Cumulus NetQ 2.2

User Interface User Guide

Table of Contents

This guide is intended for network administrators and operators who are responsible for monitoring and troubleshooting the network in their data center environment. NetQ 2.1 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 .

UI Preface

A variety of resources are available for you to become familiar with Cumulus NetQ and to take advantage of its monitoring and analytic capabilities. These resources are identified here along with information about how the content is presented.

Contents

This topic describes...

What's New in Cumulus NetQ 2.2

Cumulus NetQ is now available as a cloud service, making it even easier to scale with your network growth. Just like Cumulus NetQ deployed in your premises, real-time data collection and fabric-wide performance analysis are available through the cloud service. New functionality has also been added to the NetQ UI.

Cumulus NetQ 2.2.0 includes the following new features and improvements:

For on-site and SaaS

- Graphical User Interface (UI)
    - Added ability to monitor and validate OSPF network protocol and services operation
    - Added ability to validate MTU, Sensors, VLAN and VXLAN protocols
    - Added events for MTU, OSPF, VLAN, and VXLAN
    - Added new standard user role, *user*, with reduced access permission compared to the administrative user
    - Added Prescriptive Topology Manager (PTM) events
- Command Line Interface (CLI)
    - Included Interface Statistics as an early access feature

For SaaS only

- Released new Cumulus NetQ Cloud Appliance to speed deployment and get monitoring as quickly as possible
- Added CLI support for installation and configuration of the Cumulus NetQ Cloud Appliance
- Added support for multiple data centers

For further information regarding new features, improvements, bug fixes, and known issues present in this release, refer to the release notes.

Available Documentation

The NetQ documentation set has been reorganized and updated from prior releases. They still provide the information you need to proactively monitor your Linux-based network fabric using Cumulus NetQ. They assume that you have already installed Cumulus Linux and NetQ.

You may start anywhere in the documentation or read it from start to finish depending on your role and familiarity with the NetQ software and Linux networking. If you are new to NetQ, you may want to read the Cumulus NetQ Primer before reading the other available documents.

The following NetQ documents are available:

- Cumulus NetQ Deployment Guide
- Cumulus NetQ CLI User Guide
- Cumulus NetQ UI User Guide (this guide)
- Cumulus NetQ Release Notes
- What the NetQ Validation System Checks
- Cumulus NetQ Release Versioning and Support Policy
- Cumulus NetQ Cloud Release Versioning and Support Policy

Document Formatting

This guide uses the following typographical and note conventions.

Typographical Conventions

Throughout the guide, text formatting is used to convey contextual information about the content.

Text Format	Meaning
Green text	Link to additional content within the topic or to another topic
`Text in Monospace font`	Filename, directory and path names, and command usage
[`Text within square brackets`]	Optional command parameters; may be presented in mixed case or all caps text
<`Text within angle brackets`>	Required command parameter values–variables that are to be replaced with a relevant value; may be presented in mixed case or all caps text

Note Conventions

Several note types are used throughout the document. The formatting of the note indicates its intent and urgency.

Tip or Best Practice

Offers information to improve your experience with the tool, such as time-saving or shortcut options, or i ndicates the common or recommended method for performing a particular task or process

Information

Provides additional information or a reminder about a task or process that may impact your next step or selection

Caution

Advises that failure to take or avoid specific action can result in possible data loss

Warning

Advises that failure to take or avoid specific action can result in possible physical harm to yourself, hardware equipment, or facility

NetQ User Interface Overview

The NetQ 2.2 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 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.

Before you get started, you should refer to the release notes for this version.

Contents

This topic describes...

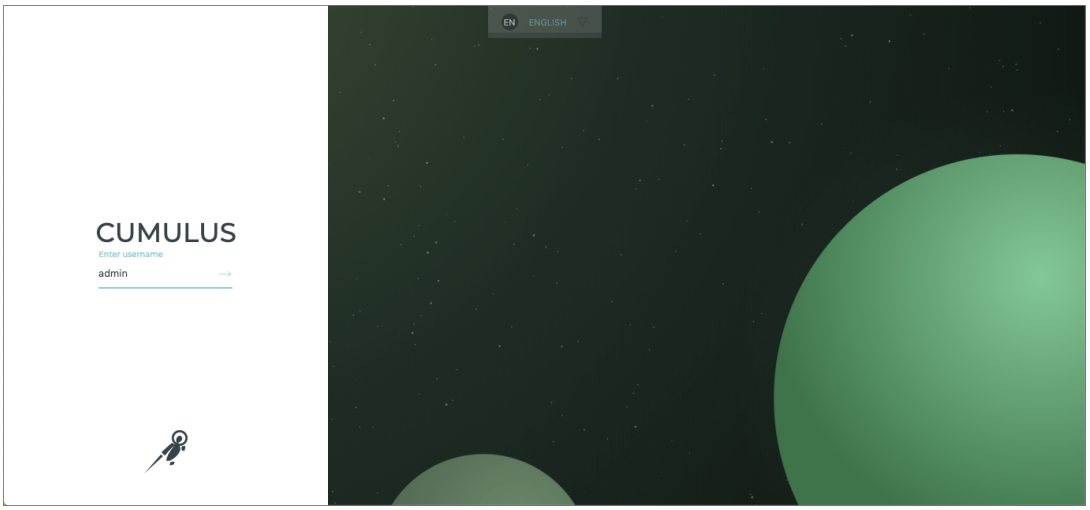
Access the NetQ UI

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

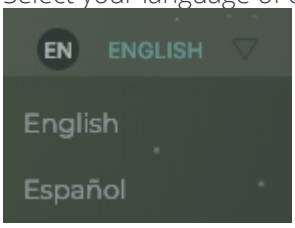
To log in to the UI:

1. Open a new Internet browser window or tab.

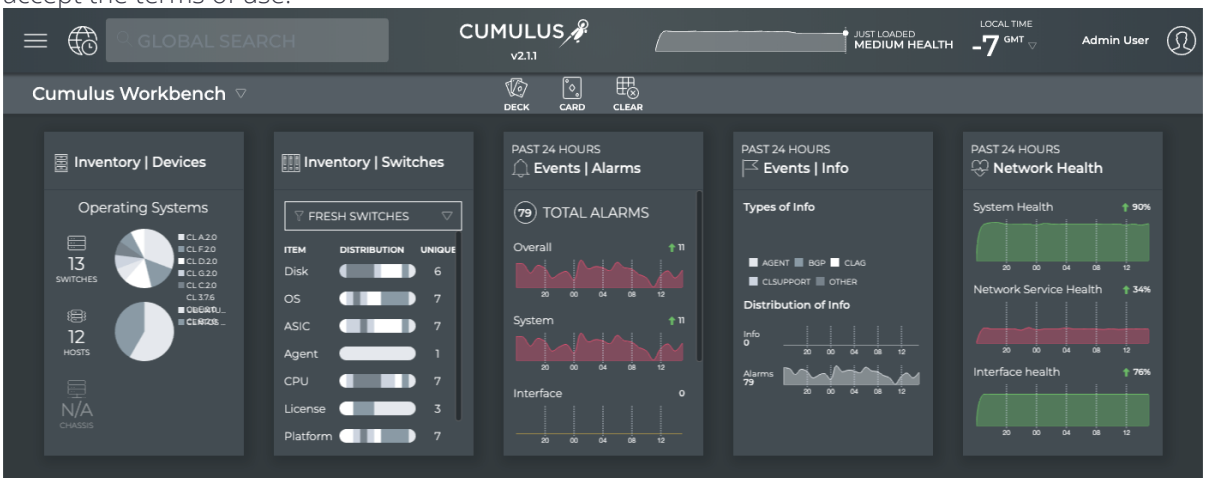
2. Enter the following URL into the Address bar for the on-site NetQ Platform/NetQ Appliance or the NetQ Cloud:
   - On-site: *http:// < netq-platform/appliance-ipaddress>:32666*
   - Cloud: *http//netq.cumulusnetworks.com*



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



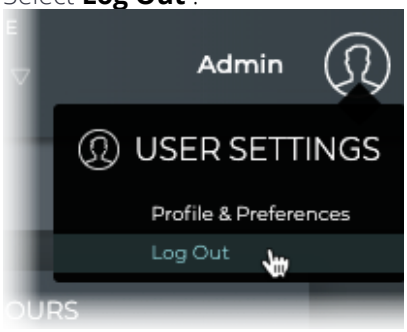
4. Enter your username and then your password:
   - NetQ Platform: *admin, admin* by default
   - NetQ Appliance: *cumulus, CumulusLinux!* by default
   - NetQ Cloud: Use credentials provided by Cumulus via email titled *Welcome to Cumulus NetQ!* and accept the terms of use.



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:

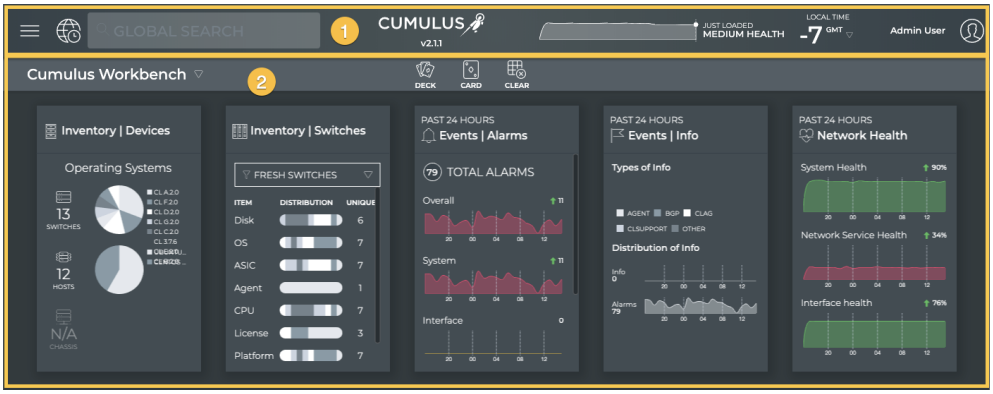
1. Click the user icon at the top right of the application.
2. Select **Log Out** .



Application Layout

The NetQ UI contains two areas:

- **Application Header** (1): Contains the main menu, navigation 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

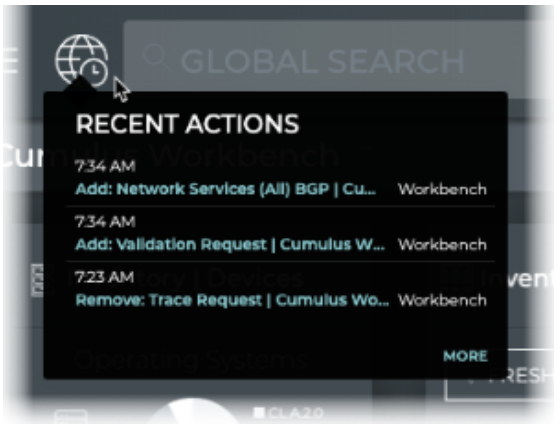
Found in the application header, click ☰ to open the main menu which provides navigation to:

- **Favorites**: contains list of links to workbenches that you have designated as favorites; Home is listed by default
- **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, the Recent Actions keeps track of every action you take on your workbench. 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.

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.

> 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.

> 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.

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.

> 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 preconfigured 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 modify a workbench by adding or removing cards or card decks, as described in Add or Remove a Card (see page 24) .

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.

