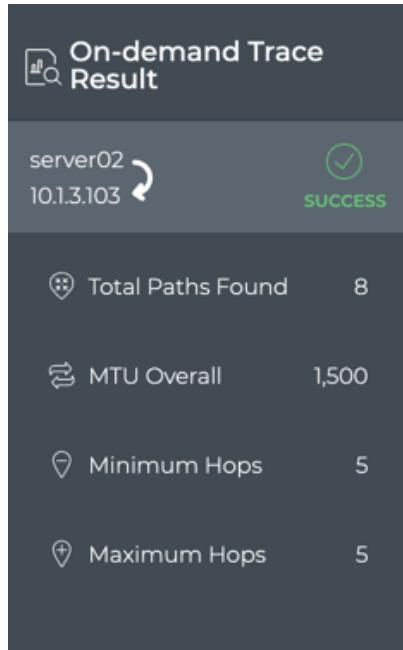
In our example, we can verify that every path option had four hops since the distribution chart only shows one hop count and the table indicates each path had a value of four hops. Similarly, you can view the MTU data. If there had been any warnings, the count would have been visible in the table.

## View Layer 3 Trace Results

When you start the trace, the corresponding results card is opened on your workbench. While it is working on the trace, a notice is shown on the card indicating it is running.



Once results are obtained, it displays them. Using our example from earlier, the following results are shown:



In this example, we see that the trace was successful. Six paths were found between the devices, each with five hops and with an overall MTU of 1500. If there was a difference between the minimum and maximum number of hops or other failures, viewing the results on the large card would provide additional information.

The image shows a larger, more detailed view of the "On-demand Trace Result" card. At the top, it shows the source device "server02" and destination IP "10.1.3.103" with a green checkmark icon. Below this, there are two tables: "Distribution by Hops" and "Distribution by MTU".

**Distribution by Hops**

HOPS
5

**Distribution by MTU**

MTU
1500

At the bottom of the card, there are three summary statistics: "Total Paths Found" (8), "MTU Overall" (1,500), and "Maximum Hops" (5). There is also a "Show All" link next to the MTU distribution table.

In our example, we can verify that every path option had five hops since the distribution chart only shows one hop count and the table indicates each path had a value of five.

hops. Similarly, you can view the MTU data. If there had been any warnings, the count would have been visible in the table.

## View Scheduled Trace Results

You can view the results of scheduled traces at any time. Results are displayed on the Scheduled Trace Results cards.

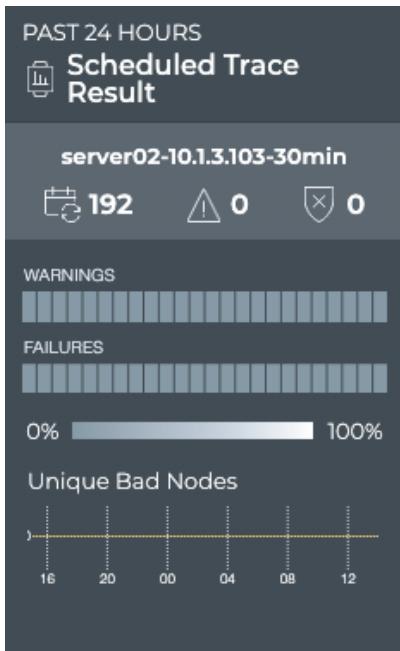
### Scheduled Trace Results Card Workflow Summary

The small Scheduled Trace Results card displays:



Item	Description
<span style="font-size: 2em;">⌚</span>	Indicates a scheduled trace result
<span style="font-size: 2em;">➔</span>	Source and destination of the trace, identified by their address or hostname. Source is listed on left with arrow pointing to destination.
<span style="font-size: 2em;">📋</span>	Summary of trace results: a successful result implies all paths were successful without any warnings or failures; a failure result implies there was at least one path with warnings or errors. <ul style="list-style-type: none"><li> • Number of trace runs completed in the designated time period</li><li> • Number of runs with warnings</li><li> • Number of runs with errors</li></ul>

The medium Scheduled Trace Results card displays:

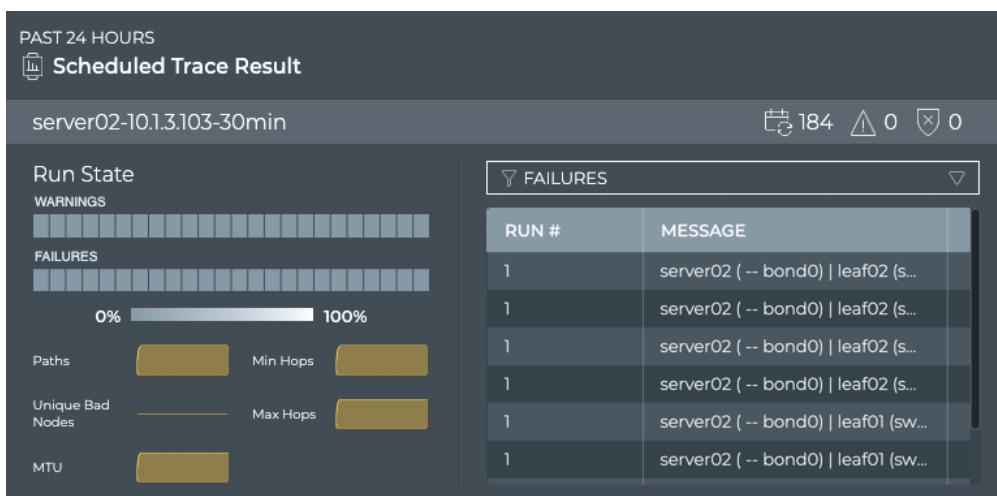


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates a scheduled trace result
Title	Scheduled Trace Result
Summary	<p>Name of scheduled validation and summary of trace results: a successful result implies all paths were successful without any warnings or failures; a failure result implies there was at least one path with warnings or errors.</p> <p></p> <ul style="list-style-type: none"> <li>• Number of trace runs completed in the designated time period</li> <li>• Number of runs with warnings</li> <li>• Number of runs with errors</li> </ul>

Item	Description
Charts	<p><b>Heat map:</b> A time segmented view of the results. For each time segment, the color represents the percentage of warning and failed results. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> for details on how to interpret the results.</p> <p><b>Unique Bad Nodes:</b> Distribution of unique nodes that generated the indicated warnings and/or failures</p>

The large Scheduled Trace Results card contains two tabs:

The *Results* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates a scheduled trace result
Title	Scheduled Trace Result

Item	Description
Summary	<p>Name of scheduled validation and summary of trace results: a successful result implies all paths were successful without any warnings or failures; a failure result implies there was at least one path with warnings or errors.</p> <ul style="list-style-type: none"> <li> • Number of trace runs completed in the designated time period</li> <li> • Number of runs with warnings</li> <li> • Number of runs with errors</li> </ul>
Charts	<p><b>Heat map:</b> A time segmented view of the results. For each time segment, the color represents the percentage of warning and failed results. Refer to <a href="#">Granularity of Data Shown Based on Time Period</a> for details on how to interpret the results.</p> <p><b>Small charts:</b> Display counts for each item during the same time period, for the purpose of correlating with the warnings and errors shown in the heat map.</p>
Table/ Filter options	<p>When the <b>Failures</b> filter option is selected, the table displays the failure messages received for each run.</p> <p>When the <b>Paths</b> filter option is selected, the table displays all of the paths tried during each run.</p> <p>When the <b>Warning</b> filter option is selected, the table displays the warning messages received for each run.</p>

The *Configuration* tab displays:

PAST 24 HOURS

 **Scheduled Trace Result**

SOURCE server02	VRF N/A
DESTINATION 10.1.3.103	VLAN -1
START TIME 7/2/19 14:05	NAME server02-10.1.3.103-30min
REPEATS EVERY 30 minutes	

[RUN NOW](#) [EDIT](#)

Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates a scheduled trace configuration
Title	Scheduled Trace Configuration (Scheduled Trace Result)
Source	Address or hostname of the device where the trace was started
Destination	Address of the device where the trace was stopped
Schedule	The frequency and starting date and time to run the trace
VRF	Virtual Route Forwarding interface, when defined
VLAN	Virtual LAN identifier, when defined
Name	User-defined name of the scheduled trace

Item	Description
Run Now	Start the trace now
Edit	Modify the trace. Opens Trace Request card with this information pre-populated.

The full screen Scheduled Trace Results card displays:

The screenshot shows a full-screen card titled "Scheduled Trace Results". At the top left is a clock icon with the text "DEFAULT TIME Past 24 Hours" and a dropdown arrow. On the right is a "4 RESULTS" indicator and a gear icon. Below the title is a "Scheduled Trace Results" section with a "Export" button. The main area is a table with the following data:

RESOLUTION TIME	SRC. IP	DST. IP	MAX HOP COUNT	MIN HOP COUNT	TOTAL PATHS	PMTU
May 8, 2019, 2:29 pm	27.0.0.19	27.0.0.20	3	3	6	9202
May 8, 2019, 1:29 pm	27.0.0.19	27.0.0.20	3	3	6	9202
May 8, 2019, 12:29 pm	27.0.0.19	27.0.0.20	3	3	6	9202
May 8, 2019, 11:29 am	27.0.0.19	27.0.0.20	3	3	6	9202

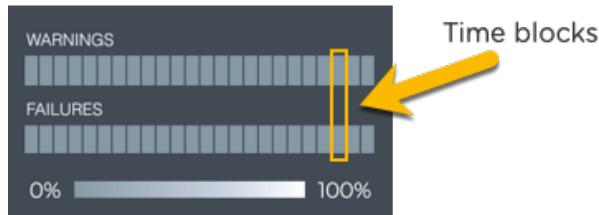
Item	Description
Title	Scheduled Trace Results
×	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab

Item	Description
Scheduled Trace Results tab	<p>Displays the basic information about the trace, including:</p> <ul style="list-style-type: none"> <li><b>Resolution Time:</b> Time that trace was run</li> <li><b>SRC.IP:</b> IP address of the source device</li> <li><b>DST.IP:</b> Address of the destination device</li> <li><b>Max Hop Count:</b> Maximum number of hops across all paths between the devices</li> <li><b>Min Hop Count:</b> Minimum number of hops across all paths between the devices</li> <li><b>Total Paths:</b> Number of available paths found between the devices</li> <li><b>PMTU:</b> Average of the maximum transmission units for all paths</li> <li><b>Errors:</b> Message provided for analysis if trace fails</li> </ul> <p>Click on a result to open a detailed view of the results.</p>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

#### Granularity of Data Shown Based on Time Period

On the medium and large Trace Result cards, the status of the runs is represented in heat maps stacked vertically; one for runs with warnings and one for runs with failures. Depending on the time period of data on the card, the number of smaller time blocks used to indicate the status varies. A vertical stack of time blocks, one from each map, includes the results from all checks during that time. The results are shown by how saturated the color is for each block. If all traces run during that time period pass, then both blocks are 100% gray. If there are only failures, the associated lower blocks are 100% saturated white and the warning blocks are 100% saturated gray. As warnings

and failures increase, the blocks increase their white saturation. As warnings or failures decrease, the blocks increase their gray saturation. An example heat map for a time period of 24 hours is shown here with the most common time periods in the table showing the resulting time blocks.



Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

#### [View Detailed Scheduled Trace Results](#)

Once a scheduled trace request has completed, the results are available in the corresponding Trace Result card.

To view the results:

1. Open the full screen Trace Request card to view all scheduled traces that have been run.

## Monitor Network Connectivity

## View Scheduled Trace Results

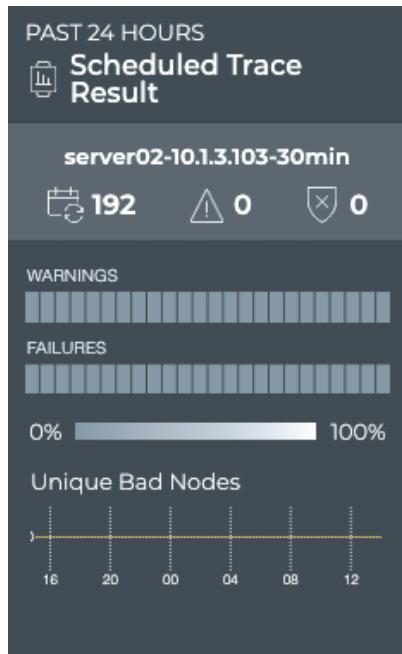
Scheduled Trace Results							
DEFAULT TIME Past 24 Hours		4 RESULTS					
Scheduled Trace Results							
	RESOLUTION TIME	SRC. IP	DST. IP	MAX HOP COUNT	MIN HOP COUNT	TOTAL PATHS	PMTU
	May 8, 2019, 2:29 pm	27.0.0.19	27.0.0.20	3	3	6	9202
	May 8, 2019, 1:29 pm	27.0.0.19	27.0.0.20	3	3	6	9202
	May 8, 2019, 12:29 pm	27.0.0.19	27.0.0.20	3	3	6	9202
	May 8, 2019, 11:29 am	27.0.0.19	27.0.0.20	3	3	6	9202

2. Select the scheduled trace you want to view results for by clicking in the first column of the result and clicking the check box.