Card Sizes

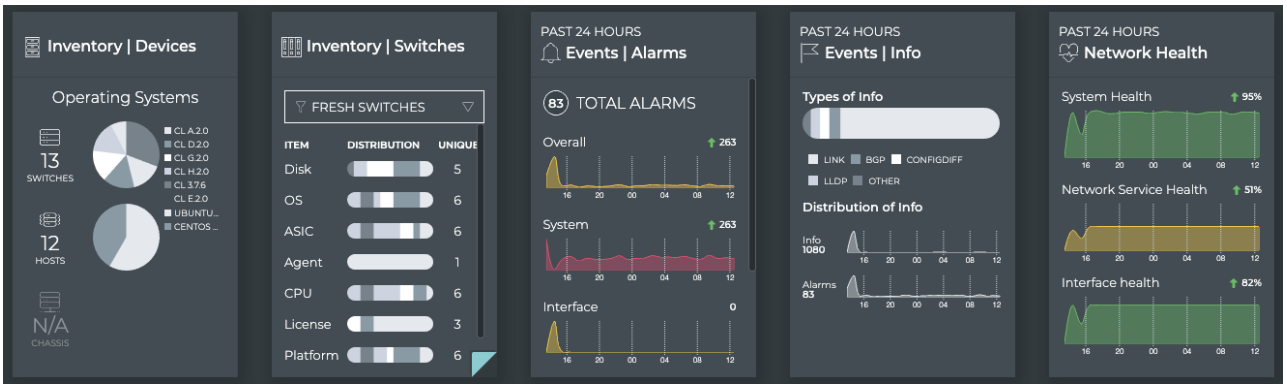
The various sizes of cards enables you to view your content at just the right level. For each aspect that you are monitoring there is typically a single card, that presents increasing amounts of data over its four sizes. For example, a snapshot of your total inventory may be sufficient, but to monitor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

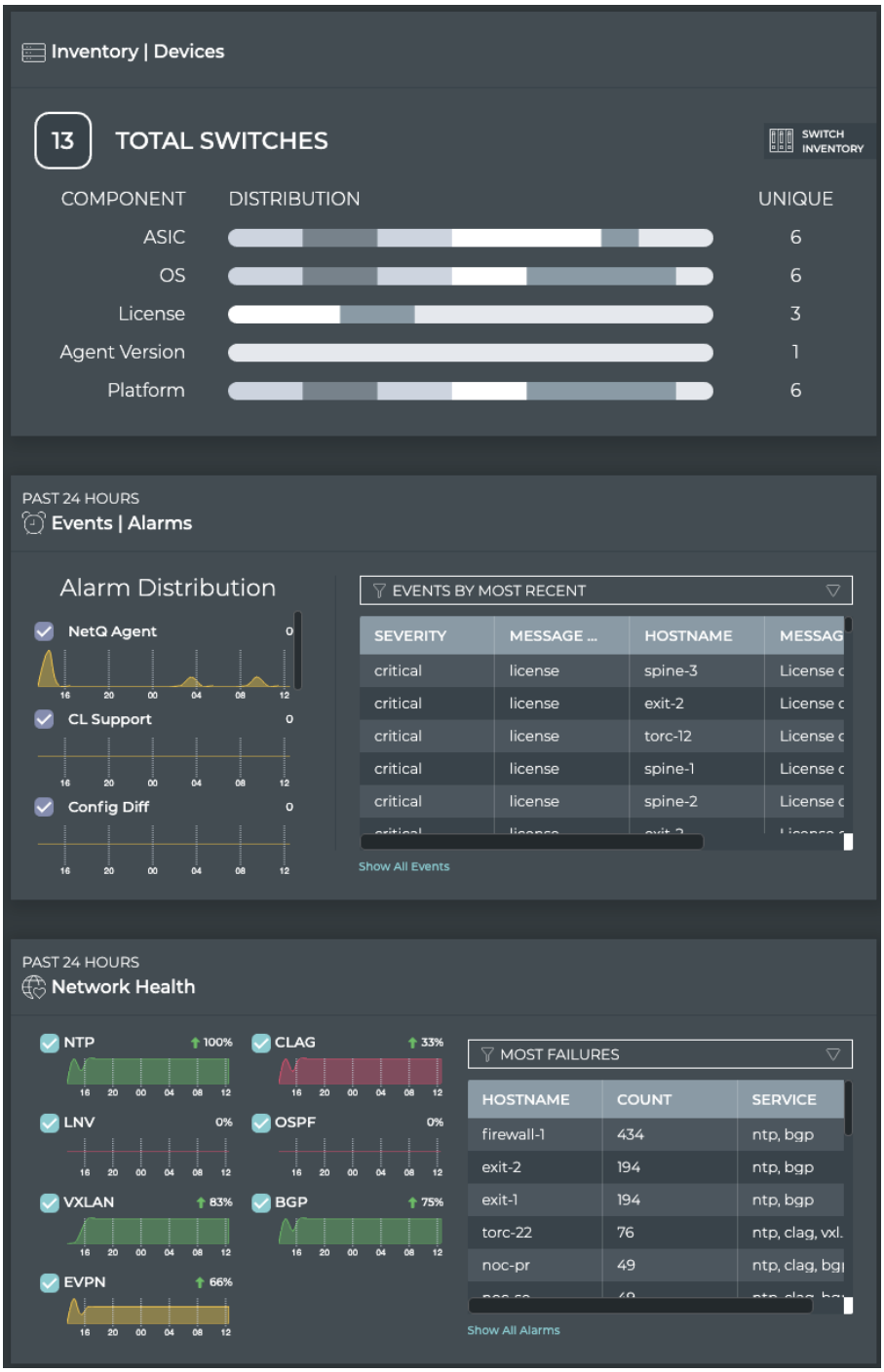
Medium Cards

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.



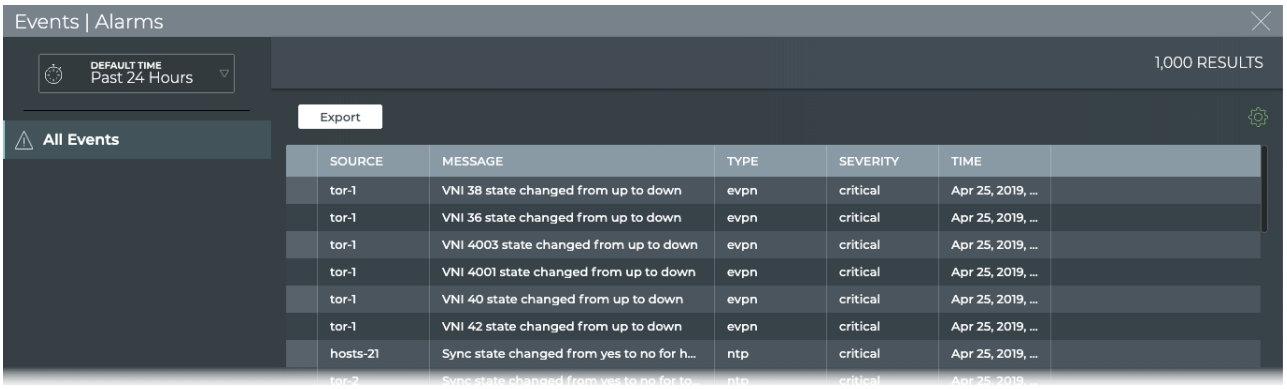
Large Cards

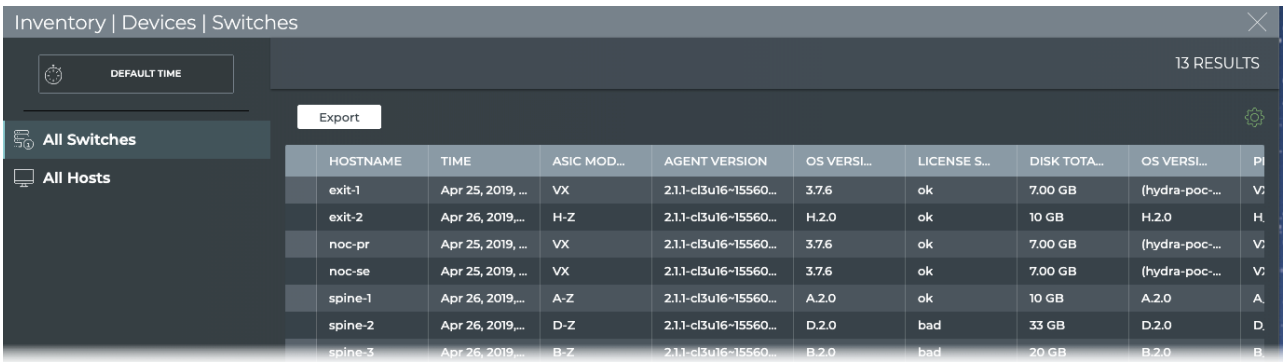
Large cards are most effective at providing the detailed information for monitoring specific components or functions of a given aspect of your network. These can aid in isolating and resolving existing issues or preventing potential issues. They are commonly comprised of detailed statistics and graphics. 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.



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





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 A Z.

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.

   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.

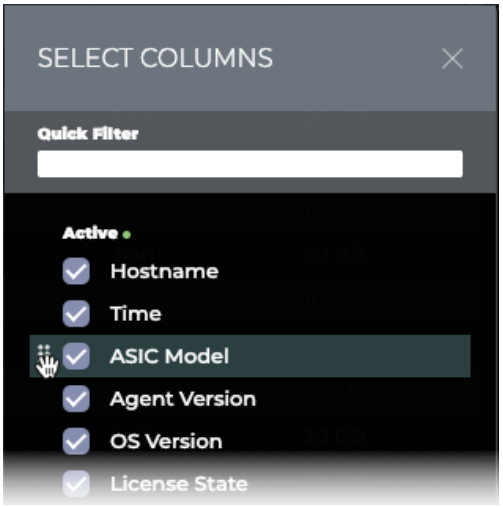
Change Order of Columns

1. Click and then click **Change Columns**.

2. Hover over a column name.

> 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.

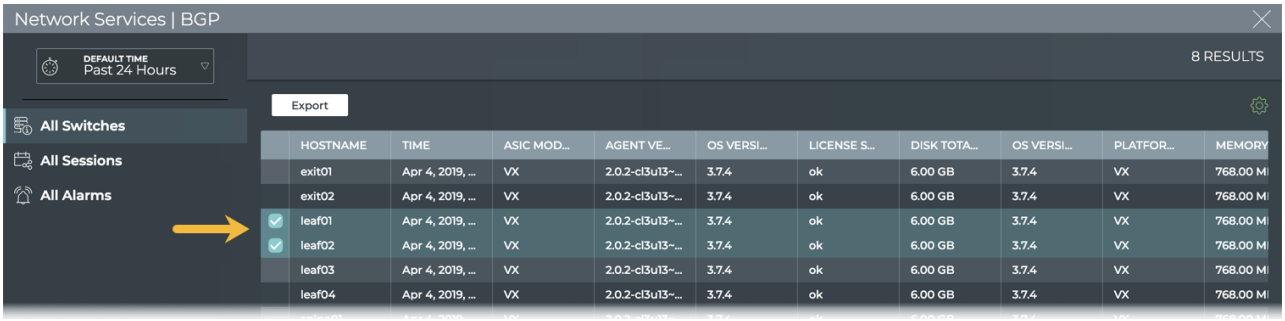


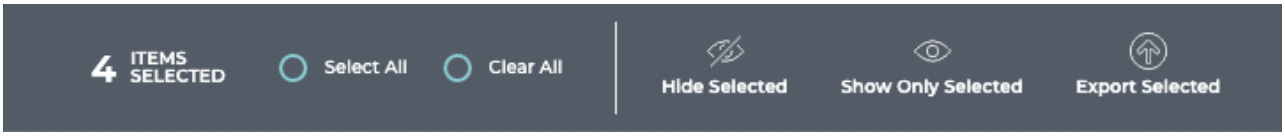
5. Click ✕ to close the selection box and view the updated data grid.

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).





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
Export Selected	Exports selected data into a .csv file. If you want to export to a .json file format, use the **Export** button.

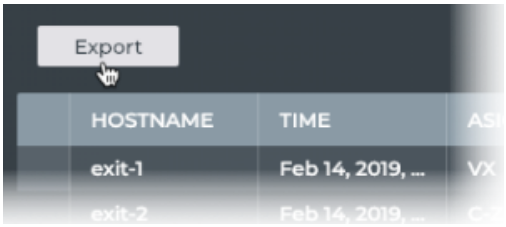
To return to original display of results, click the associated tab.

Export Data

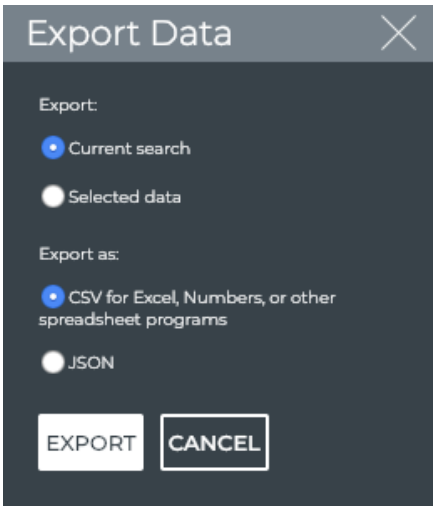
You can export tabular data from a full screen card to a CSV- or JSON-formatted file.

To export the data:

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



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 Size Summary

Card Size	Small	Medium	Large	Full Screen
Primary Purpose	• Quick view of status, typically at the level of good or bad • Enable quick actions, run a validation or trace for example	• View key performance parameters or statistics • Perform an action • Look for potential issues	• View detailed performance and statistics • Perform actions • Compare and review related information	• View all attributes for given network aspect • Free-form data analysis and visualization • Export data to third-party tools

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.

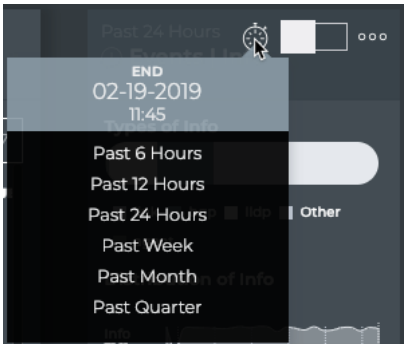
To access the time period, card size, and additional actions, hover over the card. These options appear, covering the card header, enabling you to select the desired option.

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:

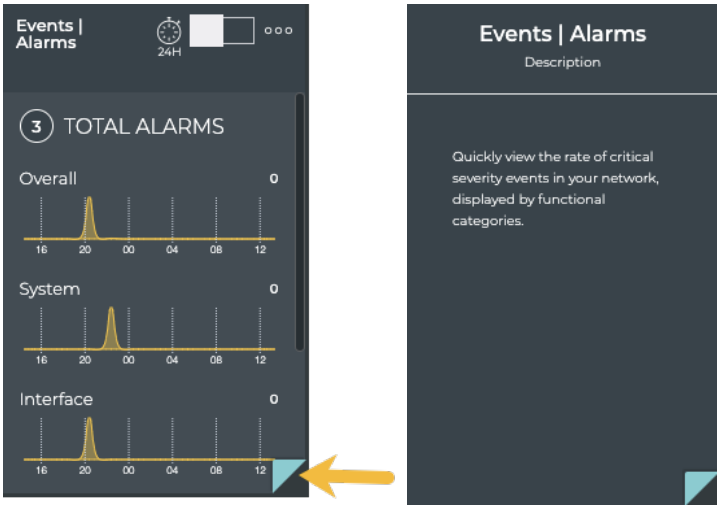
1. Hover over the card.
2. Hover over the Card Size Picker and move the cursor to the right or left until the desired size option is highlighted.

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.

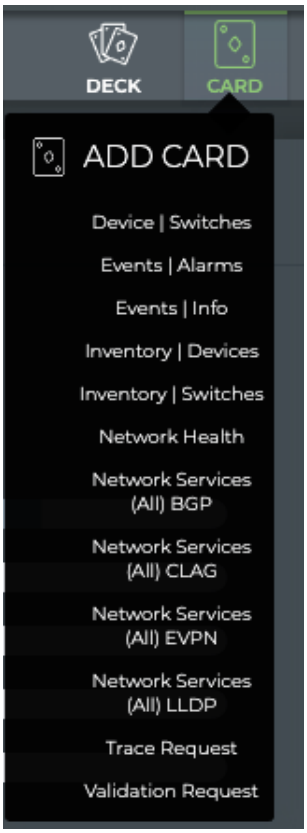
2. Release your hold on the card when the other card becomes highlighted with a dotted line. In this example, we are moving the medium Network Health card to the left of the medium Devices Inventory card.

Add or Remove a Card

You can add or remove cards from a workbench at any time.

To add a card:

1. Click .



2. Select a card from the available list.

The card is placed at the end of the set of cards currently on the workbench. You might need to scroll down to see it. By default, the medium size of the card is added to your workbench. You can move it to another location as described above.

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.

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

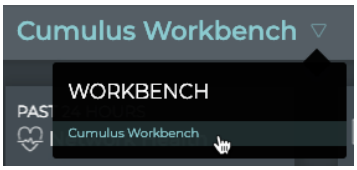
You can access a card workflow in multiple ways:

- 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

> 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 a prior search:

1. Browse your search list in the navigation panel.
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. Select the relevant card.

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 Decks

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.

User Settings

You can customize the NetQ application display, change their account password, and manage their workbenches.

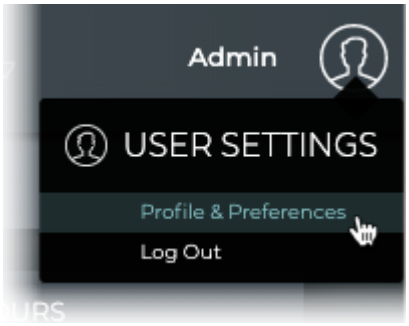
Configure Display Settings

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.

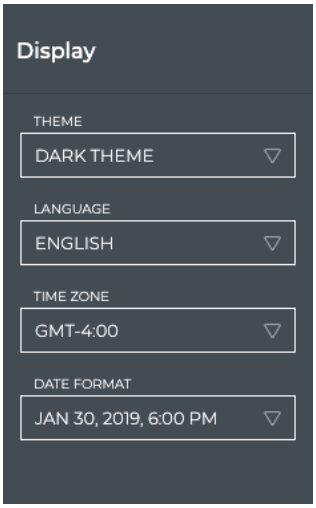
You can choose to view data in the time zone where you or your data center resides. You can also select the date and time format, choosing words or number format and a 12- or 24-hour clock. All changes take effect immediately.

To configure the display settings:

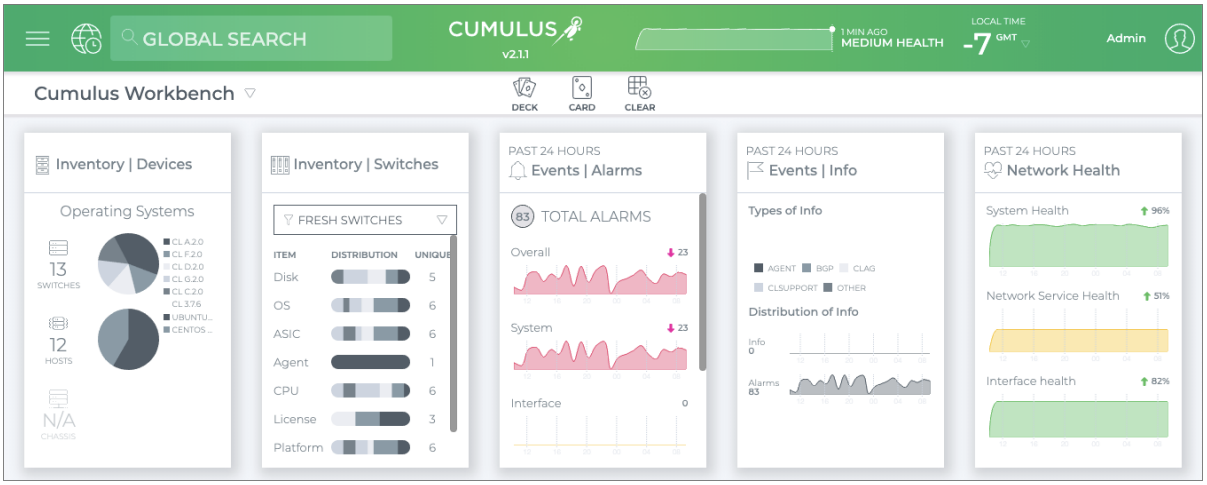
1. Click in the application header to open the **User Settings** options.



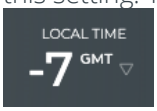
2. Click **Profile & Preferences**.
3. Locate the Display card.



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).

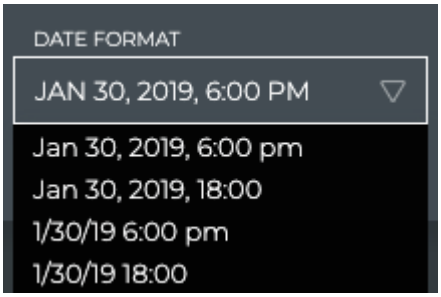


Note: *You can also change the time zone from the header display.*
If your deployment is not local to you (for example, you want to view the data from the perspective of a data center in another time zone) you can change the display to another time zone . The following table presents a sample of time 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
GMT	Greenwich Mean Time	GMT
GMT -1	Central African Time	CAT

Time Zone	Description	Abbreviation
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.

7. Return to your workbench by clicking ☰ and selecting a workbench from the NetQ list.

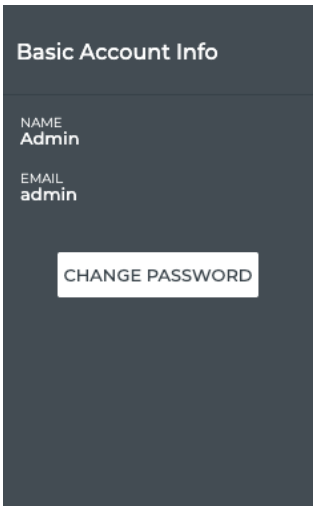
Change Your Password

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.

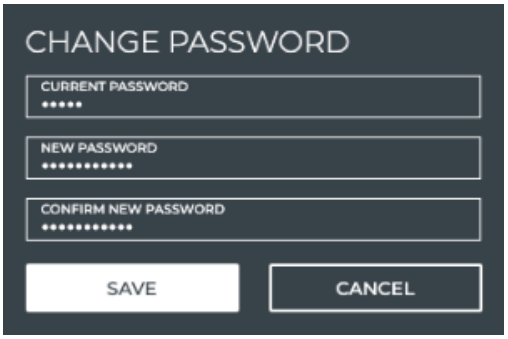
To change your password:

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.



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

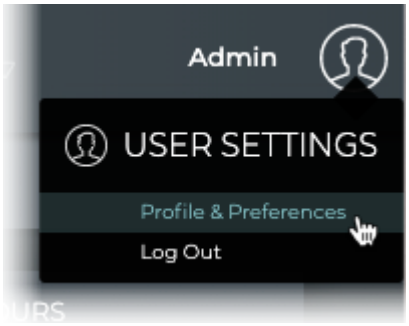
You can view all of your workbenches in a list form, making it possible to manage various aspects of them. There are public and private workbenches. Public workbenches are visible by all users. Private workbenches are visible only by the user who created the workbench. From the Workbenches card, you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

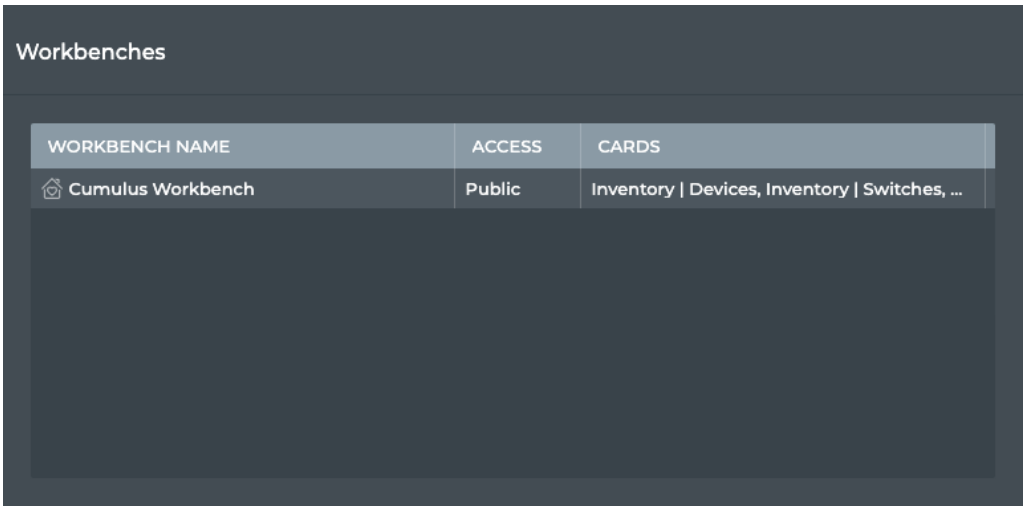
> **Caution**
>
> It is strongly recommended that you do not delete the default Cumulus Networks workbench. Once deleted, you must contact support to regain access to it. Extreme caution is recommended when deleting all other workbenches. Once they have been deleted, they cannot be restored.

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.



4. To specify a favorite workbench, click and drag next to the left of the desired workbench name.
5. To search and/or sort 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 delete a workbench, hover over the workbench name to view the **Delete** button. As an administrator, you can delete both private and public workbenches.
7. Return to your workbench by clicking and selecting a workbench from the NetQ list.

Basic Terminology and Acronyms

The following table covers some basic terms used throughout the NetQ user documentation.

Term	Definition
Agent	NetQ software that resides on a host server that provides metrics about the host to the NetQ Telemetry Server for network health analysis.
Alarm	In UI, event with critical severity.
Bridge	Device that connects two communication networks or network segments. Occurs at OSI Model Layer 2, Data Link Layer.
Clos	Multistage circuit switching network used by the telecommunications industry, first formalized by Charles Clos in 1952.
Device	UI term referring to a switch, host, or chassis or combination of these. Typically used when describing hardware and components versus a software or network topology. See also Node.
Event	Change or occurrence in network or component; may or may not trigger a notification. In the NetQ UI, there are two types of events: Alarms which indicate a critical severity event, and Info which indicate warning, informational, and debugging severity events.