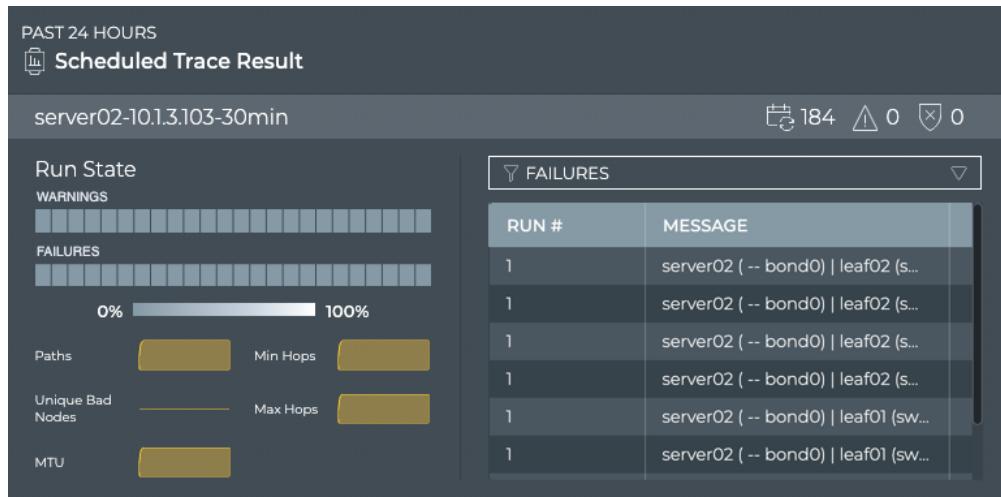
3. On the Edit Menu that appears at the bottom of the window, click



(Open Cards). This opens the medium Scheduled Trace Results card(s) for the selected items.



4. Note the distribution of results. Are there many failures? Are they concentrated together in time? Has the trace begun passing again?
5. Hover over the heat maps to view the status numbers and what percentage of the total results that represents for a given region.
6. Switch to the large Scheduled Trace Result card.



7. If there are a large number of warnings or failures, view the associated messages by selecting **Failures** or **Warning** in the filter above the table. This might help narrow the failures down to a particular device or small set of devices that you can investigate further.
8. Look for a consistent number of paths, MTU, hops in the small charts under the heat map. Changes over time here might correlate with the messages and give you a clue to any specific issues. Note if the number of bad nodes changes over time. Devices that become unreachable are often the cause of trace failures.
9. View the available paths for each run, by selecting **Paths** in the filter above the table.
10. You can view the configuration of the request that produced the results shown on this card workflow, by hovering over the card and clicking . If you want to change the configuration, click **Edit** to open the large Trace Request card, pre-populated with the current configuration. Follow the instructions in [Create a Scheduled Trace Request](#) to make your changes in the same way you created a new scheduled trace.
11. To view a summary of all scheduled trace results, switch to the full screen card.
12. Look for changes and patterns in the results for additional clues to isolate root causes of trace failures. Select and view related traces using the Edit menu.
13. View the details of any specific trace result by clicking on the trace. A new window opens similar to the following:

## Monitor Network Connectivity

## View Scheduled Trace Results

The screenshot shows a 'Trace Result Details' window with two tables: 'Path 1' and 'Path 2'.  
**Path 1:**  
Source IP: 10.2.4.102 - Destination IP: 10.1.3.103 ► Export  
The table has columns: HOP, HOSTNAME, IN. INTF, IN. MTU, IN. PORT, IN. PMTU, IN. RTRIF, IN. TUNNEL, IN. VLAN, If, and v. The data for Path 1 is:

HOP	HOSTNAME	IN. INTF	IN. MTU	IN. PORT	IN. PMTU	IN. RTRIF	IN. TUNNEL	IN. VLAN	If	v
1	server02									
2	leaf02		1500	swp2	9000	vlan24		24		v
3	spine02		9216	swp2	9216	swp2				d
4	leaf04		1500	swp52	1500	vlan4001	vni:104001			v
5	server03		9000	bond0	9000	bond0				d

  
**Path 2:**  
The table has columns: HOP, HOSTNAME, IN. INTF, IN. MTU, IN. PORT, IN. PMTU, IN. RTRIF, IN. TUNNEL, IN. VLAN, If, and v. The data for Path 2 is:

HOP	HOSTNAME	IN. INTF	IN. MTU	IN. PORT	IN. PMTU	IN. RTRIF	IN. TUNNEL	IN. VLAN	If	v
1	server02									
2	leaf02		1500	swp2	9000	vlan24		24		v
3	spine02		9216	swp2	9216	swp2				d
4	leaf03		1500	swp52	1500	vlan4001	vni:104001			v
5	server03		9000	bond0	9000	bond0				d

Scroll to the right to view the information for a given hop. Scroll down to view additional paths.

This display shows each of the hosts and detailed steps the trace takes to validate a given path between two devices. Using Path 1 as an example, each path can be interpreted as follows:

Hop 1 is from the source device, server02 in this case. It exits this device at switch port bond0 with an MTU of 9000 and over the default VRF too get to leaf02. The trace goes in to swp2 with an MTU of 9216 over the vrf1 interface. It exits leaf02 through switch port 52 and so on.

14. Export this data using the **Export** button or click



to return to the results list to view another trace in detail.

# Monitor Devices

The core capabilities of Cumulus NetQ enable you to monitor your network by viewing performance and configuration data about your individual network devices and the entire fabric network-wide. The topics contained in this section describe monitoring tasks that apply to particular device types. For network-wide monitoring refer to [Monitor Network Performance](#).

# Monitor Switches

With the NetQ UI, you can monitor individual switches separately from the network. You are able to view the status of services they are running, health of its various components, and connectivity performance. Being able to monitor switch component inventory aids in upgrade, compliance, and other planning tasks. Viewing individual switch health helps isolate performance issues.

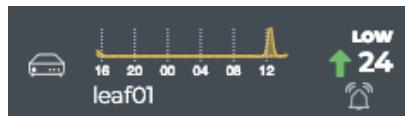
For network-wide monitoring, refer to [Monitor Network Performance](#).

## Monitor Switch Performance

Viewing detail about a particular switch is essential when troubleshooting performance issues. With NetQ you can view the overall performance and drill down to view attributes of the switch, interface performance and the events associated with a switch. This is accomplished through the Switches card.

### Switch Card Workflow Summary

The small Switch card displays:



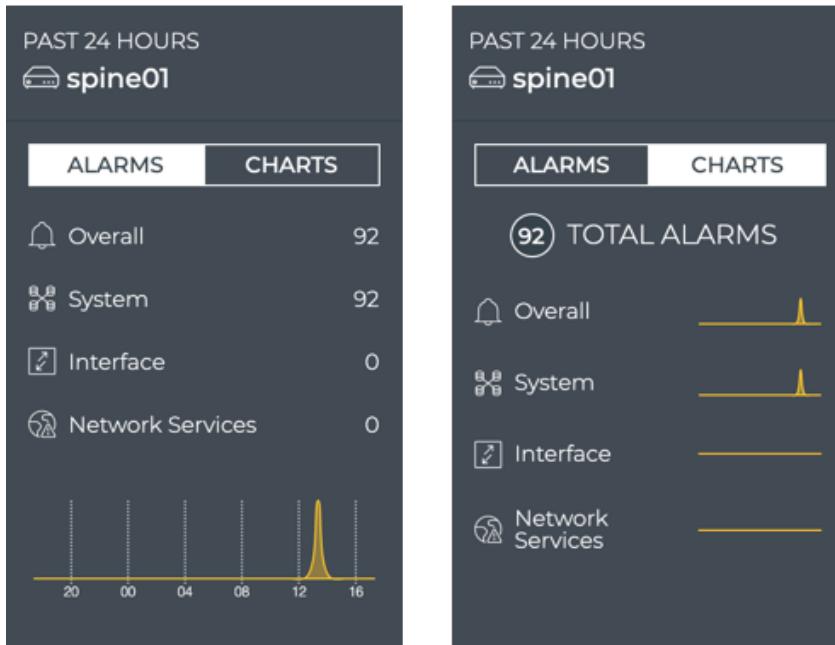
Item	Description
	Indicates data is for a single switch

Item	Description
title	Hostname of switch
Chart	Distribution of switch alarms during the designated time period
Trend	<p>Trend of alarm count, represented by an arrow:</p> <ul style="list-style-type: none"> <li>• <b>Pointing upward and green:</b> alarm count is higher than the last two time periods, an increasing trend</li> <li>• <b>Pointing downward and bright pink:</b> alarm count is lower than the last two time periods, a decreasing trend</li> <li>• <b>No arrow:</b> alarm count is unchanged over the last two time periods, trend is steady</li> </ul>
Count	Current count of alarms on the switch
Rating	<p>Overall performance of the switch. Determined by the count of alarms relative to the average count of alarms during the designated time period:</p> <ul style="list-style-type: none"> <li>• <b>Low:</b> Count of alarms is below the average count; a nominal count</li> <li>• <b>Med:</b> Count of alarms is in range of the average count; some room for improvement</li> <li>• <b>High:</b> Count of alarms is above the average count; user intervention recommended</li> </ul> 

The medium Switch card displays:

## Monitor Switches

## Monitor Switch Performance



Item	Description
	Indicates data is for a single switch
title	Hostname of switch
Alarms	When selected, displays distribution and count of alarms by alarm category, generated by this switch during the designated time period
Charts	When selected, displays distribution of alarms by alarm category, during the designated time period

The large Switch card contains three tabs:

The *Attributes* tab displays:

## Monitor Switches

## Monitor Switch Performance

The screenshot shows the 'spine01 | Attributes' page. At the top, there are navigation icons for Home, Dashboard, and Edit. On the right, there are status indicators for 24H (clock icon), a battery icon, and three dots. Below the title, the page displays the following information:

Item	Description	Value	
HOSTNAME	Cumulus Networks	spine01	
MANAGEMENT IP	OS VERSION	192.168.0.21	3.7.6
MANAGEMENT MAC	PLATFORM MODEL	a0:00:00:00:02:1	VX
AGENT STATE	ASIC VENDOR	fresh	Cumulus Networks
	ASIC MODEL		VX
	NETQ AGENT VERSION		2.2.1-cl3u19~1564507571.4cb6474
	LICENSE STATE		ok
	Total Interfaces	10	
	UP	9	
	DOWN	1	

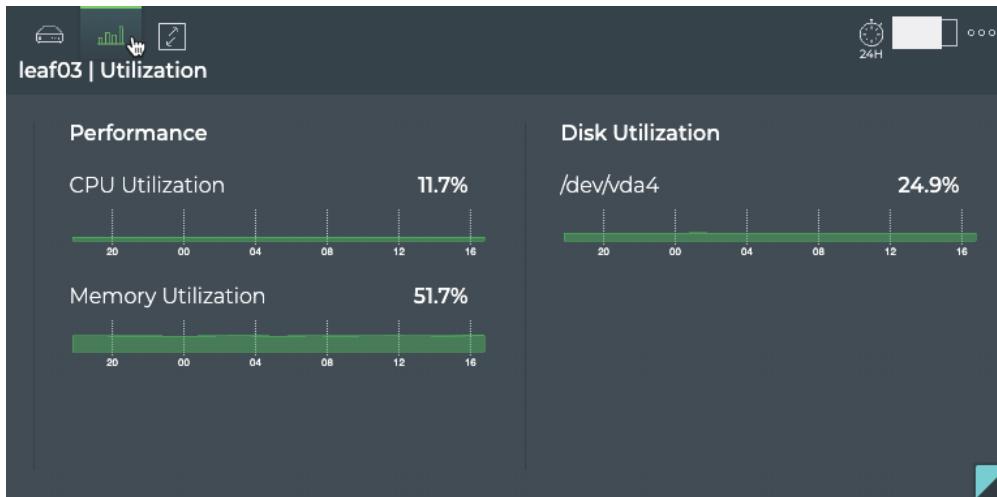
Item	Description
	Indicates data is for a single switch
title	<Hostname>   Attributes
Hostname	User-defined name for this switch
Management IP	IPv4 or IPv6 address used for management of this switch
Management MAC	MAC address used for management of this switch
Agent State	Operational state of the NetQ Agent on this switch; Fresh or Rotten
Platform Vendor	Manufacturer of this switch box. Cumulus Networks is identified as the vendor for a switch in the Cumulus in the Cloud (CITC) environment, as seen here.

Item	Description
Platform Model	Manufacturer model of this switch. VX is identified as the model for a switch in CITC environment, as seen here.
ASIC Vendor	Manufacturer of the ASIC installed on the motherboard
ASIC Model	Manufacturer model of the ASIC installed on the motherboard
OS	Operating system running on the switch. CL indicates a Cumulus Linux license.
OS Version	Version of the OS running on the switch
NetQ Agent Version	Version of the NetQ Agent running on the switch
License State	Indicates whether the license is valid ( <i>ok</i> ) or invalid/missing ( <i>bad</i> )
Total Interfaces	Total number of interfaces on this switch, and the number of those that are up and down.