Term	Definition
Fabric	Network topology where a set of network nodes is interconnected through one or more network switches.
Fresh	Node that has been heard from in the last 90 seconds.
High Availability	Software used to provide a high percentage of uptime (running and available) for network devices.
Host	Device that is connected to a TCP/IP network. May run one or more Virtual Machines.
Hypervisor	Software which creates and runs Virtual Machines. Also called a Virtual Machine Monitor.
Info	In UI, event with warning, informational, or debugging severity.
IP Address	An Internet Protocol address is comprised of a series of numbers assigned to a network device to uniquely identify it on a given network. Version 4 addresses are 32 bits and written in dotted decimal notation with 8-bit binary numbers separated by decimal points. Example: 10.10.10.255. Version 6 addresses are 128 bits and written in 16-bit hexadecimal numbers separated by colons. Example: 2018:3468:1B5F::6482:D673.
Leaf	An access layer switch in a Spine-Leaf or Clos topology. An Exit-Leaf is switch that connects to services outside of the Data Center such as firewalls, load balancers, and Internet routers. See also Spine, CLOS, Top of Rack and Access Switch.
Linux	Set of free and open-source software operating systems built around the Linux kernel. Cumulus Linux is one available distribution packages.
Node	UI term referring to a switch, host or chassis in a topology.
Notification	Item that informs a user of an event. In UI there are two types of notifications: Alert which is a n otification sent by system to inform a user about an event; specifically received through a third-party application, and Message which is a notification sent by a user to share content with another user.
Peerlink	Link, or bonded links, used to connect two switches in an MLAG pair.
Rotten	Node that has not been heard from in 90 seconds or more.
Router	Device that forwards data packets (directs traffic) from nodes on one communication network to nodes on another network. Occurs at the OSI Model Layer 3, Network Layer.
Spine	Used to describe the role of a switch in a Spine-Leaf or CLOS topology. See also Aggregation switch, End of Row switch, and distribution switch.

Term	Definition
Switch	High-speed device that connects that receives data packets from one device or node and redirects them to other devices or nodes on a network.
Telemetry server	NetQ server which receives metrics and other data from NetQ agents on leaf and spine switches and hosts.
Top of Rack	Switch that connects to the network (versus internally)
Virtual Machine	Emulation of a computer system that provides all of the functions of a particular architecture.
Web-scale	A network architecture designed to deliver capabilities of large cloud service providers within an enterprise IT environment.
Whitebox	Generic, off-the-shelf, switch or router hardware used in Software Defined Networks (SDN).

The following table covers some common acronyms used throughout the NetQ user documentation.

Acronym	Meaning
ACL	Access Control Link
ARP	Address Resolution Protocol
ASN	Autonomous System Number
BGP/eBGP/iBGP	Border Gateway Protocol, External BGP, Internal BGP
CLAG	Cumulus multi-chassis Link Aggregation Group
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Server
ECMP	Equal Cost Multi-Path routing
EVPN	Ethernet Virtual Private Network
FDB	Forwarding Data Base
GNU	GNU's Not Linux
HA	High Availability

IGMP	Internet Group Management Protocol
IPv4/IPv6	Internet Protocol, version 4 or 6
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLDP	Link Layer Data Protocol
MAC	Media Access Control
MIB	Management Information Base
MLAG	Multi-chassis Link Aggregation Group
MLD	Multicast Listener Discovery
NTP	Network Time Protocol
OOB	Out of Band (management)
OSPF	Open Shortest Path First
RFC	Remote Function Call
SDN	Software-Defined Network
SNMP	Simple Network Management Protocol
SSH	Secure SHell
SQL	Structured Query Language
STP	Spanning Tree Protocol
TCP	Transport Control Protocol
ToR	Top of Rack
UDP	User Datagram Protocol
URL	Universal Resource Locator

USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VNI	Virtual Network Instance
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRR	Virtual Router Redundancy
VTEP	VXLAN Tunnel EndPoint
VXLAN	Virtual Extensible Local Area Network
ZTP	Zero Touch Provisioning

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
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

Get Help

You can access the online user documentation for the UI from the Main Menu. Just click ☰ and select *Help Documentation* under the ADMIN category.

NetQ Management

As an administrator, you can manage access to and various application-wide settings for the 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 User Settings (see page 8) .

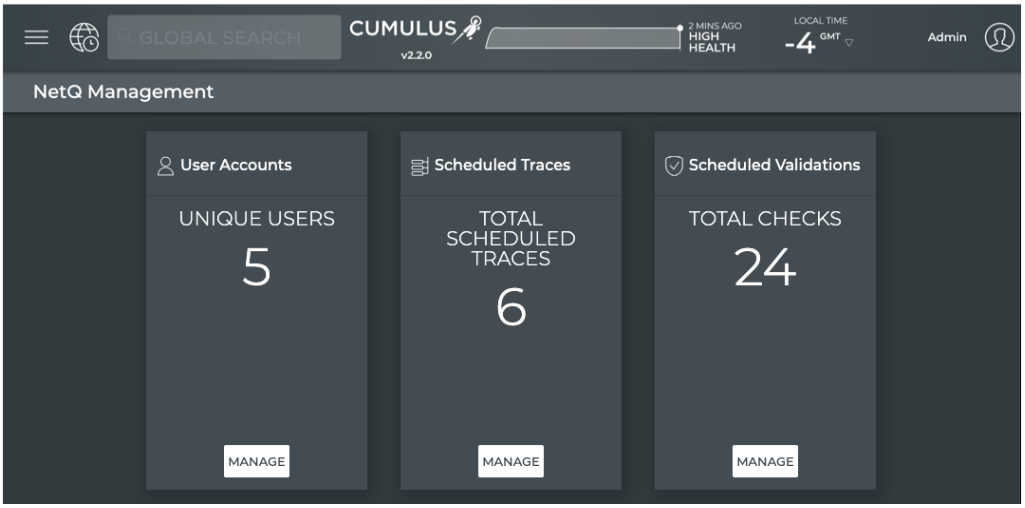
Contents

This topic describes how to...

NetQ Management Workbench

The NetQ Management workbench is accessed from the main menu and from the header of an open workbench. For the user or users 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.



Manage User Accounts

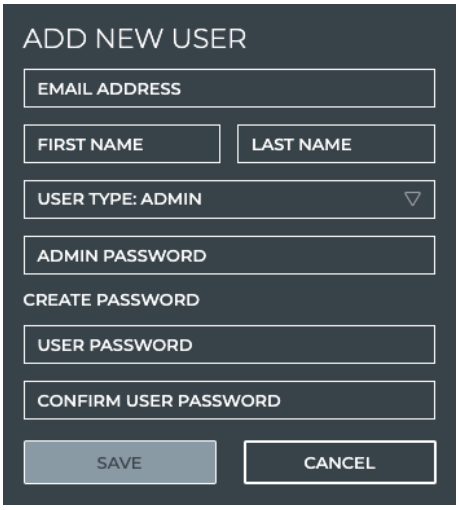
From the NetQ Management workbench, you can view the number of users with accounts in the system. As an administrator, you can also add, modify, and delete user accounts using the User Accounts card.

Add New User Account

For each user that monitors at least one aspect of your data center network, a user account is needed.

To add a new user account:

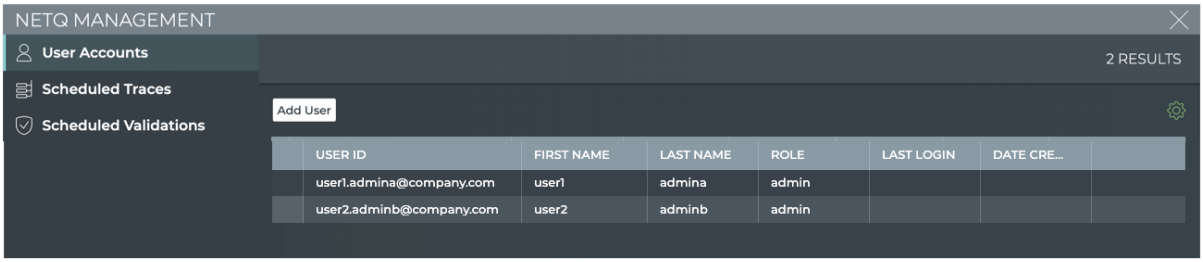
1. Click **Manage** on the User Accounts card.
2. Click the **User Accounts** tab.
3. Click **Add User**.



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

> ⚠ 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.

5. Select the user type: Admin or User.
6. Enter your password in the Admin Password field (only users with administrative permissions can add users).
7. 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.
8. Click **Save** to create the user account, or **Cancel** to discard the user account.
By default the User Accounts table is sorted by *User ID*. Change the sort by clicking in any of the headers.



> There is only the *admin* role at this time. Any user account you create will have administrator permissions.

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

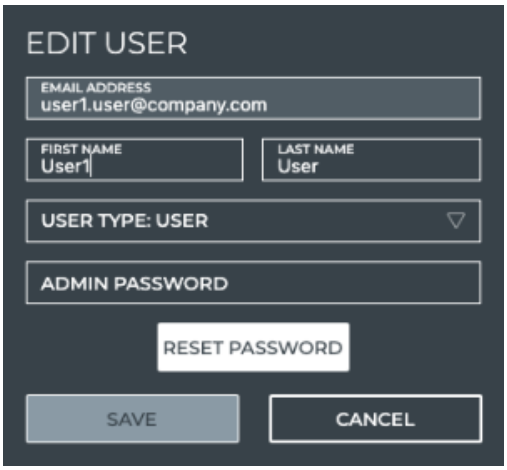
1. Click **Manage** on the User Accounts card.
2. Click the **User Accounts** tab.
3. Hover over the account you want to change, and click the checkbox next to it.
4. In the Edit menu that appears at the bottom of the window, click .
5. Modify the selected item, as described below.

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.
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. Modify the first and/or last name as needed.
6. Enter your admin password.



7. 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.
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. Click **Reset Password**.
6. Enter your admin password.

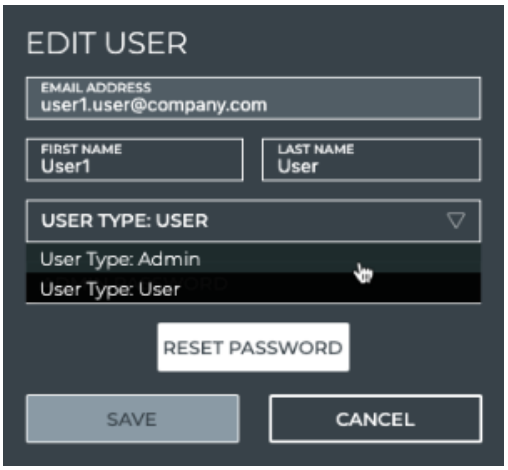
7. Enter a new password for the user.
8. Re-enter the user password. If the password you enter does not match, the Save is gray (not activated).
9. Click **Save** to commit the change, or **Cancel** to discard the change.

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.



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)

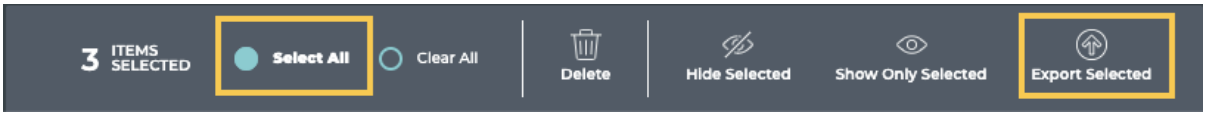
You cannot edit a user's email address, because this is the identifier the system uses for authentication. If you need to change an email address, you must create a new one for this user. Refer to Add a New User Account (see page). You should delete the incorrect user account. Select the user account, 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.
2. Click the **User Accounts** tab.
3. Hover over and select at least one user account.
4. To export all user accounts, click **Select All** and then **Export Selected**.



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

Manage Scheduled Traces

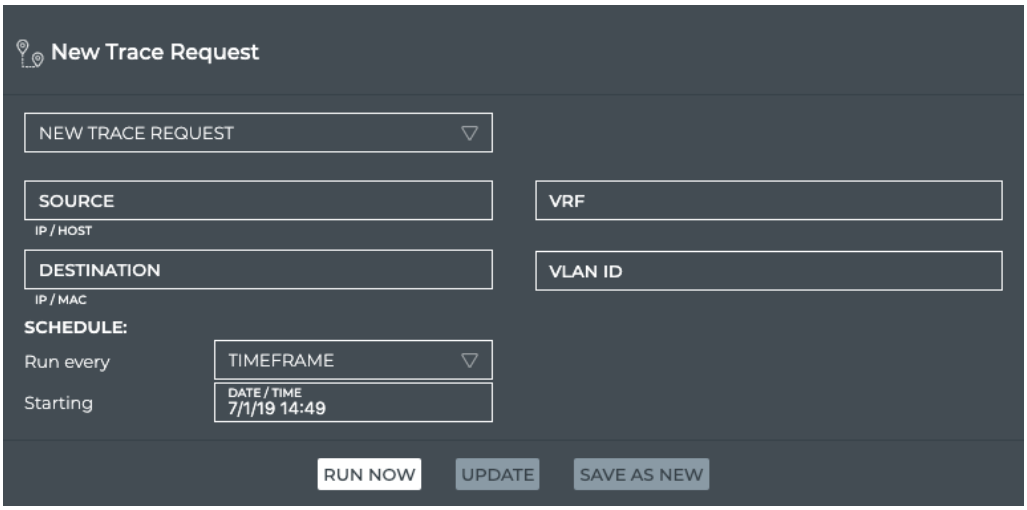
From the NetQ Management workbench, you can view the number of traces scheduled to run in the system. A set of default traces are provided with the NetQ GUI. As an administrator, you can run one or more scheduled traces, add new scheduled traces, and edit or delete existing traces.

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



4. Enter source and destination addresses.

> 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.