The *Utilization* tab displays:

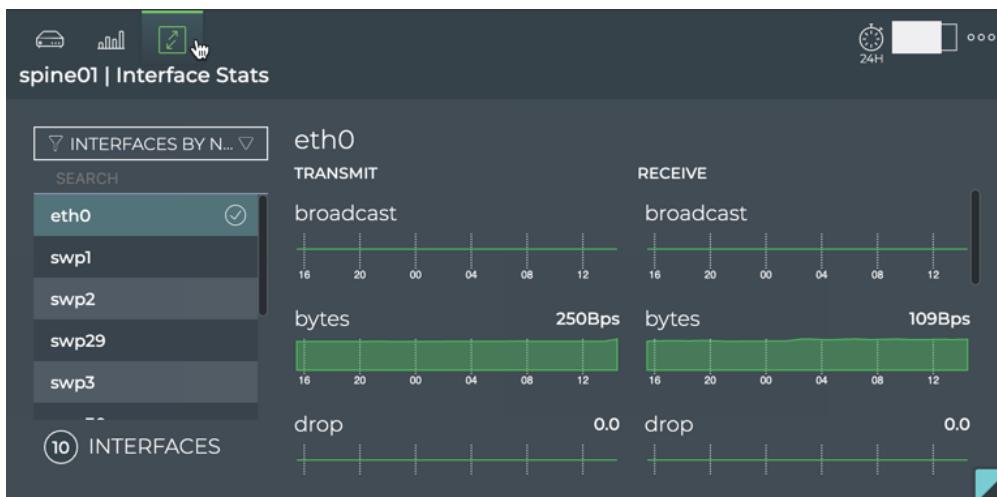
## Monitor Switches

## Monitor Switch Performance



Item	Description
	Indicates utilization data is for a single switch
Title	<Hostname>   Utilization
Performance	Displays distribution of CPU and memory usage during the designated time period
Disk Utilization	Displays distribution of disk usage during the designated time period

The *Interfaces* tab displays:



## Monitor Switches

## Monitor Switch Performance

Item	Description
	Indicates interface statistics for a single switch
Title	<Hostname>   Interface Stats
Interface List	List of interfaces present during the designated time period
Interface Filter	Sorts interface list by Name, Rx Util (receive utilization), or Tx Util (transmit utilization)
Interfaces Count	Number of interfaces present during the designated time period
Interface Statistics	Distribution and current value of various transmit and receive statistics associated with a selected interface: <ul style="list-style-type: none"><li>• <b>Broadcast:</b> Number of broadcast packets</li><li>• <b>Bytes:</b> Number of bytes per second</li><li>• <b>Drop:</b> Number of dropped packets</li><li>• <b>Errs:</b> Number of errors</li><li>• <b>Frame:</b> Number of frames received</li><li>• <b>Multicast:</b> Number of multicast packets</li><li>• <b>Packets:</b> Number of packets per second</li><li>• <b>Utilization:</b> Bandwidth utilization as a percentage of total available bandwidth</li></ul>

The full screen Switch card provides tabs for all IP addresses, all MAC addresses, and all interfaces.

## Monitor Switches

## Monitor Switch Performance

leaf02									
		8 RESULTS							
		Export							
<b>IP Addresses</b>									
DB STATE	HOSTNAME	IFNAME	IS IPV6	MASK	OPID	PREFIX	TIME	VRF	
Update	leaf02	vlan3-v0	false	24	30001	10.1.3.1	11/5/19 10:21 ...	vrf1	
Update	leaf02	peerlink4094	false	30	30001	169.254.1.2	11/5/19 10:21 ...	default	
Update	leaf02	lo	false	32	30001	10.0.0.12	11/5/19 10:21 ...	default	
Update	leaf02	vlan24-v0	false	24	30001	10.2.4.1	11/5/19 10:21 ...	vrf1	
Update	leaf02	lo	false	32	30001	10.0.0.112	11/5/19 10:21 ...	default	
Update	leaf02	eth0	false	24	30001	192.168.0.12	11/5/19 10:21 ...	mgmt	
Update	leaf02	vlan24	false	24	30001	10.2.4.12	11/5/19 10:21 ...	vrf1	
Update	leaf02	vlan13	false	24	30001	10.1.3.12	11/5/19 10:21 ...	vrf1	

Item	Description
Title	Switches
×	Closes full screen card and returns to workbench
Default Time	Displayed data is current as of this moment
Results	Number of results found for the selected tab
IP Addresses	<p>Displays all known IP addresses for the switch. This tab provides the following additional data about each address:</p> <ul style="list-style-type: none"> <li>• <b>DB State:</b> Session state of the DB; for internal use only</li> <li>• <b>Hostname:</b> User-defined name of the switch</li> <li>• <b>IfName:</b> Name of the interface</li> <li>• <b>Is IPv6:</b> Indicates whether the address is an IPv6 address (true) or an IPv4 address (false)</li> <li>• <b>Mask:</b> Mask for the address</li> <li>• <b>OpId:</b> Process identifier; for internal use only</li> <li>• <b>Prefix:</b> Prefix for the address</li> <li>• <b>Time:</b> Date and time the table was generated</li> <li>• <b>VRF:</b> Name of the virtual route forwarding (VRF) interface if deployed</li> </ul>

Item	Description
MAC Addresses	<p>Displays all known MAC addresses for the switch. This tab provides the following additional data about each address:</p> <ul style="list-style-type: none"> <li>• <b>DB State:</b> Session state of the DB; for internal use only</li> <li>• <b>Egress Port:</b> Importance of the event—critical, warning, info, or debug</li> <li>• <b>Hostname:</b> User-defined name of the switch</li> <li>• <b>Last Changed:</b> Data and time that the address was last updated or deleted</li> <li>• <b>OpId:</b> Process identifier; for internal use only</li> <li>• <b>Origin:</b> Indicates whether this switch owns this address (true) or if another switch owns this address (false)</li> <li>• <b>Remote:</b> Indicates whether this address is reachable via a VXLAN on another switch (true) or is reachable locally on the switch (false)</li> <li>• <b>Time:</b> Date and time the table was generated</li> <li>• <b>VLAN Id:</b> Identifier of an associated VLAN if deployed</li> </ul>
All Interfaces	<p>Displays all known interfaces on the switch. This tab provides the following additional data about each interface:</p> <ul style="list-style-type: none"> <li>• <b>Details:</b> Information about the interface, such as MTU, table number, members, protocols running, VLANs</li> <li>• <b>Hostname:</b> Hostname of the given event</li> <li>• <b>IfName:</b> Name of the interface</li> <li>• <b>Last Changed:</b> Data and time that the interface was last enabled, updated, deleted, or changed state to down</li> <li>• <b>OpId:</b> Process identifier; for internal use only</li> <li>• <b>State:</b> Indicates if the interface is <i>up</i> or <i>down</i></li> <li>• <b>Time:</b> Date and time the table was generated</li> <li>• <b>Type:</b> Kind of interface; for example, VRF, switch port, loopback, ethernet</li> <li>• <b>VRF:</b> Name of the associated virtual route forwarding (VRF) interface if deployed</li> </ul>

Item	Description
SSD Utilization	<p>Displays overall health and utilization of a 3ME3 solid state drive (SSD). This tab provides the following data about each drive:</p> <ul style="list-style-type: none"><li>• <b>DB State:</b> Session state of the DB; for internal use only</li><li>• <b>Device Name:</b> SSD model name</li><li>• <b>Health:</b> Current percentage health of the drive</li><li>• <b>Hostname:</b> Hostname of the device with the 3ME3 drive installed</li><li>• <b>OpId:</b> Process identifier; for internal use only</li><li>• <b>PE Cycles (Average):</b> Average number of program-erase (PE) cycles used in a 24 hour period</li><li>• <b>Time:</b> Date and time the data was generated</li></ul>
BTRFS Utilization	<p>Displays disk utilization information for devices running Cumulus Linux 3.x and the b-tree file system (BTRFS):</p> <ul style="list-style-type: none"><li>• <b>Device Allocated:</b> Percentage of the disk space allocated by BTRFS</li><li>• <b>Hostname:</b> Hostname of the given device</li><li>• <b>Largest Chunk Size:</b> Largest remaining chunk size on disk</li><li>• <b>Last Changed:</b> Data and time that the storage allocation was last updated</li><li>• <b>Rebalance Recommended:</b> Based on rules described in <a href="#">When to Rebalance BTRFS Partitions</a>, a rebalance is suggested</li><li>• <b>Unallocated Space:</b> Amount of space remaining on the disk</li><li>• <b>Unused Data Chunks Space:</b> Amount of available data chunk space</li></ul>

Item	Description
Installed Packages	<p>Displays all known interfaces on the switch. This tab provides the following additional data about each interface:</p> <ul style="list-style-type: none"> <li>• <b>Details:</b> Information about the interface, such as MTU, table number, members, protocols running, VLANs</li> <li>• <b>Hostname:</b> Hostname of the given event</li> <li>• <b>IfName:</b> Name of the interface</li> <li>• <b>Last Changed:</b> Data and time that the interface was last enabled, updated, deleted, or changed state to down</li> <li>• <b>OpId:</b> Process identifier; for internal use only</li> <li>• <b>State:</b> Indicates if the interface is <i>up</i> or <i>down</i></li> <li>• <b>Time:</b> Date and time the table was generated</li> <li>• <b>Type:</b> Kind of interface; for example, VRF, switch port, loopback, ethernet</li> <li>• <b>VRF:</b> Name of the associated virtual route forwarding (VRF) interface if deployed</li> </ul>
Export	Enables export of all or selected items in a CSV or JSON formatted file
	Enables manipulation of table display; choose columns to display and reorder columns

### View the Overall Health of a Switch

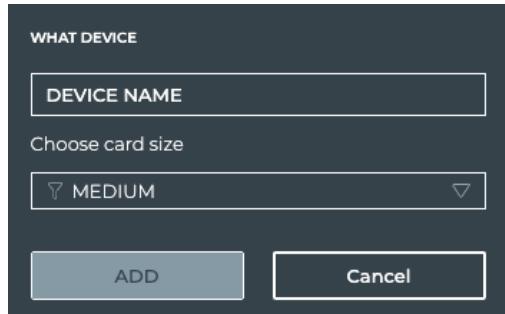
When you want to monitor the health of a particular switch, open the small Switch card. It is unlikely that you would have this card open for every switch in your network at the same time, but it is useful for tracking selected switches that may have been problematic in the recent past or that you have recently installed. The card shows you alarm status and summary performance score and trend.

To view the summary:

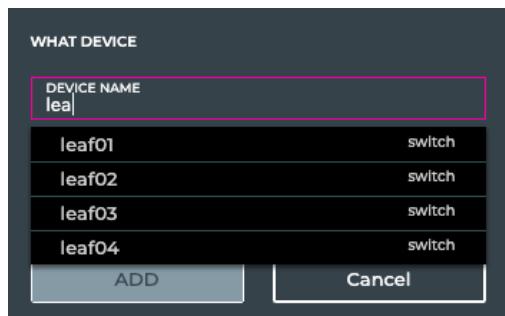
1. Click



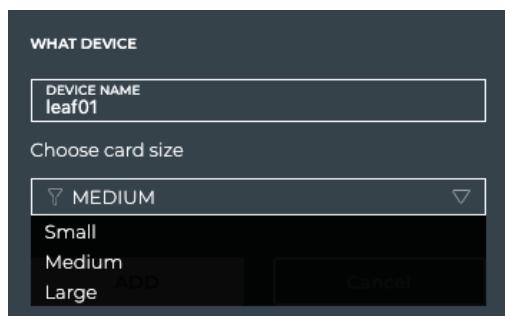
, and select Device | Switches. A dialog box opens.



2. Begin typing the hostname of the device you are interested in. Select it from the suggested matches when it appears.



3. Select the size of the card, *L1*, to open the small size card.



4. Click **Add**, or **Cancel** to exit the process.



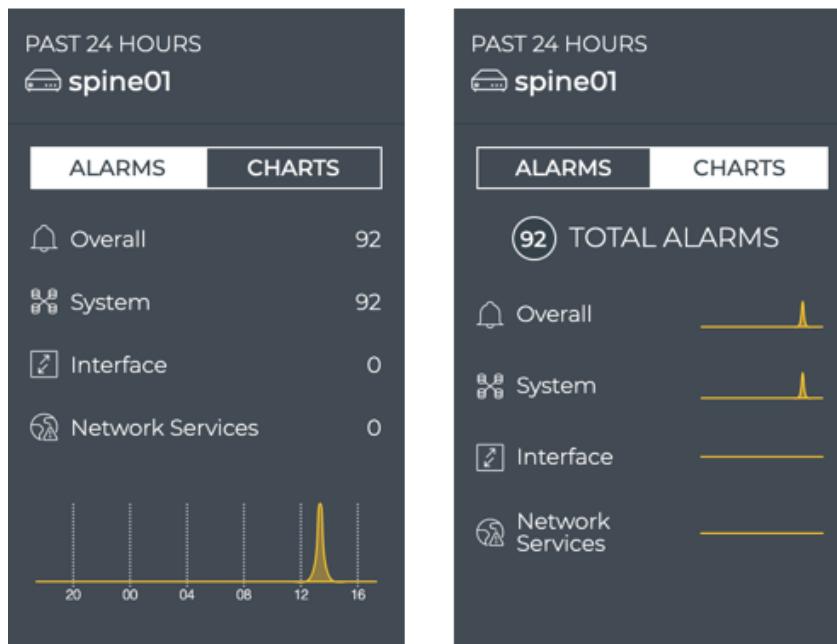
In this example, we see that the leaf01 switch has had very few alarms overall, but the number is trending upward, with a total count of 24 alarms currently.