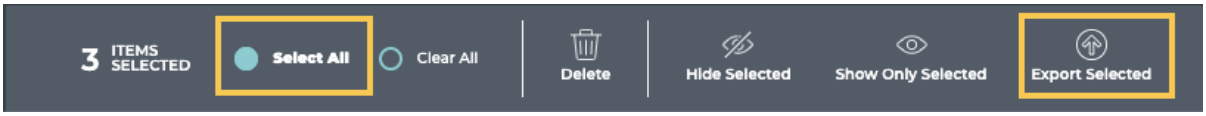
5. Specify a VLAN for a layer 2 trace or (optionally) a VRF for a layer 3 trace.
6. Set the schedule for the trace, by selecting how often to run the trace and when to start it the first time.
7. Click **Save As New** to add the trace. You are prompted to enter a name for the trace in the **Name** field.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

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.
2. Click the **Scheduled Traces** tab.
3. Hover over and select at least one trace.
4. To export all validations, click **Select All** and then **Export Selected**.



5. 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 preconfigured with the NetQ UI. 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:

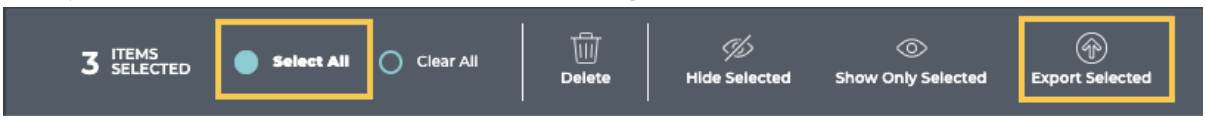
1. Click **Manage** on the Scheduled Validations card.
2. Click the **Scheduled Validations** tab.
3. Click ✕ in the top right to return to your NetQ Management cards.

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**.



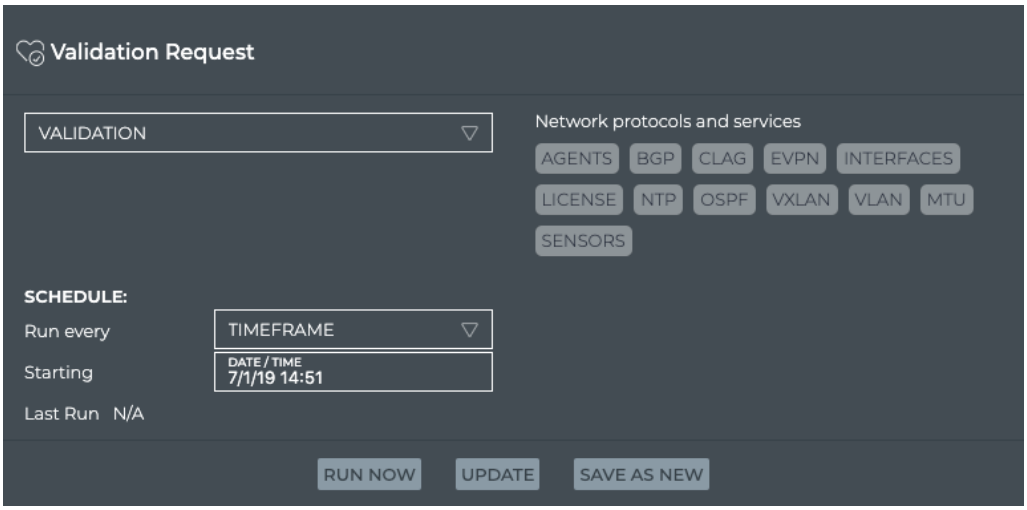
5. To export specific validations, select only those validations you want to export, and click **Export Selected**.

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.



4. Configure the request. Refer to Validate Network Protocol and Service Operations (see page 57) for details.

Monitor the Network

The topics contained in this section describe monitoring tasks that apply across the entire network. For device-specific monitoring refer to Monitor Switches (see page 258).

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.

Contents

This topic describes how to...

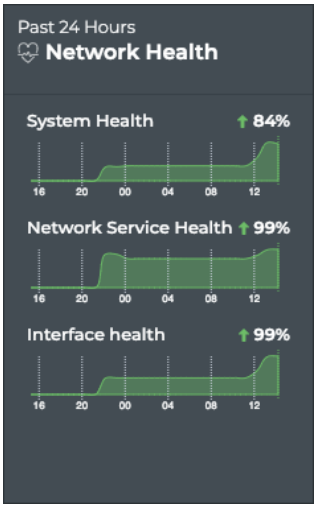
Network Health Card Workflow Summary

The small Network Health card displays:

Item	Description
	Indicates data is for overall Network Health
	Trend of overall network health, represented by an arrow:

Item	Description
Health trend	• **Pointing upward and green**: Health score in the most recent window is higher than in the last two data collection windows, an increasing trend • **Pointing downward and bright pink**: Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend • **No arrow**: Health score is unchanged over the last two data collection windows, trend is steady 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.
Health score	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. 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.
Health rating	Performance rating based on the health score during the time window: • **Low**: Health score is less than 40% • **Med**: Health score is between 40% and 70% • **High**: Health score is greater than 70%
Chart	Distribution of overall health status during the designated time period

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

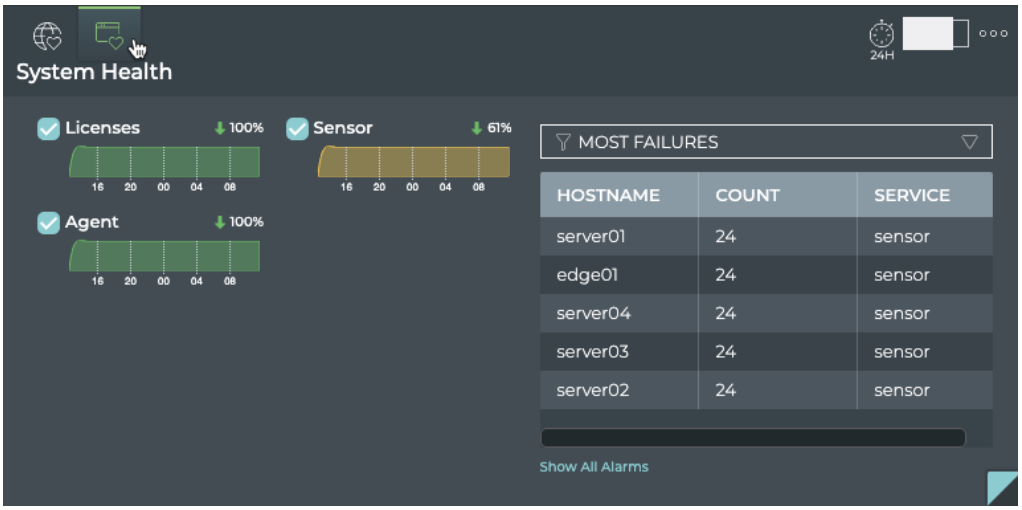


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes

Item	Description
	Indicates data is for overall Network Health
Health trend	Trend of system, network service, and interface health, represented by an arrow: • **Pointing upward and green**: Health score in the most recent window is higher than in the last two data collection windows, an increasing trend • **Pointing downward and bright pink**: Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend • **No arrow**: Health score is unchanged over the last two data collection windows, trend is steady 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.
Health score	Percentage of devices which passed validation versus the number of devices checked during the time window for: • **System health**: NetQ Agent health, Cumulus Linux license status, and sensors • **Network services health**: BGP, CLAG, EVPN, LNV, NTP, OSPF, and VXLAN health • **Interface health**: interfaces MTU, VLAN health 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.
Chart	Distribution of overall health status during the designated time period

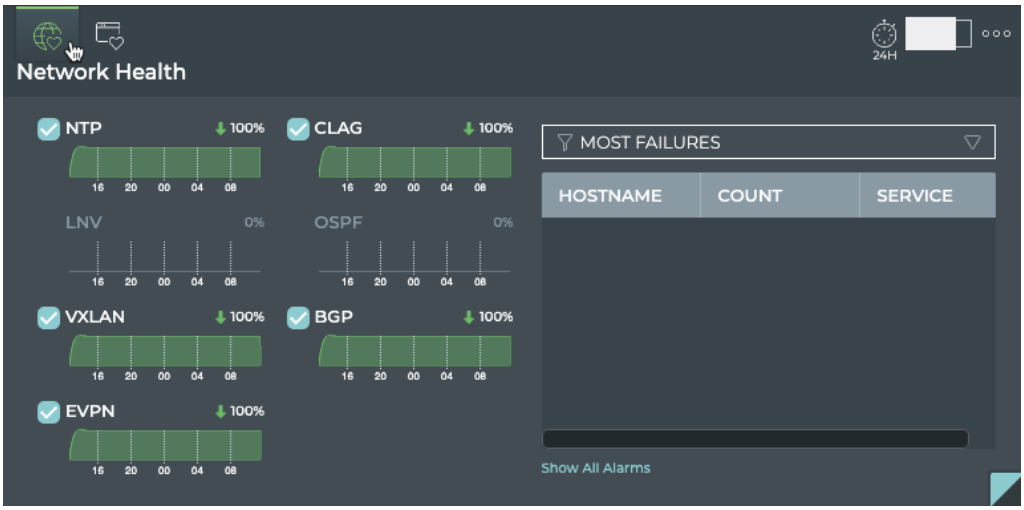
The large Network Health card contains two tabs.

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 overall Network Health
Health trend	Trend of NetQ Agents, Cumulus Linux licenses, and sensor health, represented by an arrow: • **Pointing upward and green**: Health score in the most recent window is higher than in the last two data collection windows, an increasing trend • **Pointing downward and bright pink**: Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend • **No arrow**: Health score is unchanged over the last two data collection windows, trend is steady 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.
Health score	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. 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.
Charts	Distribution of health score for NetQ Agents, Cumulus Linux license status, and platform sensors during the designated time period
Table	Listing of items that match the filter selection: • **Most Failures**: Devices with the most validation failures are listed at the top • **Recent Failures**: Most recent validation failures are listed at the top
Show All Devices	Opens full screen Network Health card with a listing of all events

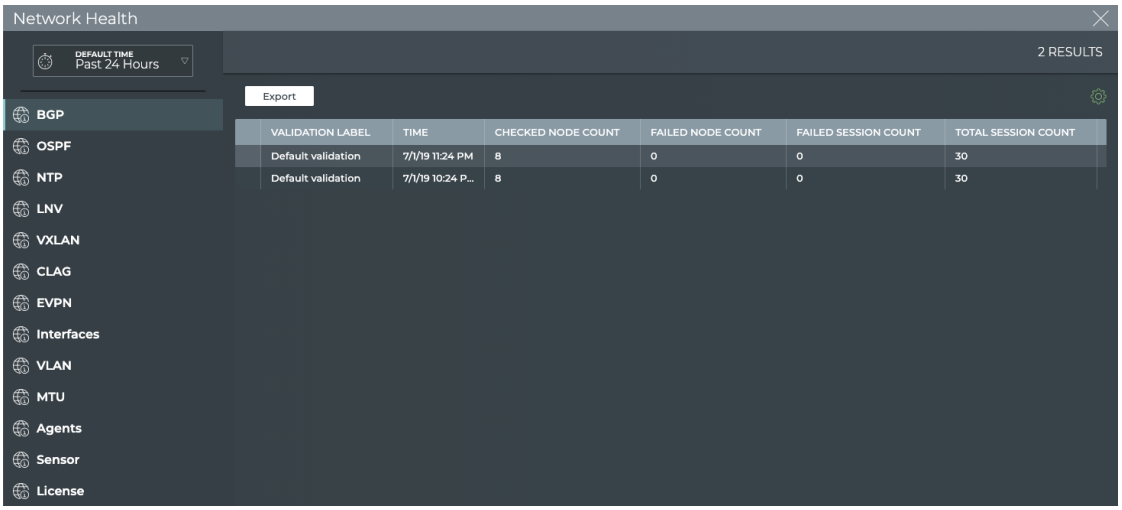
The *Network Services Health* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for overall Network Health
Health trend	Trend of BGP, CLAG, EVPN, LNV, NTP, and VXLAN services health, represented by an arrow: • **Pointing upward and green**: Health score in the most recent window is higher than in the last two data collection windows, an increasing trend • **Pointing downward and bright pink**: Health score in the most recent window is lower than in the last two data collection windows, a decreasing trend • **No arrow**: Health score is unchanged over the last two data collection windows, trend is steady 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.
Health score	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. 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.
Charts	Distribution of passing validations for BGP, CLAG, EVPN, LNV, NTP, and VXLAN services during the designated time period
Table	Listing of devices that match the filter selection: • **Most Failures**: Devices with the most validation failures are listed at the top • **Recent Failures**: Most recent validation failures are listed at the top

Item	Description
Show All Devices	Opens full screen Network Health card with a listing of all events

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



Item	Description
Title	Network Health
X	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
Each network protocol or service	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 (**Time**). This tab provides the following additional data about each protocol and service: • **Validation Label**: User-defined name of a validation or Default validation • **Checked Node Count**: Number of nodes running the service included in the validation • **Failed Node Count**: Number of nodes that failed the validation • **Failed Session Count**: Number of sessions that failed the validation. Only applies to BGP, CLAG, EVPN, and OSPF. • **Total Session Count**: Number of sessions running the protocol or service included in the validation. Only applies to BGP, CLAG, EVPN, and OSPF.

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 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.

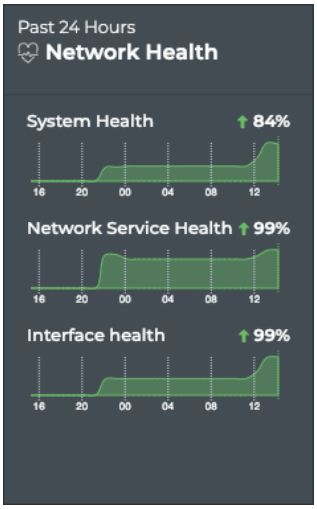
To view a summary of your network health, open the small Network Health card.

In this example, the overall health is quite low and digging further for causes is definitely warranted. 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 the percentage of successful validations, a trend indicator, and a distribution of the validation results.



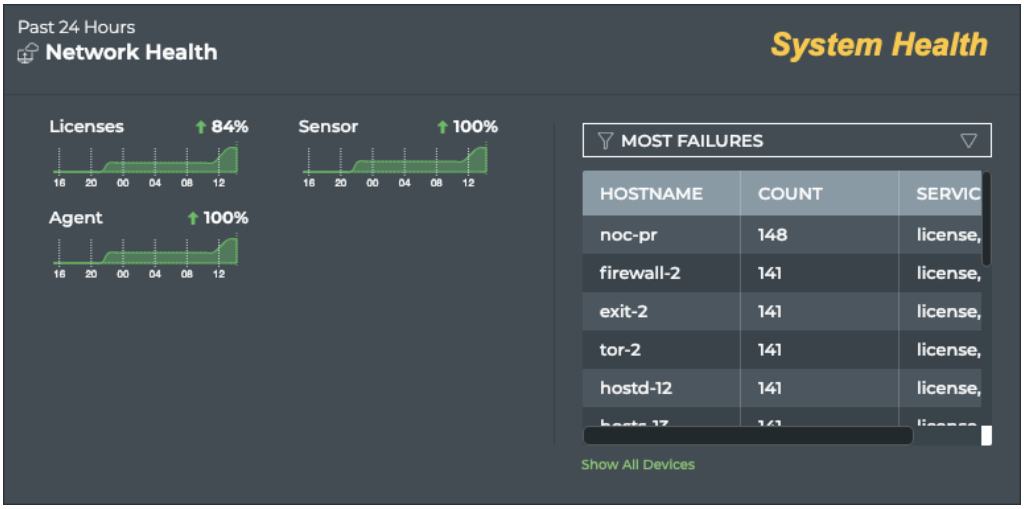
In this example, the health of each of the three key metrics are all good. You might choose to dig further on the system health if it did not continue to improve. Refer to the following section for additional details.

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:

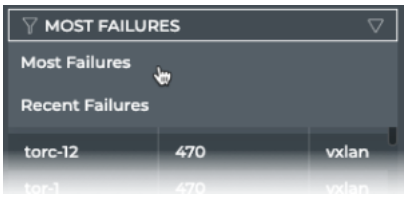
1. Open the large Network Health card.
2. Hover over the card and click .



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.



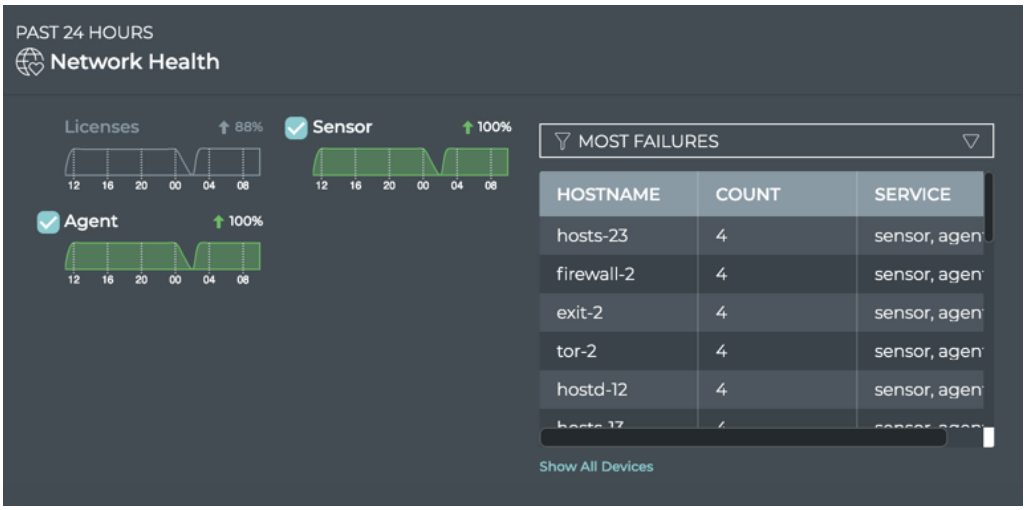
Devices with the highest number of issues are listed at the top. Scroll down to view those with fewer issues. To further investigate the critical devices, open the Event cards and filter on the indicated switches.

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.



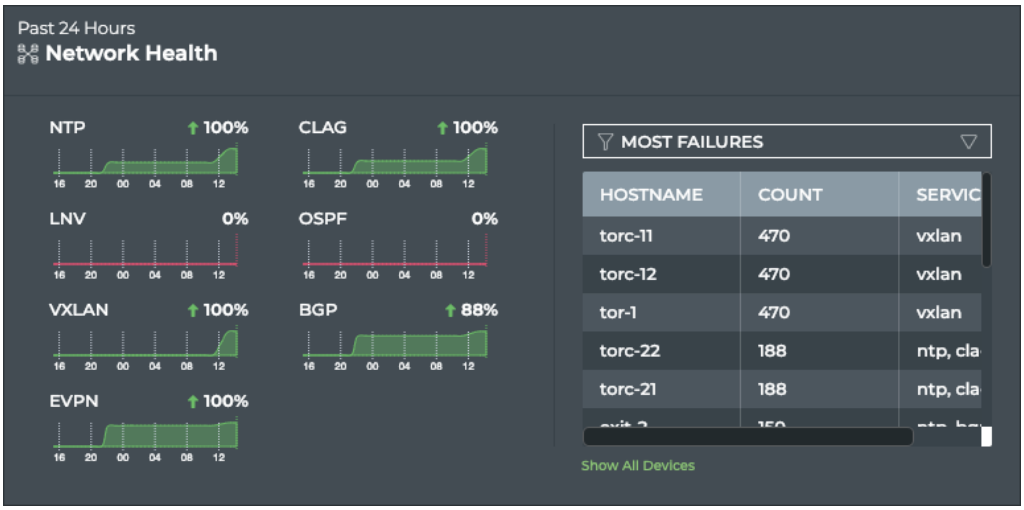
This grays out the associated chart and temporarily removes the data related to that service from the table.

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 .



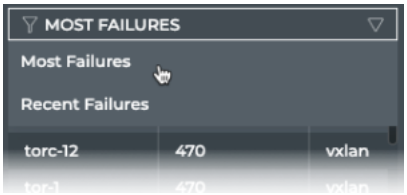
The health of each protocol or service is represented on the left side of the card by a distribution of the health score, a trend indicator, and a percentage of successful results. The right side of the card provides a listing of devices running the services.

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.



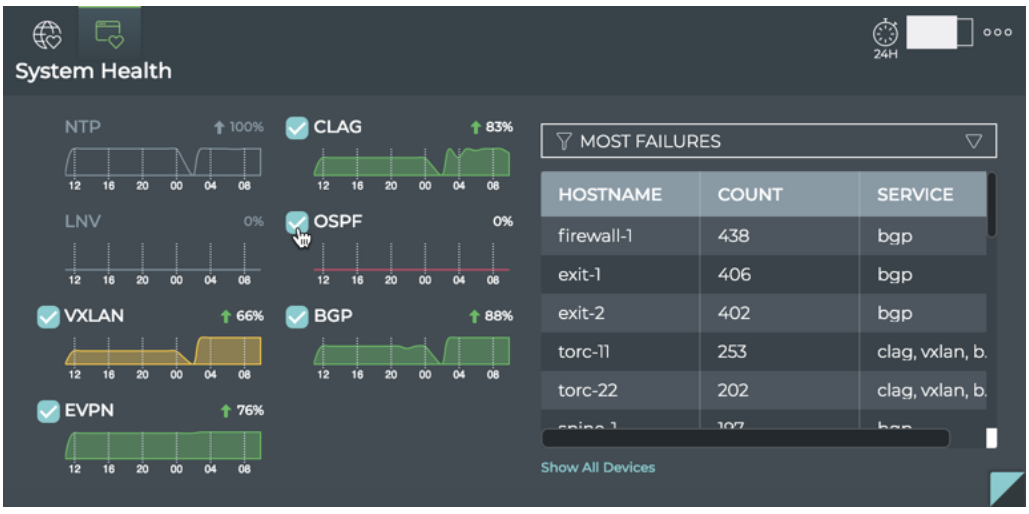
Devices with the highest number of issues are listed at the top. Scroll down to view those with fewer issues. To further investigate the critical devices, open the Event cards and filter on the indicated switches.

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 are removed NTP and LNV and are in the process of removing OSPF.



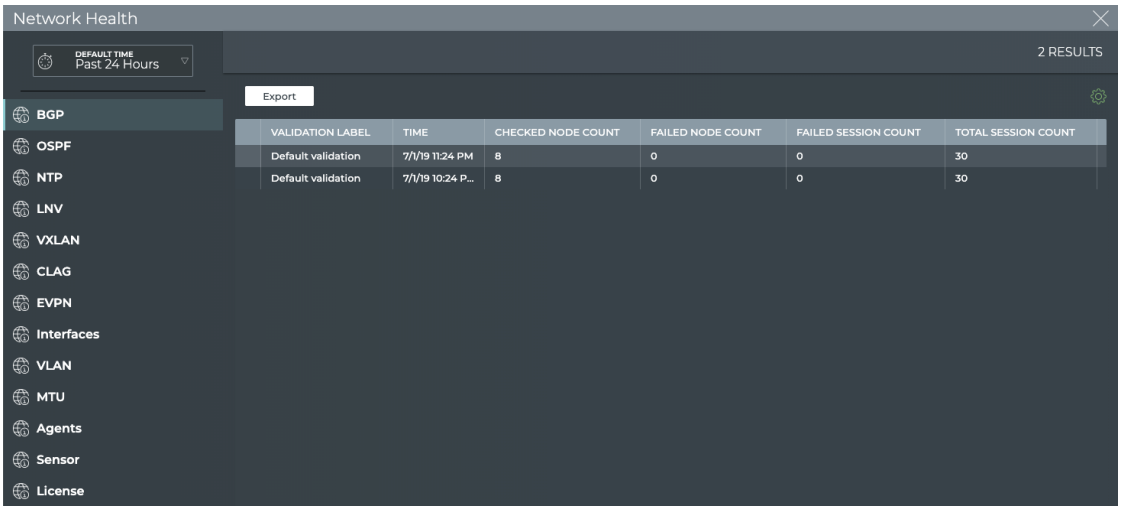
This grays out the charts and temporarily removes the data related to that service from the table.

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?



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 (see page 47) topic.

Contents

This topic describes how to...

Create Validation Requests

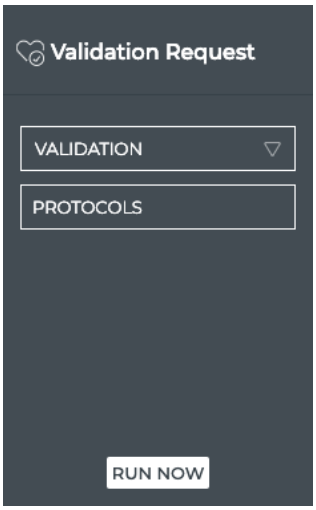
The Validation Request card workflow is used to create on-demand validation requests to evaluate the health of your network protocols and services.