### View Health Performance Metrics

When you are monitoring switches that have been problematic or are newly installed, you might want to view more than a summary. Instead, seeing key performance metrics can help you determine where issues might be occurring or how new devices are functioning in the network.

To view the key metrics, open the medium Switch card. The card shows you the overall switch health score and the scores for the key metrics that comprise that score. The key metric scores are based on the number of alarms attributed to the following activities on the switch:

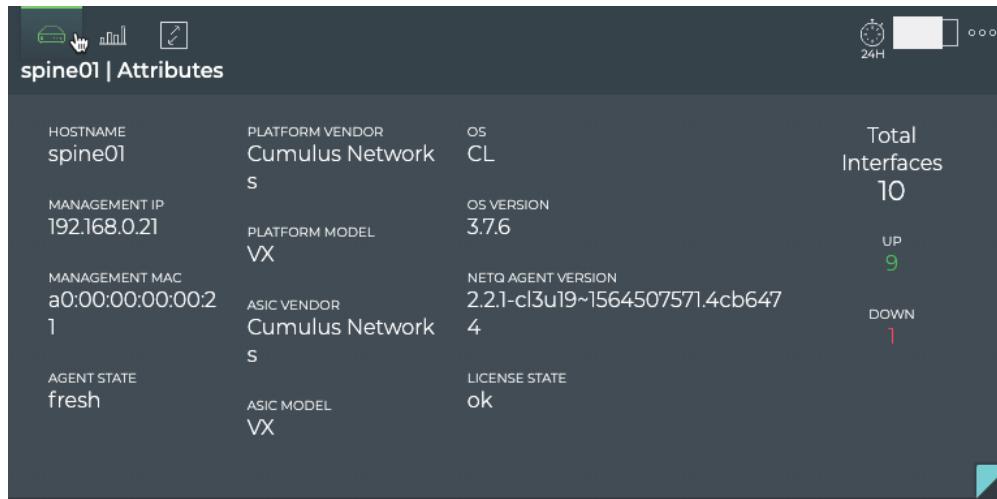
- network services, such as BGP, EVPN, CLAG, NTP, and so forth
- scheduled traces
- interface performance
- platform performance



Also included on the card is the total alarm count for all of these metrics. You can view the key performance metrics as numerical scores or as line charts over time, by clicking **Charts** or **Alarms** at the top of the card.

### View Attributes of a Switch

For a quick look at the key attributes of a particular switch, open the large Switch card. Attributes are displayed as the default tab.



HOSTNAME	PLATFORM VENDOR	OS	Total Interfaces
spine01	Cumulus Networks	CL	10
MANAGEMENT IP	PLATFORM MODEL	OS VERSION	UP
192.168.0.21	VX	3.7.6	9
MANAGEMENT MAC	ASIC VENDOR	NETQ AGENT VERSION	DOWN
a0:00:00:00:00:21	Cumulus Networks	2.2.1-c13u19~1564507571.4cb647	1
AGENT STATE	ASIC MODEL	LICENSE STATE	
fresh	VX	ok	

In this example, the items of interest might be the five interfaces that are down and what version of OS and NetQ Agent the switch is running.

### View Current Resource Utilization for a Switch

The NetQ GUI enables you to easily view the performance of various hardware components and the network tables. This enables you to determine whether a switch is reaching its maximum load and compare its performance with other switches.

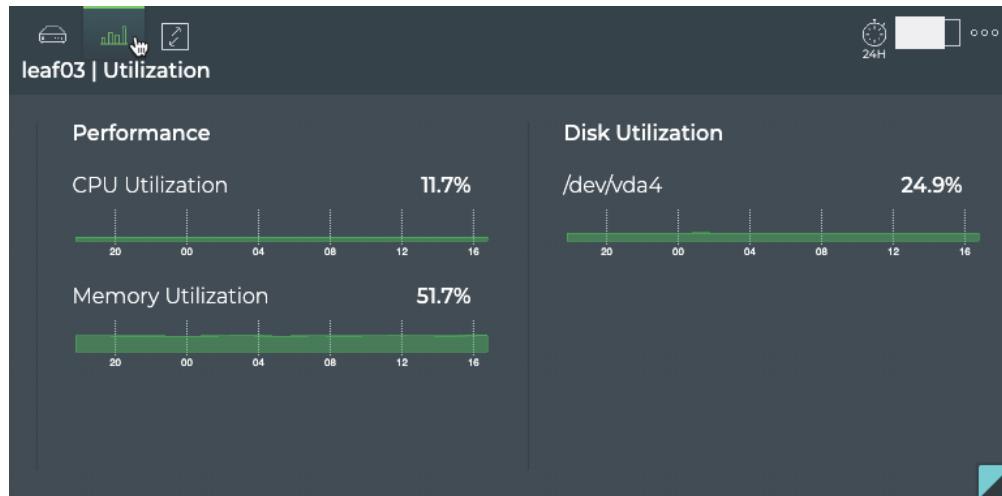
To view the resource utilization on a particular switch:

1. Open the large Switch card.
2. Hover over the card and click



.

3. The card is divided into two sections, displaying hardware-related performance through a series of charts.



4. Look at the hardware performance charts. Are there any that are reaching critical usage levels?
5. Is usage high at a particular time of day?
6. Change the time period. Is the performance about the same? Better? Worse? The results can guide your decisions about upgrade options.
7. Open a different Switch card for a comparable switch. Is the performance similar?

#### View Interface Statistics for a Switch

If you suspect that a particular switch is having performance problems, you might want to view the status of its interfaces. The statistics can also provide insight into interfaces that are more heavily loaded than others.

To view interface statistics:

1. Click .
2. Begin typing the name of the switch of interest, and select when it appears in the suggestions list.
3. Select the *Large* card size.

4. Click **Add**.
5. Hover over the card and click



to open the Interface Stats tab.



6. Select an interface from the list, scrolling down until you find it. By default the interfaces are sorted by Name, but you may find it easier to sort by the highest transmit or receive utilization using the filter above the list.
7. The charts update according to your selection. Scroll up and down to view the individual statistics.

What you view next depends on what you see, but a couple of possibilities include:

- Open the full screen card to view details about all of the IP addresses, MAC addresses, and interfaces on the switch.
- Open another switch card to compare performance on a similar interface.

### View All Addresses for a Switch

It can be useful to view all of the configured addresses that this switch is using. You can view all IP addresses or all MAC addresses using the full screen Switch card.

To view all IP addresses:

1. Open the full screen Switch card. The **IP addresses** tab is shown by default.

## Monitor Switches

## Monitor Switch Performance

DB STATE	HOSTNAME	IFNAME	IS IPV6	MASK	OPID	PREFIX	TIME	VRF
Update	leaf02	vlan13-v0	false	24	30001	10.1.3.1	11/5/19 10:21 ...	vrfl
Update	leaf02	peerlink.4094	false	30	30001	169.254.1.2	11/5/19 10:21 ...	default
Update	leaf02	lo	false	32	30001	10.0.0.12	11/5/19 10:21 ...	default
Update	leaf02	vlan24-v0	false	24	30001	10.2.4.1	11/5/19 10:21 ...	vrfl
Update	leaf02	lo	false	32	30001	10.0.0.12	11/5/19 10:21 ...	default
Update	leaf02	eth0	false	24	30001	192.168.0.12	11/5/19 10:21 ...	mgmt
Update	leaf02	vlan24	false	24	30001	10.2.4.12	11/5/19 10:21 ...	vrfl
Update	leaf02	vlan13	false	24	30001	10.1.3.12	11/5/19 10:21 ...	vrfl

2. Review the addresses for any anomalies, to obtain prefix information, determine if it is an IPv4 or IPv6 address, and so forth.
3. To return to the workbench, click in the top right corner.

To view all MAC addresses:

1. Open the full screen Switch card and click the **MAC Addresses** tab.

DB STATE	EGRESS P...	HOSTNAME	LAST CHA...	MAC ADD...	OPID	ORIGIN	REMOTE	TIME
Update	vn124:10.0.0...	leaf02	11/5/19 10:21 ...	02:03:00:44:...	30001	false	true	11/6/19 2:
Update	vn13:10.0.0.1...	leaf02	11/5/19 10:21 ...	02:03:00:33:...	30001	false	true	11/6/19 2:
Update	bond02	leaf02	11/5/19 10:21 ...	02:03:00:22:...	30001	false	false	11/6/19 2:
Update	bridge	leaf02	11/5/19 10:21 ...	44:38:39:00:...	30001	true	false	11/6/19 2:
Update	bond01	leaf02	11/5/19 10:21 ...	02:03:00:11:...	30001	false	false	11/6/19 2:
Update	bridge	leaf02	11/5/19 10:21 ...	44:38:39:00:...	30001	true	false	11/6/19 2:
Update	vlan4001-1	leaf02	11/5/19 10:21 ...	8a:2c:0e:44:...	30001	false	true	11/6/19 2:

2. Review the addresses for any anomalies, to see the associated egress port, associated VLANs, and so forth.
3. To return to the workbench, click in the top right corner.

### View All Interfaces on a Switch

You can view all of the configured interfaces on a switch in one place making it easier to see inconsistencies in the configuration, quickly see when changes were made, and the operational status.

To view all interfaces:

1. Open the full-screen Switch card and click the **All Interfaces** tab.

DETAILS	HOSTNAME	IFNAME	LAST CHA...	OPID	STATE	TIME	TYPE	VRF
VLANs: PVI...	leaf02	swp48	1/5/19 10:21 ...	30001	down	1/6/19 2:39 A...	swp	default
VLANs: PVI...	leaf02	swp52	1/5/19 10:21 ...	30001	up	1/6/19 2:39 A...	swp	default
Slave: swp2 (...)	leaf02	bond02	1/5/19 10:21 ...	30001	up	1/6/19 2:39 A...	bond	default
MTU: 1500	leaf02	vlan24	1/5/19 10:21 ...	30001	up	1/6/19 2:39 A...	vlan	vrfl
Slave: swp1 (...)	leaf02	bond01	1/5/19 10:21 ...	30001	up	1/6/19 2:39 A...	bond	default
MTU: 65536	leaf02	lo	1/5/19 10:21 ...	30001	up	1/6/19 2:39 A...	loopback	default
MTU: 1500	leaf02	eth0	1/5/19 10:21 ...	30001	up	1/6/19 2:39 A...	eth	mgmt

2. Look for interfaces that are down, shown in the **State** column.
3. Look for recent changes to the interfaces, shown in the **Last Changed** column.
4. View details about each interface, shown in the **Details** column.
5. Verify they are of the correct kind for their intended function, shown in the **Type** column.
6. Verify the correct VRF interface is assigned to an interface, shown in the **VRF** column.
7. To return to the workbench, click  in the top right corner.

### View All Software Packages on a Switch

You can view all of the software installed on a given switch to quickly validate versions and total software installed.

To view all software packages:

1. Open the full-screen Switch card and click the **Installed Packages** tab.

CL VERSION	HOSTNAME	LAST CHANGED	PACKAGE NAME	PACKAGE STATUS	VERSION
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	libruby2.1	installed	2.1.5-2+deb8u7
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	lzma	installed	9.22-2
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	python-cumulus-restapi	installed	0.1-c13u9
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	inserv	installed	1.14.0-5
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	libjqg0	installed	2.1-3.1
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	snmptrapd	installed	5.8.0-c13u11
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	iproute	installed	1.4.20-c13u13
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	libfile-copy-recursive-perl	installed	0.38-1
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	libglib2.0-0	installed	2.42.1-1+deb8u2
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	file	installed	1:5.22+15.2+deb8u5
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	libisccc90	installed	1:9.95.dfsg-9+deb8u8
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	watchdog	installed	5.14-c13u4
Cumulus Linux 3.7.8	spine01	1/4/19 10:21 PM	netq-apps	installed	2.3.1-c13u22-15723891...

2. Look for packages of interest and their version and status. Sort by a particular parameter by hovering over the column and clicking

↓ <sup>A</sup>  
Z

3. Optionally, export the list by selecting all or a specific package, then clicking **Export** above the table, or **Export Select** in the Edit Menu.

### View Disk Storage After BTRFS Allocation

Customers running Cumulus Linux 3.x which uses the BTRFS (b-tree file system) might experience issues with disk space management. This is a known problem of BTRFS because it does not perform periodic garbage collection, or rebalancing. If left unattended, these errors can make it impossible to rebalance the partitions on the disk. To avoid this issue, Cumulus Networks recommends rebalancing the BTRFS partitions in a preemptive manner, but only when absolutely needed to avoid reduction in the lifetime of the disk. By tracking the state of the disk space usage, users can determine when rebalancing should be performed. For details about when a rebalance is recommended, refer to [When to Rebalance BTRFS Partitions](#).

To view the disk state:

1. Open the full-screen Switch card for a switch of interest:

- Type the switch name in the Search box, then use the card size picker to open the full-screen card, or

## Monitor Switches

## Monitor Switch Performance

- Click



(Switches) and enter the switch name and select the full-screen card size.

2. Select the BTRFS Utilization tab.

A screenshot of a software interface showing a table titled "BTRFS Utilization" for the switch "spine01". The table has columns: DEVICE ALLOCATED, HOSTNAME, LARGEST CHUNK SIZE, LAST CHANGED, REBALANCE RECOMMENDED, UNALLOCATED SPACE, and UNUSED DATA CHUNKS SPACE. One row is present: DEVICE ALLOCATED is 31.16 %, HOSTNAME is spine01, LARGEST CHUNK SIZE is 0.57 GB, LAST CHANGED is 11/5/19 7:00 PM, REBALANCE RECOMMENDED is no, UNALLOCATED SPACE is 3.96 GB, and UNUSED DATA CHUNKS SPACE is 10.7 MB. There is a "RESULTS" count of 1 in the top right corner.