Validation Request Card Workflow

The small Validation Request card displays:

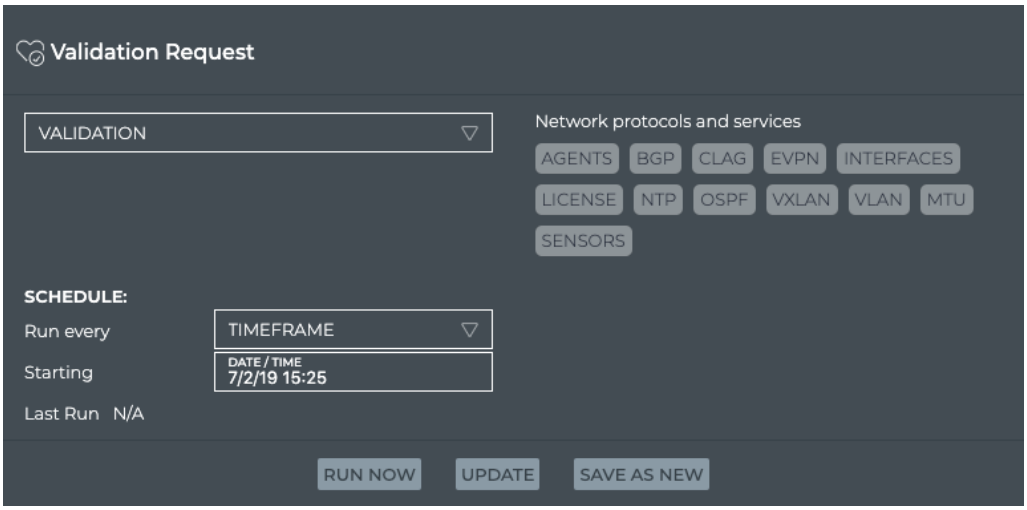
Item	Description
	Indicates a validation request
Validation	Select a scheduled request to run that request on-demand. A default validation is provided for each supported network protocol and service, which runs a network-wide validation check. These validations run every 60 minutes, but you may run them on-demand at any time. **Note**: 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	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. **Note**: No new requests can be configured from this size card.
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

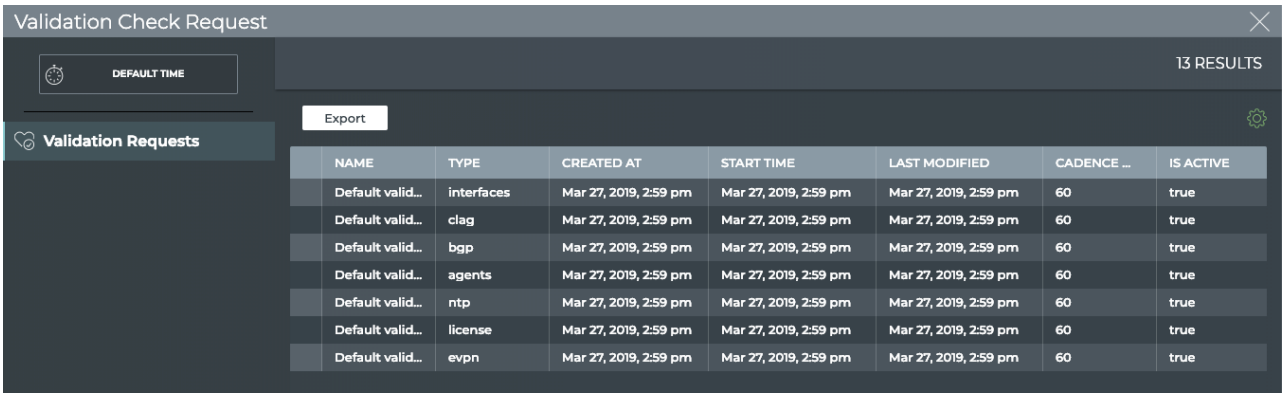
The large Validation Request card displays:



Item	Description
	Indicates a validation request
Title	Validation Request
Validation	Depending on user intent, this field is used to: • 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. • Leave as is to create a new scheduled validation request • Select a scheduled request to modify
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:	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. • Run Every: Select how often to run the request. Choose from 30 minutes, 1, 3, 6, or 12 hours, or 1 day. • Starting: Select the date and time to start the first request in the series • Last Run: Timestamp of when the selected validation was started
Run Now	Start the validation request
Update	When changes are made to a selected validation request, **Update** becomes available so that you can save your changes.

Item	Description
	Be aware, that if you update a previously saved validation request, the historical data collected will no longer match the data results of future runs of the request. If your intention is to leave this request unchanged and create a new request, click **Save As New** instead.
Save As New	When changes are made to a previously saved validation request, **Save As New** 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.



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	Displays all *scheduled* validation requests. By default, the requests list is sorted by the date and time that it was originally created (**Created At**). This tab provides the following additional data about each request: • **Name**: Text identifier of the validation • **Type**: Name of network protocols and/or services included in the validation • **Start Time**: Data and time that the validation request was run • **Last Modified**: Date and time of the most recent change made to the validation request • **Cadence (Min)**: How often, in minutes, the validation is scheduled to run. This is empty for new on-demand requests.

Item	Description
	• **Is Active**: Indicates whether the request is currently running according to its schedule (*true*) or it is not running (*false*)
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

Creating 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:

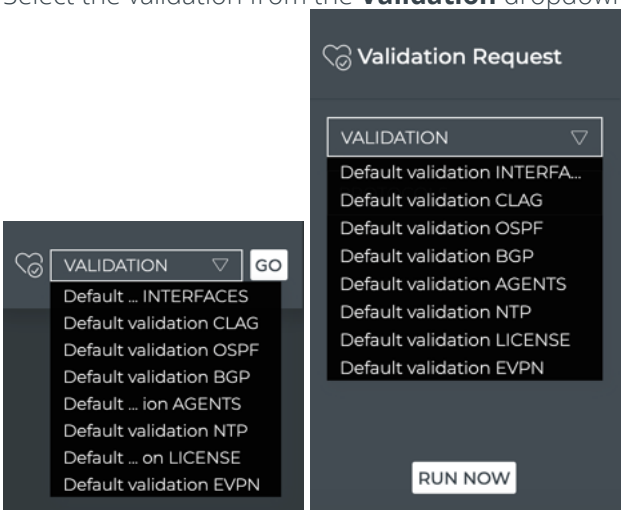
- Run an Existing Scheduled Validation Request On Demand (see page)
- Create a New On-demand Validation Request (see page)
- Modify an On-demand Validation Request (see page)
- Save and Schedule an On-demand Validation Request (see page)
- Create a New Scheduled Validation Request (see page)
- Modify a Scheduled Validation Request (see page)

Run an Existing Scheduled Validation Request On Demand

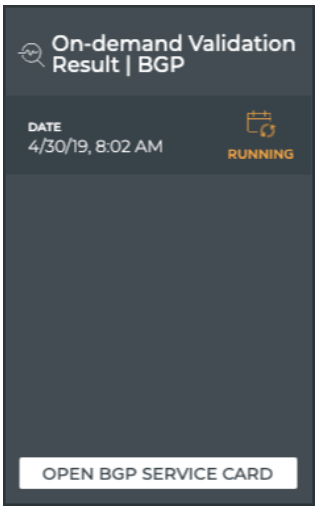
You may find that although you have a validation scheduled to run at a later time, you would like to run it now.

To run a scheduled validation now:

1. Open either the small or medium 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 (see page).

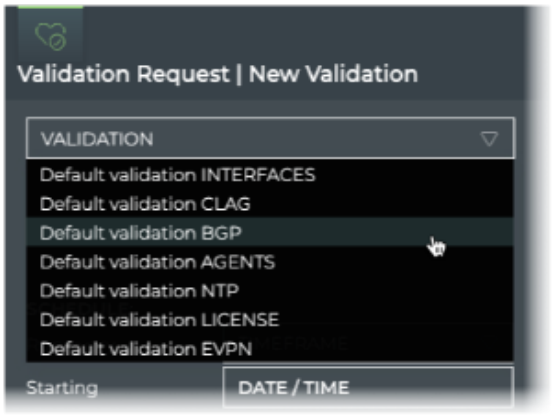


Create a New On-demand Validation Request

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:

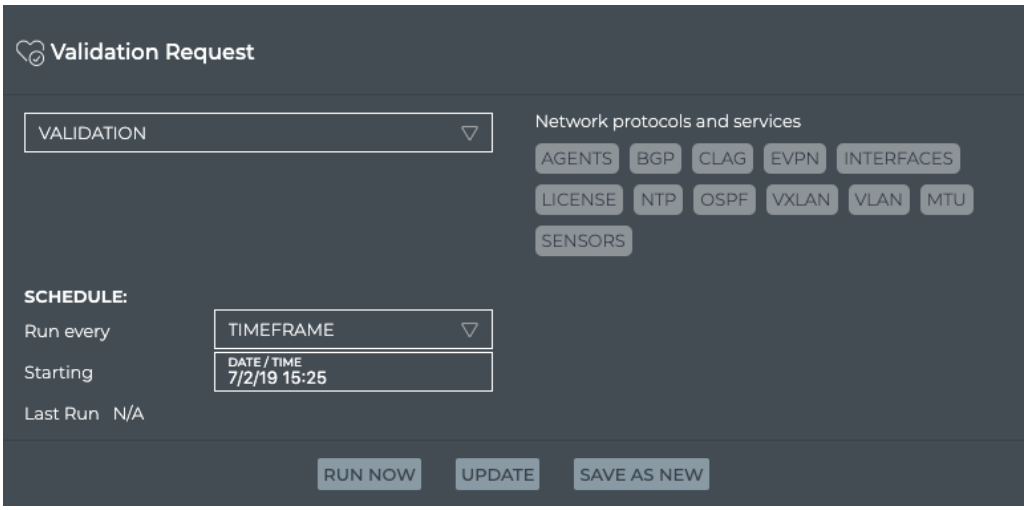
1. Open the small, medium or large Validation Request card.
2. Select the validation from the **Validation** dropdown list.



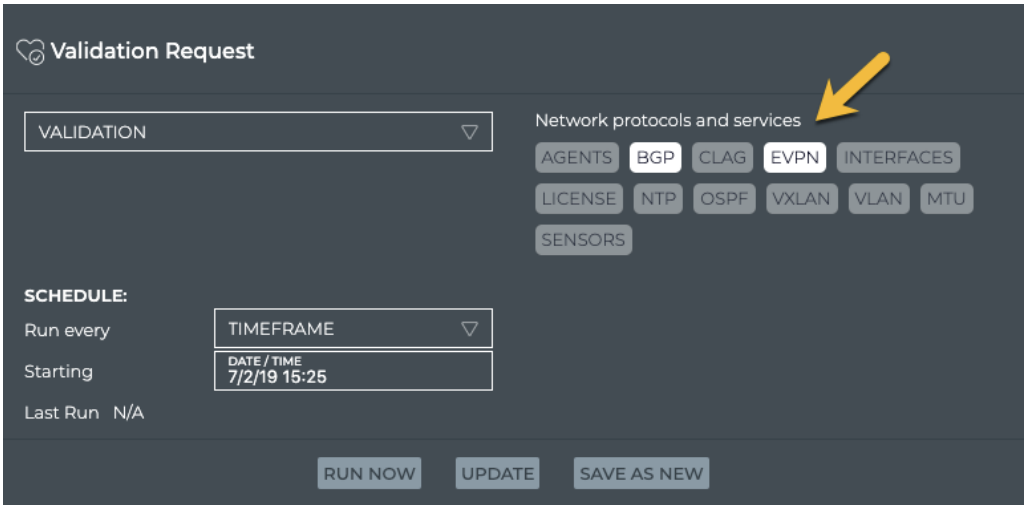
3. Click **Go** or **Run Now**.
   The associated Validation Result card is opened on your workbench. Refer to View On-demand Validation Results (see page).

To create and run a request for *more than one* protocol and/or service, essentially a custom validation request, you must first save it as a scheduled request. After which you can run it on demand.

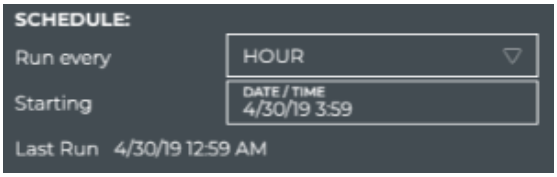
1. Open the large Validation Request card.



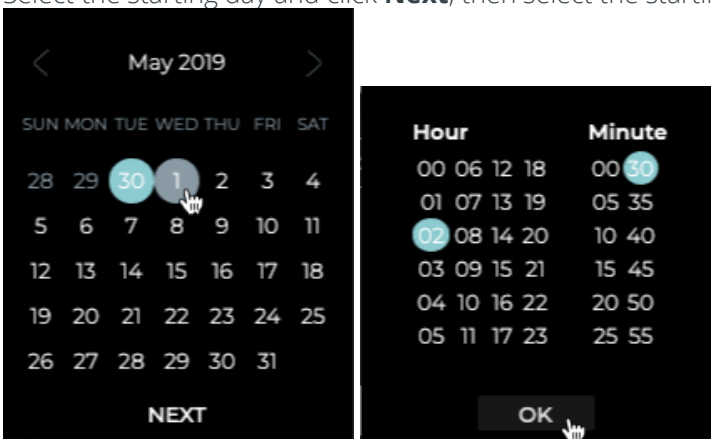
2. Click the names of the protocols and services you want to validate. We selected BGP and EVPN in this example.