DEVICE ALLOCATED	HOSTNAME	LARGEST CHUNK SIZE	LAST CHANGED	REBALANCE RECOMMENDED	UNALLOCATED SPACE	UNUSED DATA CHUNKS SPACE
31.16 %	spine01	0.57 GB	11/5/19 7:00 PM	no	3.96 GB	10.7 MB

3. Look for the **Rebalance Recommended** column. If the value in that column says *Yes*, then you are strongly encouraged to rebalance the BTRFS partitions. If it says *No*, then you can review the other values in the table to determine if you are getting close to needing a rebalance, and come back to view this table at a later time.

### View SSD Utilization

For NetQ servers and appliances that have 3ME3 solid state drives (SSDs) installed (primarily in on-premises deployments), you can view the utilization of the drive on-demand. An alarm is generated for drives that drop below 10% health, or have more than a two percent loss of health in 24 hours, indicating the need to rebalance the drive. Tracking SSD utilization over time enables you to see any downward trend or instability of the drive before you receive an alarm.

To view SSD utilization:

1. Open the full screen Switch card and click the **SSD Utilization** tab.

A screenshot of a software interface showing a table titled "SSD Utilization" for the switch "spine01". The table has columns: PE CYCLES(AVERAGE), DB STATE, DEVICE NAME, HEALTH, HOSTNAME, OPID, and TIME. One row is present: PE CYCLES(AVERAGE) is 576, DB STATE is Update, DEVICE NAME is M.2 (S42) 3ME3, HEALTH is 80, HOSTNAME is spine01, OPID is 1569345807, and TIME is 10/5/19 9:45 ... There is a "RESULTS" count of 0 in the top right corner.

PE CYCLES(AVERAGE)	DB STATE	DEVICE NAME	HEALTH	HOSTNAME	OPID	TIME
576	Update	M.2 (S42) 3ME3	80	spine01	1569345807	10/5/19 9:45 ...

2. View the average PE Cycles value for a given drive. Is it higher than usual?

3. View the Health value for a given drive. Is it lower than usual? Less than 10%?

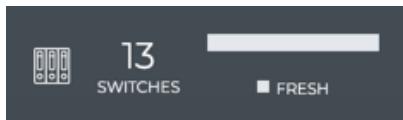
Consider adding the switch cards that are suspect to a workbench for easy tracking.

## Monitor Switch Component Inventory

Knowing what components are included on all of your switches aids in upgrade, compliance, and other planning tasks. Viewing this data is accomplished through the Switch Inventory card.

### Switch Inventory Card Workflow Summary

The small Switch Inventory card displays:



Item	Description
	Indicates data is for switch inventory
Count	Total number of switches in the network inventory
Chart	Distribution of overall health status during the designated time period; fresh versus rotten

The medium Switch Inventory card displays:

## Monitor Switches

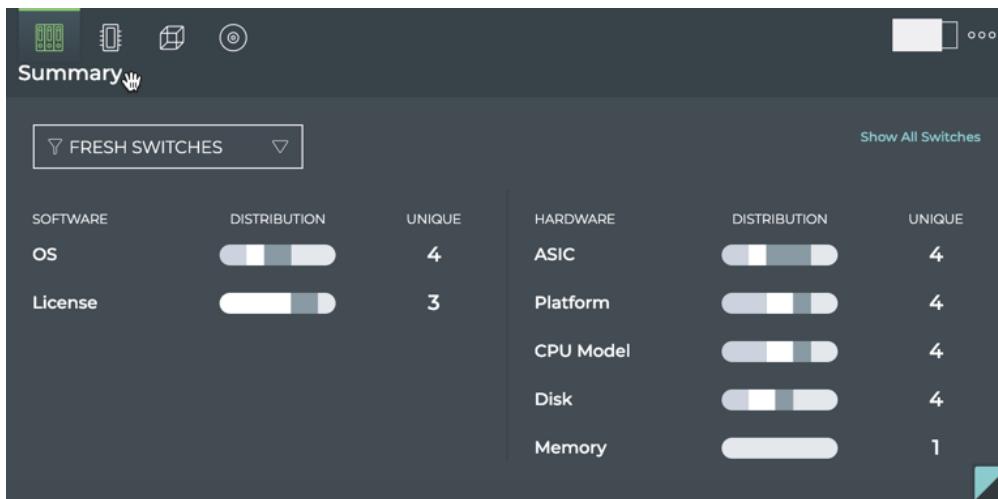
## Monitor Switch Component Inventory



Item	Description
	Indicates data is for switch inventory
Filter	View fresh switches (those you have heard from recently) or rotten switches (those you have not heard from recently) on this card
Chart	<p>Distribution of switch components (disk size, OS, ASIC, NetQ Agents, CPU, Cumulus Linux licenses, platform, and memory size) during the designated time period. Hover over chart segment to view versions of each component.</p> <p><b>Note:</b> You should only have one version of NetQ Agent running and it should match the NetQ Platform release number. If you have more than one, you likely need to upgrade the older agents.</p>
Unique	Number of unique versions of the various switch components. For example, for OS, you might have CL 3.7.1 and CL 3.7.4 making the unique value two.

The large Switch Inventory card contains four tabs.

The *Summary* tab displays:



Item	Description
	Indicates data is for switch inventory
Filter	View fresh switches (those you have heard from recently) or rotten switches (those you have not heard from recently) on this card
Charts	<p>Distribution of switch components (disk size, OS, ASIC, NetQ Agents, CPU, Cumulus Linux licenses, platform, and memory size), divided into software and hardware, during the designated time period. Hover over chart segment to view versions of each component.</p> <p><b>Note:</b> You should only have one version of NetQ Agent running and it should match the NetQ Platform release number. If you have more than one, you likely need to upgrade the older agents.</p>
Unique	Number of unique versions of the various switch components. For example, for OS, you might have CL 3.7.6 and CL 3.7.4 making the unique value two.

The *ASIC* tab displays:

## Monitor Switches

## Monitor Switch Component Inventory



Item	Description
	Indicates data is for ASIC information
Filter	View fresh switches (those you have heard from recently) or rotten switches (those you have not heard from recently) on this card
Vendor chart	Distribution of ASIC vendors. Hover over chart segment to view the number of switches with each version.
Model chart	Distribution of ASIC models. Hover over chart segment to view the number of switches with each version.
Show All	Opens full screen card displaying all components for all switches

The *Platform* tab displays:

## Monitor Switches

## Monitor Switch Component Inventory

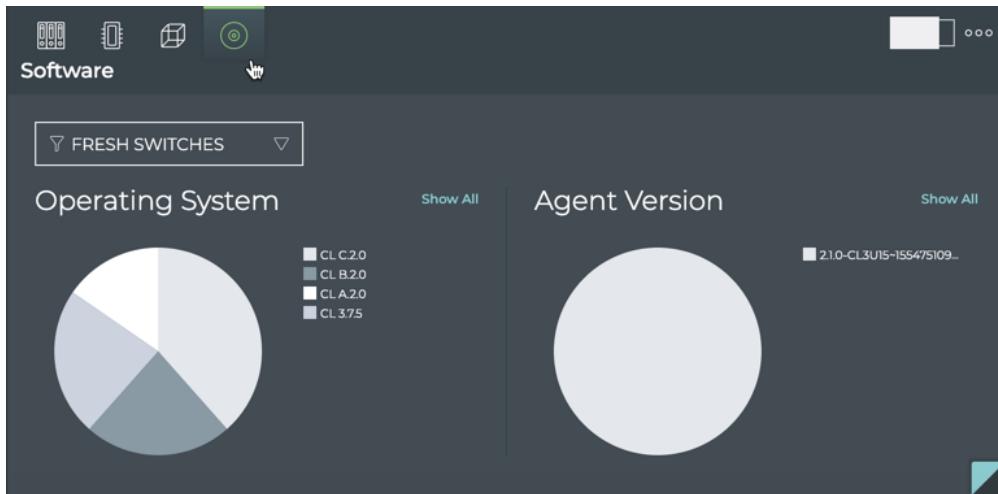


Item	Description
	Indicates data is for platform information
Filter	View fresh switches (those you have heard from recently) or rotten switches (those you have not heard from recently) on this card
Vendor chart	Distribution of platform vendors. Hover over chart segment to view the number of switches with each vendor.
Platform chart	Distribution of platform models. Hover over chart segment to view the number of switches with each model.
License State chart	Distribution of Cumulus Linux license status. Hover over chart segments to highlight the vendor and platforms that have that license status.
Show All	Opens full screen card displaying all components for all switches

The *Software* tab displays:

## Monitor Switches

## Monitor Switch Component Inventory



Item	Description
(⌚)	Indicates data is for software information
Filter	View fresh switches (those you have heard from recently) or rotten switches (those you have not heard from recently) on this card
Operating System chart	Distribution of OS versions. Hover over chart segment to view the number of switches with each version.
Agent Version chart	Distribution of NetQ Agent versions. Hover over chart segment to view the number of switches with each version. <b>Note:</b> You should only have one version of NetQ Agent running and it should match the NetQ Platform release number. If you have more than one, you likely need to upgrade the older agents.
Show All	Opens full screen card displaying all components for all switches

The full screen Switch Inventory card provides tabs for all components, ASIC, platform, CPU, memory, disk, and OS components.

## Monitor Switches

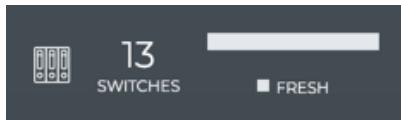
## Monitor Switch Component Inventory

Inventory   Switch									
		13 RESULTS							
Show All		Export							
HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...	
edge01	8/5/19 6:54 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	
exit01	8/5/19 6:54 P...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	
exit02	8/5/19 6:54 P...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	
leaf01	8/5/19 6:54 P...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	
leaf02	8/5/19 6:53 PM	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	
leaf03	8/5/19 6:54 P...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	
leaf04	8/5/19 6:54 P...	VX	2.21-cl3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX	
server01	8/6/19 4:03 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	
server02	8/6/19 4:03 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A	

There are a multitude of ways to view and analyze the available data within this workflow. A few examples are provided here.

### View a Summary of Communication Status for All Switches

A communication status summary for all of your switches across the network is available from the small Switch Inventory card.



In this example, we see all 13 switches have been heard from recently (they are fresh).

### View the Number of Types of Any Component Deployed

For each of the components monitored on a switch, NetQ displays the variety of those component by way of a count. For example, if you have three operating systems running on your switches, say Cumulus Linux, Ubuntu and RHEL, NetQ indicates a total unique count of three OSs. If you only use Cumulus Linux, then the count shows as one.

To view this count for all of the components on the switch:

1. Open the medium Switch Inventory card.



2. Note the number in the **Unique** column for each component.

In the above example, there are four different disk sizes deployed, four different OSs running, four different ASIC vendors and models deployed, and so forth.

3. Scroll down to see additional components.

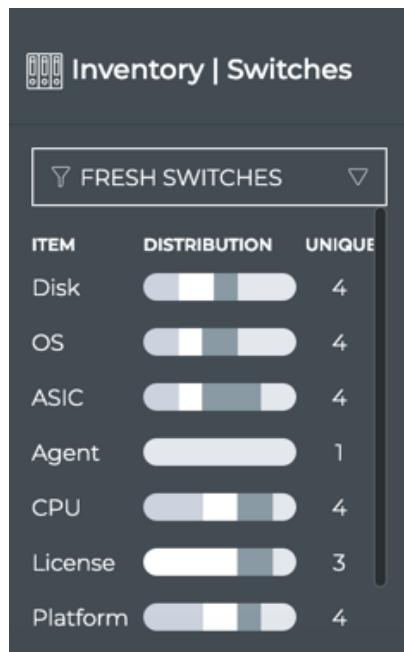
By default, the data is shown for switches with a fresh communication status. You can choose to look at the data for switches in the rotten state instead. For example, if you wanted to see if there was any correlation to a version of OS to the switch having a rotten status, you could select **Rotten Switches** from the dropdown at the top of the card and see if they all use the same OS (count would be 1). It may not be the cause of the lack of communication, but you get the idea.

#### View the Distribution of Any Component Deployed

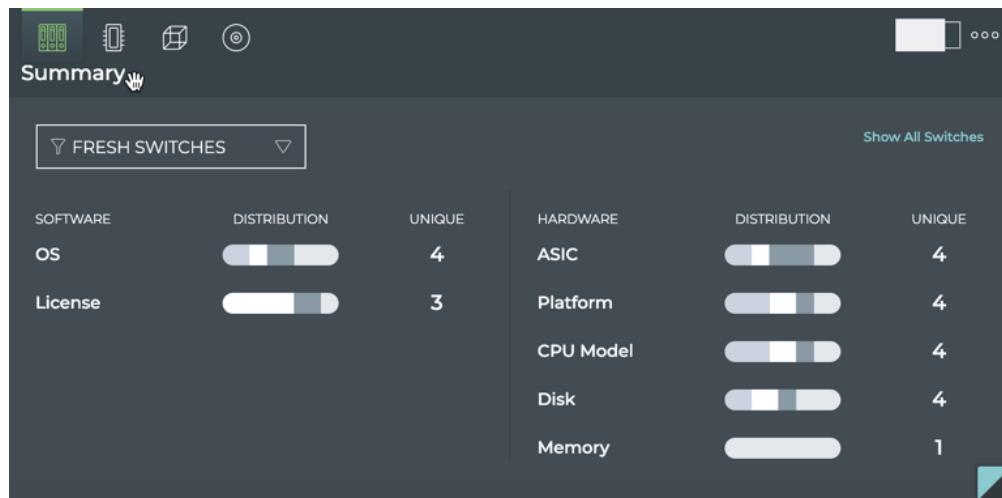
NetQ monitors a number of switch components. For each component you can view the distribution of versions or models or vendors deployed across your network for that component.

To view the distribution:

1. Open the medium or large Switch Inventory card. Each component has a chart showing the distribution.



OR



2. Hover over a segment of the chart to view the name, version, model or vendor and the number of switches that have been deployed. You can also see the percentage of all switches this total represents. On the large Switch Inventory card, hovering also

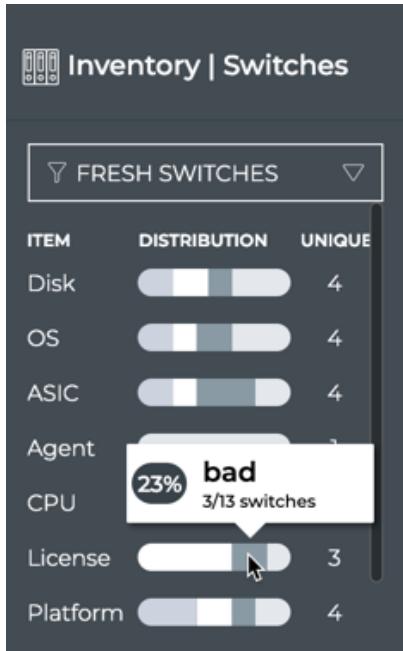
highlights the related components for the selected component. This is shown in blue here.



3. Point to additional segments on that component or other components to view their detail.
4. Scroll down to view additional components.

#### View the Number of Switches with Invalid or Missing Licenses

It is important to know when you have switches that have invalid or missing Cumulus Linux licenses, as not all of the features are operational without a valid license. Simply open the medium or large Switch Inventory card, and hover over the License chart to see the count.



To view which vendors and platforms have bad or missing licenses, open the large Switch Inventory card, and click



to open the **Platform** tab. Hover over the License State bar chart to highlight the vendor and platforms with the various states.

To view *which* switches have invalid or missing licenses, either:

- hover over the large Switch Inventory card and click



to open the **Platform** tab. Above the Licenses State or the Vendor chart, click

**Show All.**

- open the full screen Switch Inventory card. Then sort the **All Switches** tab data table by the **License State** column to locate the switches with bad or missing licenses.

## Monitor Switches

## Monitor Switch Component Inventory

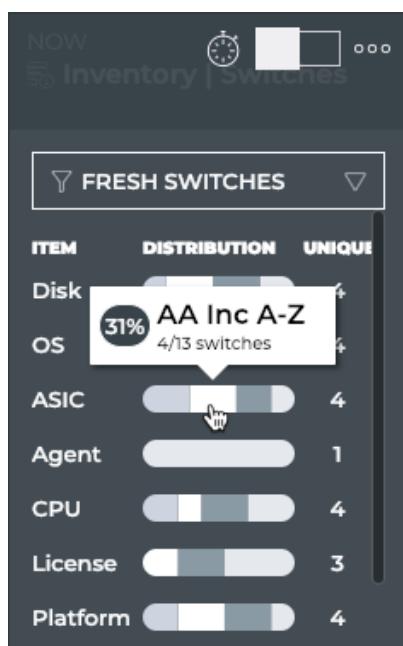
HOSTNAME	TIME	ASIC MOD...	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...
edge01	8/5/19 6:54 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A
exit01	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/5/19 6:53 PM	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf04	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
server01	8/6/19 4:03 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A
server02	8/6/19 4:03 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A

### View the Most Commonly Deployed ASIC

It can be useful to know the quantity and ratio of many components deployed in your network to determine the scope of upgrade tasks, balance vendor reliance, or for detailed troubleshooting. You can view the most commonly deployed components in generally the same way. Some components have additional details contained in large card tabs.

To view the most commonly deployed ASIC, for example:

1. Open the medium or large Switch Inventory card.
2. Hover over the *largest* segment in the ASIC chart. The tooltip that appears shows you the number of switches with the given ASIC and the percentage of your entire switch population with this ASIC.



Click on any other component in a similar fashion to see the most common type of that component.

3. If you opened the medium Switch Inventory card, switch to the large card.

4. Hover over the card, and click

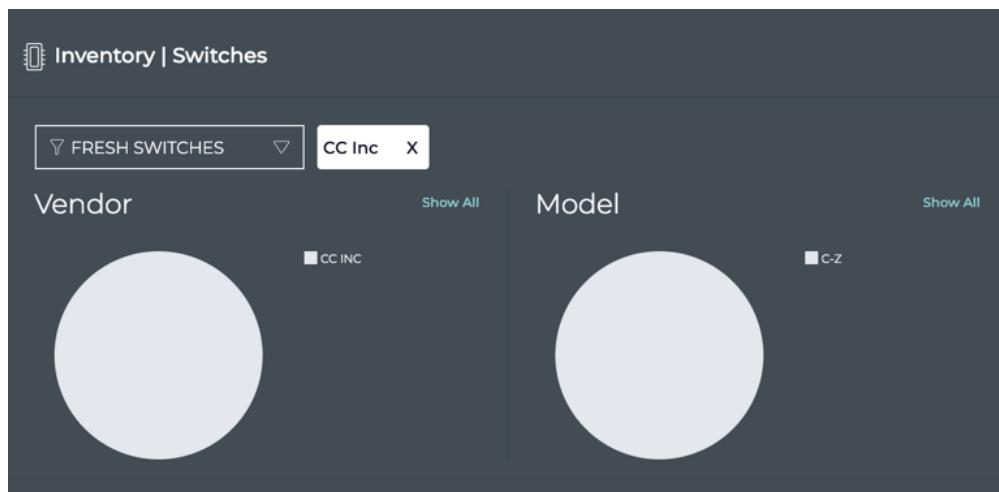


to open the **ASIC** tab. Here you can more easily view the various vendors and platforms based on the ASIC deployed.

5. Hover over the **Vendor** pie chart to highlight which platforms are supported by the vendor; and vice versa, hover over the **Model** pie chart to see which vendor supports that platform. Moving your cursor off of the carts removes the highlight.



6. Click on a segment of the **Vendor** pie chart to drill down and see only that Vendor and its supported models. A filter tag is placed at the top of the charts.

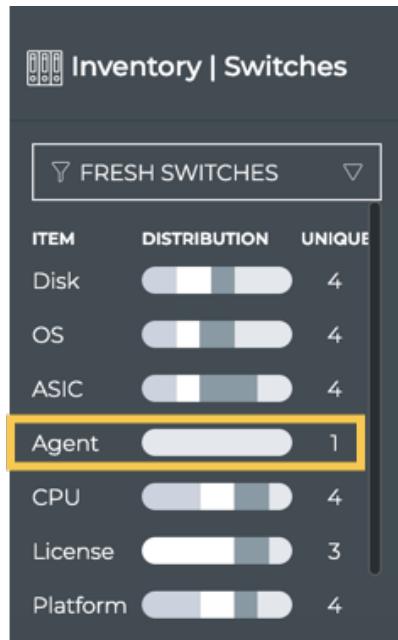


7. To return to the complete view of vendors and platforms, click  on the filter tag.

### View the Number of Switches with a Particular NetQ Agent

It is recommended that when you upgrade NetQ that you also upgrade the NetQ Agents. You can determine if you have covered all of your agents using the medium or large Switch Inventory card. To view the NetQ Agent distribution by version:

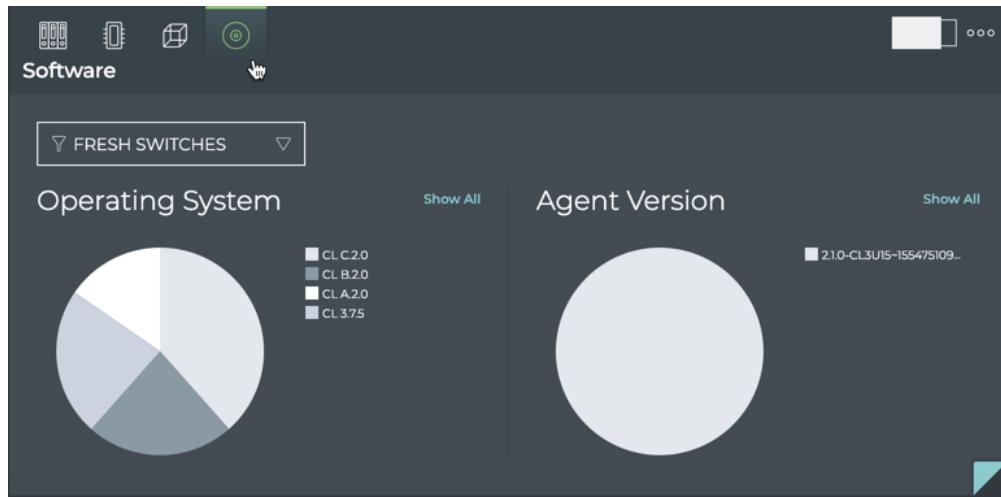
1. Open the medium Switch Inventory card.
2. View the number in the **Unique** column next to Agent.



3. If the number is greater than one, you have multiple NetQ Agent versions deployed.
4. If you have multiple versions, hover over the Agent chart to view the count of switches using each version.
5. For more detail, switch to the large Switch Inventory card.
6. Hover over the card and click  to open the **Software** tab.

## Monitor Switches

## Monitor Switch Component Inventory



7. Hover over the chart on the right to view the number of switches using the various versions of the NetQ Agent.
8. Hover over the Operating System chart to see which NetQ Agent versions are being run on each OS.



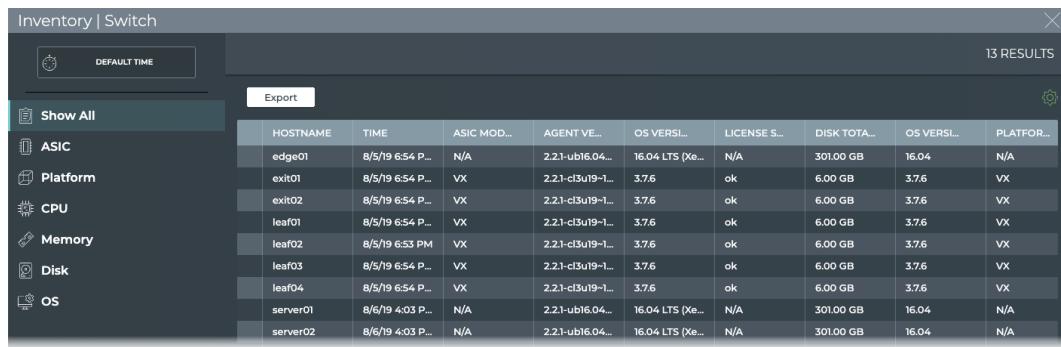
9. Click either chart to focus on a particular OS or agent version.
10. To return to the full view, click  in the filter tag.
11. Filter the data on the card by switches that are having trouble communicating, by selecting *Rotten Switches* from the dropdown above the charts.

## Monitor Switches

## Monitor Switch Component Inventory

View a List of All Data for a Specific Component

When the small, medium and large Switch Inventory cards do not provide either enough information or are not organized in a fashion that provides the information you need, open the full screen Switch Inventory card. Select the component tab of interest and filter and sort as desired. Export the data to a third-party tool, by clicking **Export**.



The screenshot shows a software interface titled "Inventory | Switch". On the left, there's a sidebar with icons for ASIC, Platform, CPU, Memory, Disk, and OS. The "Show All" option is selected. At the top right, it says "13 RESULTS". In the center, there's a table with the following columns: HOSTNAME, TIME, ASIC MOD., AGENT VE..., OS VERSI..., LICENSE S..., DISK TOTA..., OS VERSI..., and PLATFOR... . The table contains 13 rows of data, each representing a different device or server.

HOSTNAME	TIME	ASIC MOD.	AGENT VE...	OS VERSI...	LICENSE S...	DISK TOTA...	OS VERSI...	PLATFOR...
edge01	8/5/19 6:54 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A
exit01	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
exit02	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf01	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf02	8/5/19 6:53 PM	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf03	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
leaf04	8/5/19 6:54 P...	VX	2.21-c3u19-1...	3.7.6	ok	6.00 GB	3.7.6	VX
server01	8/6/19 4:03 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A
server02	8/6/19 4:03 P...	N/A	2.21-ub16.04...	16.04 LTS (Xe...	N/A	301.00 GB	16.04	N/A

# Monitor Network Elements

In addition to network performance monitoring, the Cumulus NetQ UI provides a view into the current status and configuration of the network elements in a tabular, network-wide view. These are helpful when you want to see all data for all of a particular element in your network for troubleshooting, or you want to export a list view.

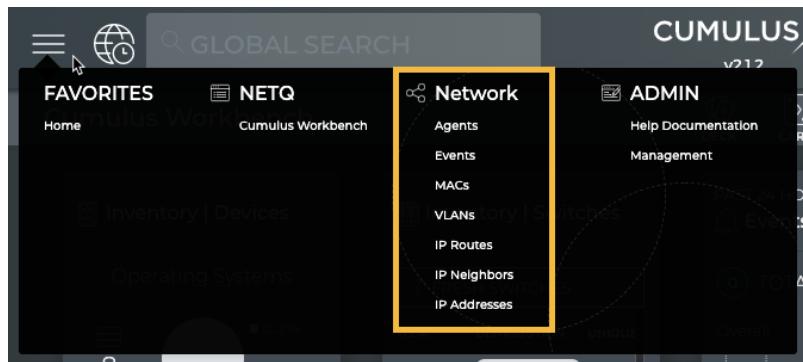
Some of these views provide data that is also available through the card workflows, but these views are not treated like cards. They only provide the current status; you cannot change the time period of the views, or graph the data within the UI.

The tables can be manipulated as described in [Data Grid settings](#).

Access these tables through the Main Menu (



), under the **Network** heading.



## View All NetQ Agents

The Agents view provides all available parameter data about all NetQ Agents in the system.

## Monitor Network Elements

[View All Events](#)

AGENTS											X
13 RESULTS											Export
ACTIVE	DB STATE	HOSTNAME	LAST REINIT	LAST UPDA...	LASTBOOT	NTP STATE	OPID	SYS UPTIME	TIMESTAMP	VERSION	⚙️
true	Update	edge01	8/28/19 3:20 PM	9/12/19 7:55 PM	8/28/19 3:20 PM	yes	80005	15 days, 19 hours, 49 minutes	9/12/19 7:55 PM	2.2.1-ub16.04...	
true	Update	exit01	8/28/19 3:21 PM	9/12/19 7:44 PM	8/28/19 3:21 PM	yes	80005	15 days, 19 hours, 49 minutes	9/12/19 7:44 PM	2.2.1-c13u19-1...	
true	Update	exit02	8/28/19 3:21 PM	9/12/19 7:43 PM	8/28/19 3:21 PM	yes	80005	15 days, 19 hours, 49 minutes	9/12/19 7:43 PM	2.2.1-c13u19-1...	
true	Update	leaf01	8/28/19 3:21 PM	9/12/19 7:44 PM	8/28/19 3:21 PM	yes	80005	15 days, 19 hours, 49 minutes	9/12/19 7:44 PM	2.2.1-c13u19-1...	
true	Update	leaf02	9/10/19 3:18 PM	9/12/19 7:43 PM	8/28/19 3:20 PM	yes	80005	15 days, 19 hours, 49 minutes	9/12/19 7:43 PM	2.2.1-c13u19-1...	
true	Update	leaf03	8/28/19 3:20 PM	9/12/19 7:44 PM	8/28/19 3:20 PM	yes	80005	15 days, 19 hours, 49 minutes	9/12/19 7:44 PM	2.2.1-c13u19-1...	

## View All Events

The Events view provides all available parameter data about all events in the system.

EVENTS						X
1,000 RESULTS						Export
HOSTNAME	MESSAGE	MESSAGE TYPE	SEVERITY	TIMESTAMP		⚙️
server02	server02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM		
leaf02	leaf02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM		
spine02	spine02 config file lldpd was created	configdiff	info	9/10/19 3:19 PM		
spine01	spine01 config file lldpd was created	configdiff	info	9/10/19 3:19 PM		
server01	server01 config file lldpd was created	configdiff	info	9/10/19 3:19 PM		
leaf04	leaf04 config file lldpd was created	configdiff	info	9/10/19 3:19 PM		

## View All MACs

The MACs (media access control addresses) view provides all available parameter data about all MAC addresses in the system.

MACS											X
114 RESULTS											Export
DB STATE	EGRESS PORT	HOSTNAME	LAST CHANGED	MAC ADDR...	OPID	ORIGIN	IS REMOTE	TIMESTAMP	VLAN	⚙️	
Update	vxlan400t:leaf04	exit01	9/12/19 7:55 PM	44:39:39:ff:40:...	80005	false	true	9/13/19 11:32 AM	4001		
Update	vxlan400t:leaf02	exit01	9/12/19 7:55 PM	44:39:39:ff:40:...	80005	false	true	9/13/19 11:32 AM	4001		
Update	bridge	exit01	9/12/19 3:18 PM	6e:7e:02:c4:fd:...	80005	true	false	9/13/19 11:32 AM	4001		
Update	vxlan400t:leaf04	exit02	9/12/19 7:55 PM	44:39:39:ff:40:...	80005	false	true	9/13/19 11:32 AM	4001		
Update	bridge	exit02	9/12/19 3:18 PM	7a:2f:14:80:c4:3c	80005	true	false	9/13/19 11:32 AM	4001		
Update	vxlan400t:leaf02	exit02	9/12/19 7:55 PM	44:39:39:ff:40:...	80005	false	true	9/13/19 11:32 AM	4001		

## View All VLANs

The VLANs (virtual local area networks) view provides all available parameter data about all VLANs in the system.

## Monitor Network Elements

View All IP Routes

VLANS									
6 RESULTS									
<button>Export</button> <span>⚙️</span>									
DB STATE	HOSTNAME	IFNAME	LAST CHANGED	OPID	PORTS	SVI	TIMESTAMP	VLANs	
Update	exit01	bridge	9/12/19 3:18 PM	80005		4001	9/13/19 11:34 AM	4001	
Update	exit02	bridge	9/12/19 3:17 PM	80005		4001	9/13/19 11:34 AM	4001	
Update	leaf01	bridge	9/12/19 3:18 PM	80005	vni13,vni24	13 24 4001	9/13/19 11:34 AM	1,13,24,4001	
Update	leaf02	bridge	9/12/19 3:19 PM	80005	vni13,vni24	13 24 4001	9/13/19 11:34 AM	1,13,24,4001	
Update	leaf03	bridge	9/12/19 3:18 PM	80005	vni13,vni24,bond04	13 24 4001	9/13/19 11:34 AM	1,13,24,4001	

## View All IP Routes

The IP Routes view provides all available parameter data about all IP routes, all IPv4 routes, and all IPv6 routes in the system.

IP ROUTES										
373 RESULTS										
<button>Export</button> <span>⚙️</span>										
DB STATE	HOSTNAME	IS IPV6	MESSAGE TY...	NEXTH...	OPID	ORIGIN	PREFIX	PROTOCOL	ROUTE TY...	RT TABLE I...
Update	edge01	true	Route	[[null,"o"]]	80005	true	:/0	kernel	1	0
Update	exit01	true	Route	[[null,"o"]]	80005	false	:/0	boot	1	1001
Update	exit01	true	Route	[[null,"o"]]	80005	false	:/0	boot	1	1002
Update	exit02	true	Route	[[null,"o"]]	80005	false	:/0	boot	1	1001
Update	exit02	true	Route	[[null,"o"]]	80005	false	:/0	boot	1	1002
Update	leaf01	true	Route	[[null,"o"]]	80005	false	:/0	boot	1	1001

## View All IP Neighbors

The IP Neighbors view provides all available parameter data about all IP neighbors, all IPv4 neighbors, and all IPv6 neighbors in the system.

IP NEIGHBORS										
504 RESULTS										
<button>Export</button> <span>⚙️</span>										
DB STATE	HOSTNAME	IFINDEX	IFNAME	IP ADDRESS	IS IPV6	IS REMOTE	MAC ADD...	MESSAGE ...	OPID	TIMESTA...
Update	edge01	3	eth0	fe80:a200ff:...	true	false	a0:00:00:00:...	Neighbor	80005	9/12/19 3:1
Update	edge01	1	lo	:1	true	false	00:00:00:00:...	Neighbor	80005	9/12/19 3:1
Update	edge01	3	eth0	ff02::1:ff00:51	true	false	33:33:ff:00:...	Neighbor	80005	9/12/19 3:1
Update	edge01	3	eth0	ff02::16	true	false	33:33:00:00:...	Neighbor	80005	9/12/19 3:1
Update	edge01	3	eth0	ff02::2	true	false	33:33:00:00:...	Neighbor	80005	9/12/19 3:1
Update	exit01	12	swp51	ff02::1	true	false	33:33:00:00:...	Neighbor	80005	9/12/19 3:1

## View All IP Addresses

The IP Addresses view provides all available parameter data about all IP addresses, all IPv4 addresses, and all IPv6 addresses in the system.

## Monitor Network Elements

## View All IP Addresses

The screenshot shows a network monitoring interface with a sidebar on the left containing three filter buttons: 'ALL' (selected), 'IPV4', and 'IPV6'. The main area is titled 'IP ADDRESSES' and displays a table with 157 results. The table has columns: DB STATE, HOSTNAME, IFNAME, IS IPV6, MASK, OPID, PREFIX, TIMESTAMP, and VRF. The data includes entries for hosts like 'edge01' and 'exit01' across various interfaces (lo, eth0, swp52, bridge) with specific MAC addresses and timestamps.

DB STATE	HOSTNAME	IFNAME	IS IPV6	MASK	OPID	PREFIX	TIMESTAMP	VRF
Update	edge01	lo	true	128	80005	::1	9/12/19 3:19 PM	default
Update	edge01	eth0	true	64	80005	fe80::a200:fffe0...	9/12/19 3:19 PM	default
Update	exit01	swp52	true	64	80005	fe80::4638:39ff...	9/12/19 3:18 PM	default
Update	exit01	bridge	true	64	80005	fe80::6c7e:2ffffe...	9/12/19 3:18 PM	default
Update	exit01	eth0	true	64	80005	fe80::a200:fffe0...	9/12/19 3:18 PM	mgmt
Update	exit01	lo	true	128	80005	::1	9/12/19 3:18 PM	default

# Monitor Using Topology View

The core capabilities of Cumulus NetQ enable you to monitor your network by viewing performance and configuration data about your individual network devices and the entire fabric network-wide. The topics contained in this section describe monitoring tasks that can be performed from a topology view rather than through the NetQ UI card workflows or the NetQ CLI.

## Access the Topology View

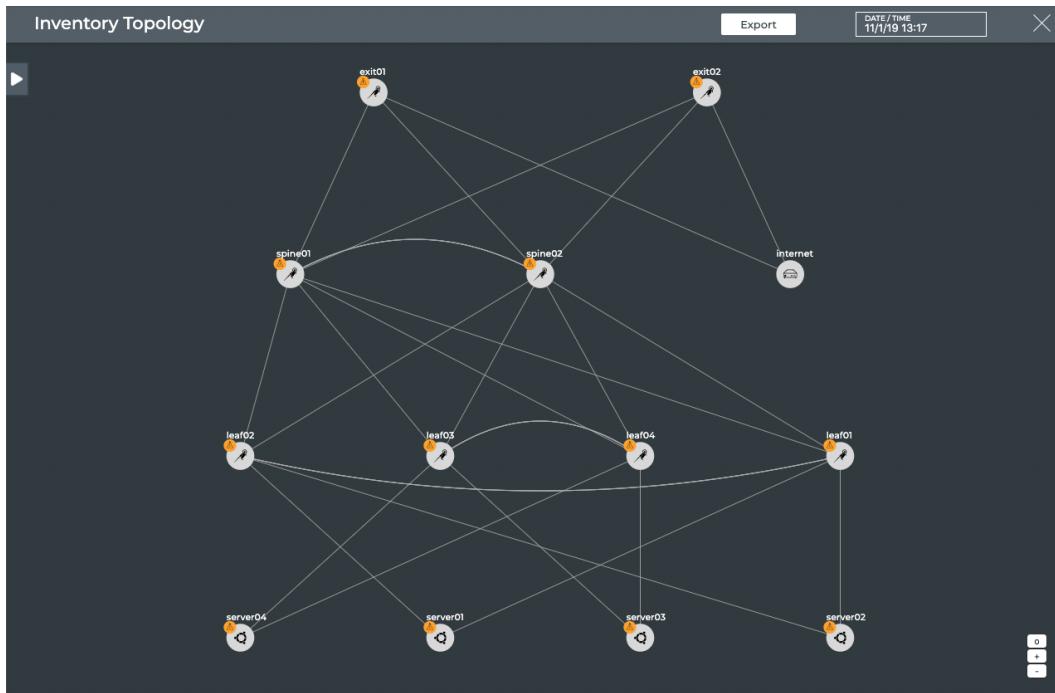
To open the topology view, click



in any workbench header.



This opens the full screen view of your network topology.



This document uses the Cumulus Networks [reference topology](#) for all examples.

To close the view, click



in the top right corner.

## Topology Overview

The topology view provides a visual representation of your Linux network, showing the connections and device information for all monitored nodes, for an alternate monitoring and troubleshooting perspective. The topology view uses a number of icons and elements to represent the nodes and their connections as follows:

Symbol	Usage
	Switch running Cumulus Linux OS
	Switch running RedHat, Ubuntu, or CentOS
	Host with unknown operating system

Symbol	Usage
	Host running Ubuntu
Red	Alarm (critical) event is present on the node
Yellow	Info event is present
Lines	Physical links or connections

## Interact with the Topology

There are a number of ways in which you can interact with the topology.

### Move the Topology Focus

You can move the focus on the topology closer to view a smaller number of nodes, or further out to view a larger number of nodes. As with mapping applications, the node labels appear and disappear as you move in and out on the diagram for better readability. To zoom, you can use:

- the zoom controls,  

- , in the bottom right corner of the screen; the ‘+’ zooms you in closer, the ‘-’ moves you further out, and the ‘o’ resets to the default size.
- a scrolling motion on your mouse
- your trackpad

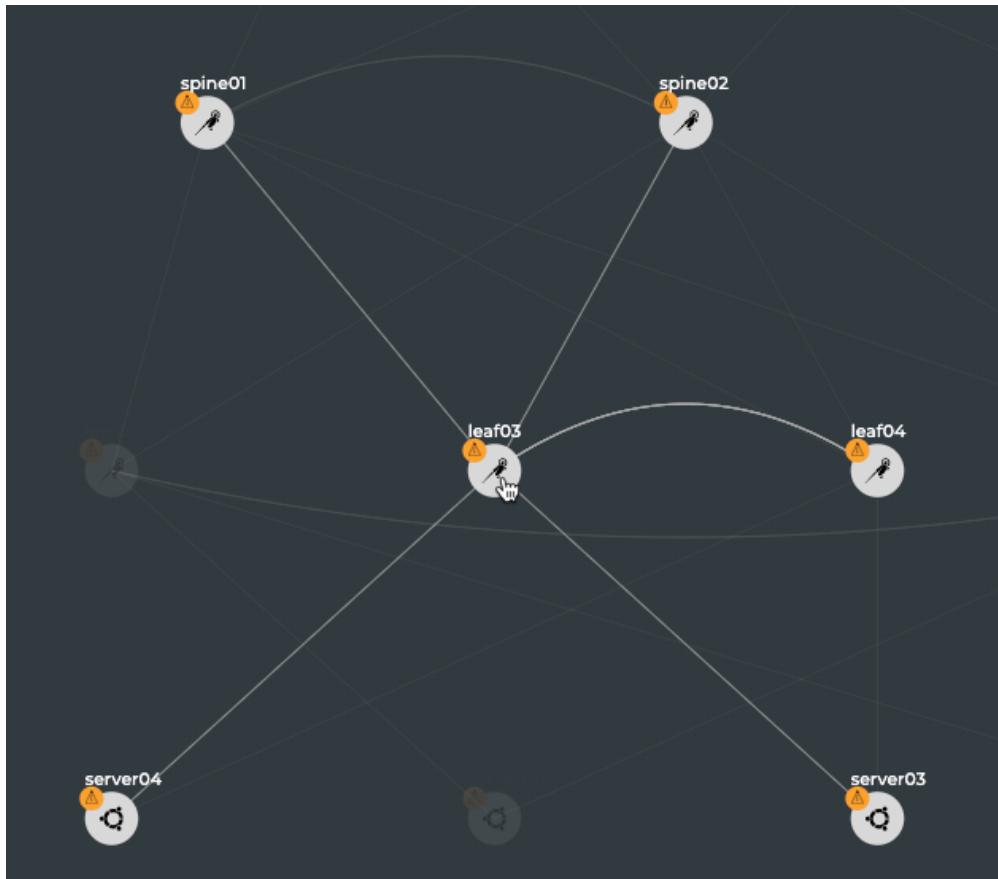
You can also click anywhere on the topology, and drag it left, right, up, or down to view a different portion of the network diagram. This is especially helpful with larger topologies.

## Monitor Using Topology View

## Interact with the Topology

### View Data About the Network

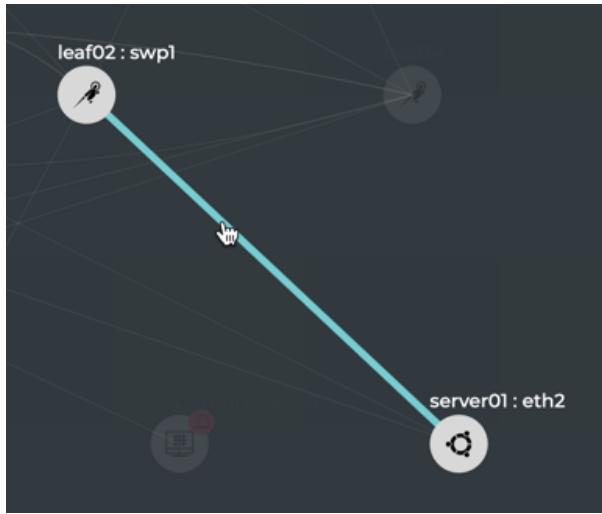
You can hover over the various elements to view data about them. Hovering over a node highlights its connections to other nodes, temporarily de-emphasizing all other connections.



Hovering over a line highlights the connection and displays the interface ports used on each end of the connection. All other connections are temporarily de-emphasized.

## Monitor Using Topology View

## Interact with the Topology

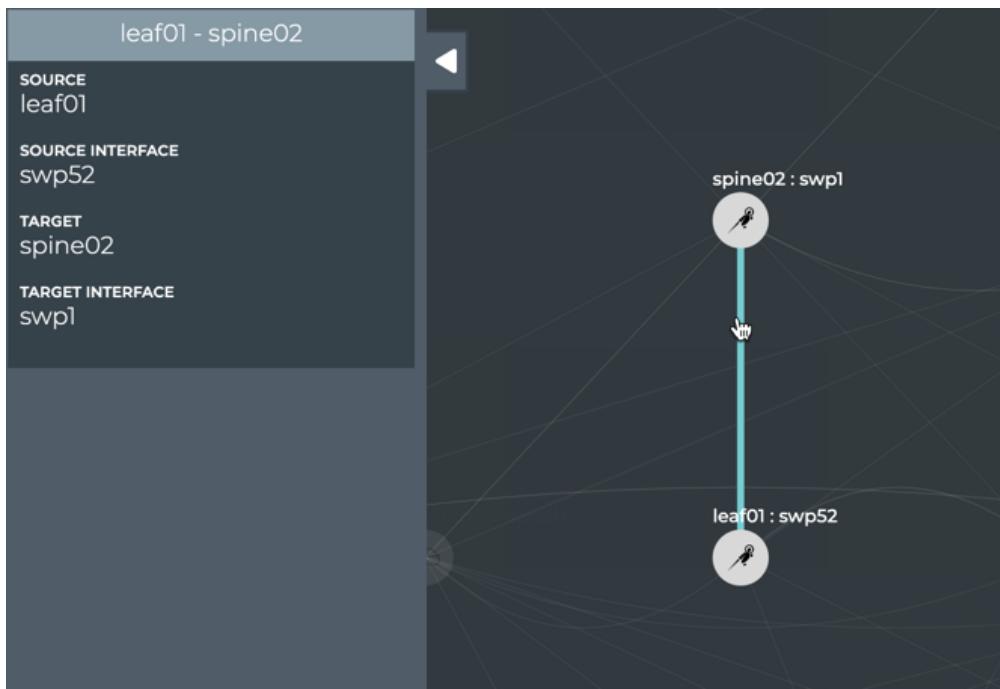


You can also click on the nodes and links to open the Configuration Panel with additional data about them.



## Monitor Using Topology View

## Interact with the Topology



From the Configuration Panel, you can view the following data about nodes and links:

Node Data	Description
ASIC	Name of the ASIC used in the switch. A value of Cumulus Networks VX indicates a virtual machine.
License State	Status of the Cumulus Linux license for the switch; OK, BAD (missing or invalid), or N/A (for hosts)
NetQ Agent Status	Operational status of the NetQ Agent on the switch; Fresh, Rotten
NetQ Agent Version	Version ID of the NetQ Agent on the switch
OS Name	Operating system running on the switch
Platform	Vendor and name of the switch hardware
Open Card/s	Opens the Event
⚠	Number of alarm events present on the switch
⚠	Number of info events present on the switch

Link Data	Description
Source	Switch where the connection originates
Source Interface	Port on the source switch used by the connection
Target	Switch where the connection ends
Target Interface	Port on the destination switch used by the connection

After reviewing the provided information, click



to close the panel, or to view data for another node or link without closing the panel, simply click on that element. The panel is hidden by default.

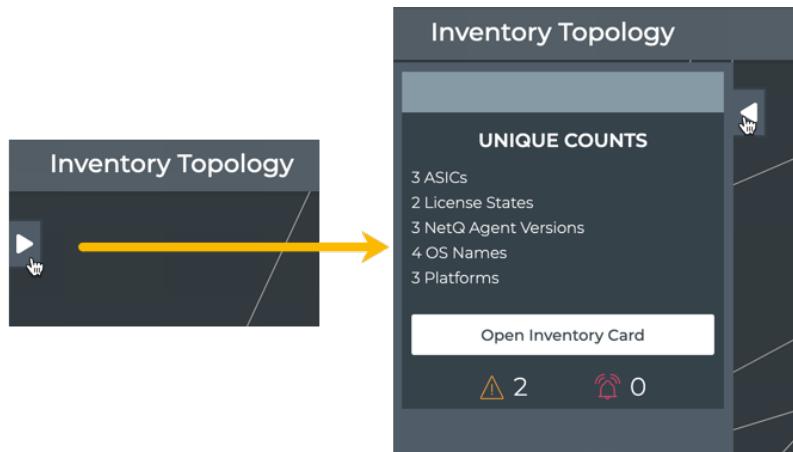
When no devices or links are selected, you can view the unique count of items in the network by clicking on the



on the upper left to open the count summary. Click



to close the panel.



You can change the time period for the data as well. This enables you to view the state of the network in the past and compare it with the current state. Click in the timestamp box in the topology header to select an alternate time period.



### Export Your NetQ Topology Data

The topology view provides the option to export your topology information as a JSON file. Click **Export** in the header.



The JSON file will be similar to this example:

```
{"inventory":{"unique_counts":{"asic":3,"license_state":2,"netq_agent_version":3,"os":4,"platform":3}}, "name":"topology", "tiers":{"0":"Tier 0","1":"Tier 1","2":"Tier 2","3":"Tier 3"}, "links":[{"id":35,"interfaces":[{"interface":"swp1","node":"leaf04"}, {"interface":"eth2","node":"server03"}]},{ "id":10,"interfaces": [{"interface":"swp51","node":"exit02"}, {"interface":"swp29","node":"spine01"}]}, {"id":32,"interfaces":[{"interface":"swp2","node":"leaf03"}, {"interface":"eth1","node":"server04"}]}, {"id":13,"interfaces": [{"interface":"swp51","node":"leaf02"}, {"interface":"swp2","node":"spine01"}]}, {"id":26,"interfaces": [{"interface":"swp44","node":"exit01"}, {"interface":"swp1","node":"internet"}]}, {"id":30,"interfaces": [{"interface":"swp31","node":"spine01"}, {"interface":"swp31","node":"spine02"}]}, {"id":23,"interfaces": [{"interface":"swp1","node":"leaf01"}, {"interface":"eth1","node":"server01"}]}, {"id":42,"interfaces": [{"interface":"swp51","node":"exit01"}, {"interface":"swp30","node":"spine01"}]}]
```

```
{"id":17,"interfaces":[{"interface":"swp52","node":"exit02"}, {"interface":"swp29","node":"spine02"}],"id":24,"interfaces": [{"interface":"swp50","node":"leaf03"}, {"interface":"swp50","node":"leaf04"}],"id":9,"interfaces": [{"interface":"eth0","node":"server04"}, {"interface":"swp5","node":"oob-mgmt-switch"}],"id":28,"interfaces": [{"interface":"swp50","node":"leaf01"}, {"interface":"swp50","node":"leaf02"}],"id":40,"interfaces": [{"interface":"swp51","node":"leaf04"}, {"interface":"swp4","node":"spine01"}],"id":12,"interfaces": [{"interface":"swp32","node":"spine01"}, {"interface":"swp32","node":"spine02"}],"id":29,"interfaces": [{"interface":"eth0","node":"leaf01"}, {"interface":"swp6","node":"oob-mgmt-switch"}],"id":25,"interfaces": [{"interface":"swp51","node":"leaf03"}, {"interface":"swp3","node":"spine01"}],"id":22,"interfaces": [{"interface":"swp1","node":"leaf03"}, {"interface":"eth1","node":"server03"}], ...}, {"inventory": {"asic": "Cumulus Networks VX", "license_state": "ok", "netq_agent_status": "Fresh", "netq_agent_version": "2.2.1-cl3u19~1564507571.4cb6474", "os": "CL 3.7.6", "platform": "Cumulus Networks VX"}, "name": "leaf04", "tier": 1, "interfaces": [{"name": "swp50", "connected_to": {"interface": "swp50", "link": 24, "node": "leaf03"}, {"name": "swp51", "connected_to": {"interface": "swp4", "link": 40, "node": "spine01"}, {"name": "swp2", "connected_to": {"interface": "eth2", "link": 5, "node": "server04"}, {"name": "swp1", "connected_to": {"interface": "eth2", "link": 35, "node": "server03"}, {"name": "swp49", "connected_to": {"interface": "swp49", "link": 2, "node": "leaf03"}, {"name": "swp52", "connected_to": {"interface": "swp4", "link": 11, "node": "spine02"}}], "protocol": {"bgp": false, "clag": false, "evpn": false, "lldp": true, "vni": []}, "events": {"count_alarm": 0, "count_info": 0}}, {"events": {"count_alarm": 0, "count_info": 0}}]
```