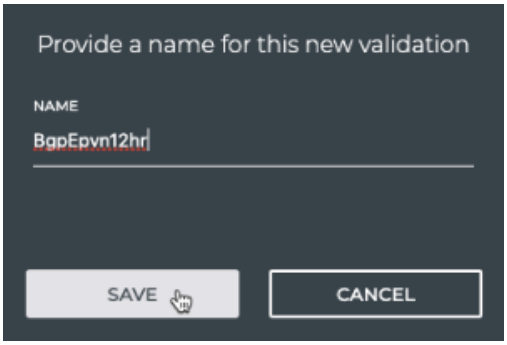
3. Enter the schedule frequency (30 min, 1 hour, 3 hours, 6 hours, 12 hours, or 1 day) by selecting it from the **Run every** field.



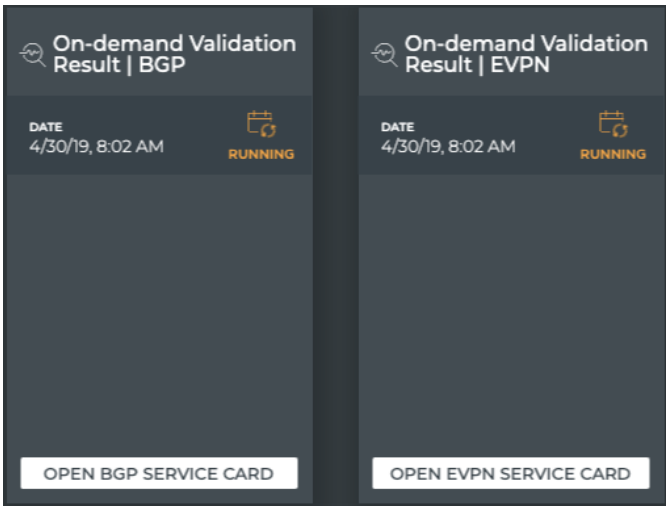
4. Select the starting day and click **Next**, then select the starting time and click **OK**.



5. Click **Save As New**.
6. Give the validation a unique name, and click **Save**.



7. Select the newly create validation from the **Validation** list.
8. 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 (see page).

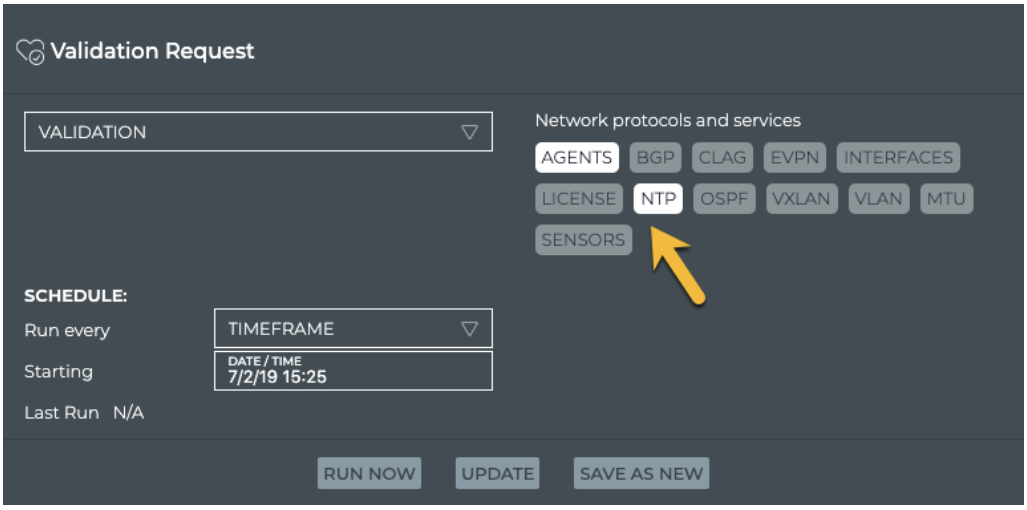


Create a New Scheduled Validation Request

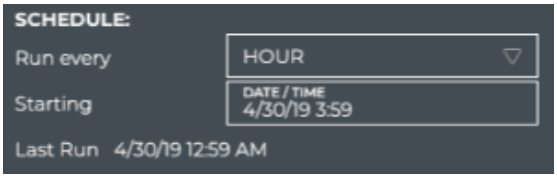
When you want to see validation results on a regular basis, it is useful to configure a scheduled validation request to avoid re-creating the request each time.

To create and run a new scheduled validation:

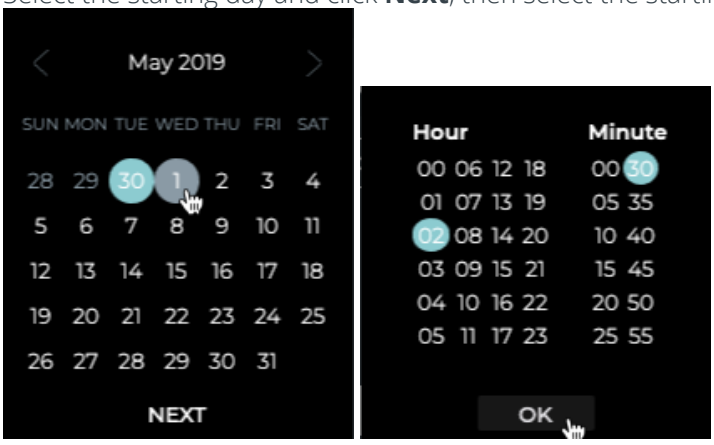
1. Open the large Validation Request card.
2. Select the protocols and/or services you want to include in the validation. In this example we have chosen the Agents and NTP services.



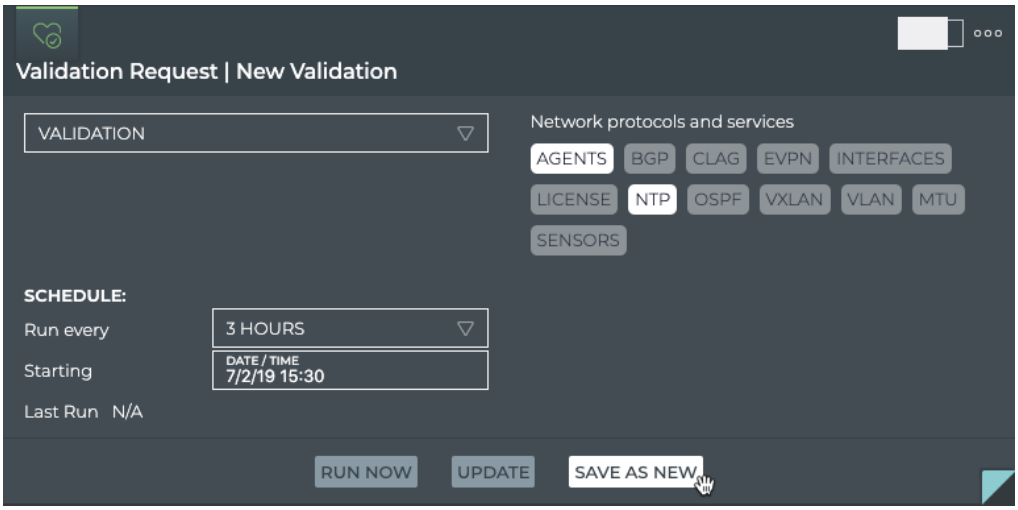
3. Enter the schedule frequency (30 min, 1 hour, 3 hours, 6 hours, 12 hours, or 1 day) by selecting it from the **Timeframe** list.



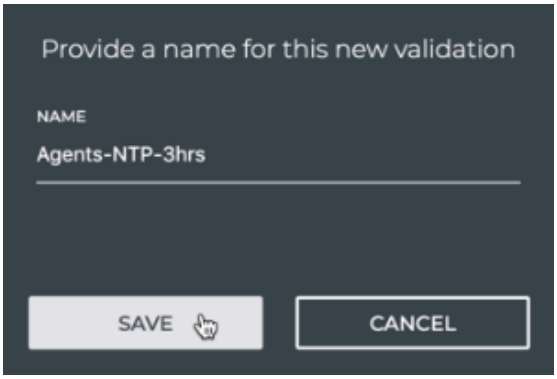
4. Select the starting day and click **Next**, then select the starting time and click **OK**.



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

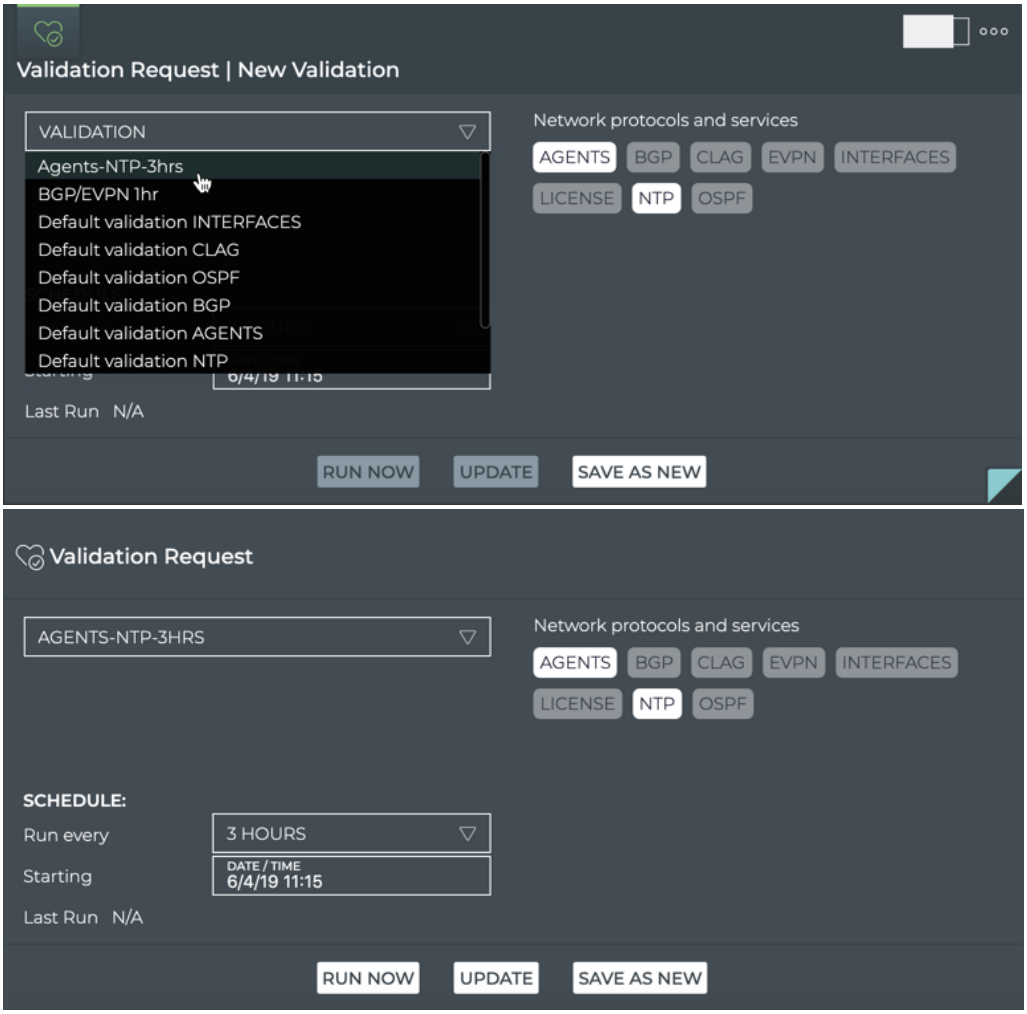


7. Enter a name for the validation.



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 (see page).



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.

> 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**.

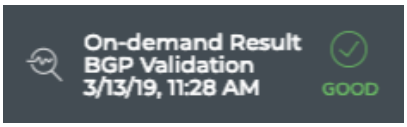
The validation can now be selected from the Validation listing (on the small, medium or large size card) and run immediately using **Run Now**, or you can wait for it to run the first time according to the schedule you specified. Refer to View Scheduled Validation Results (see page).

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.

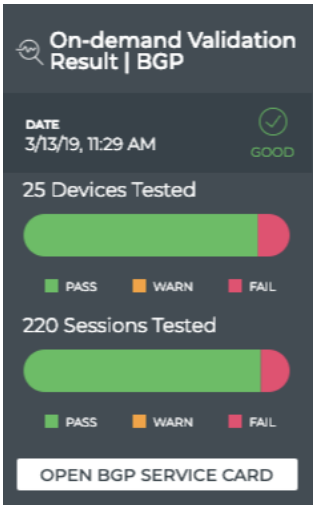
On-Demand Validation Result Card Workflow

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
,	Status of the validation job, where: • **Good**: Job ran successfully. One or more warnings may have occurred during the run. • **Failed**: Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.

The medium Validation Result card displays:



Item	Description
	Indicates an on-demand validation result
Title	On-demand Validation Result | <Network Protocol or Service Name>
Timestamp	Date and time the validation was completed
	Status of the validation job, where: • **Good**: Job ran successfully. • **Warning**: Job encountered issues, but it did complete its run. • **Failed**: Job encountered errors which prevented the job from completing.
Devices Tested	Chart with the total number of devices included in the validation and the distribution of the results. • **Pass**: Number of devices tested that had successful results • **Warn**: Number of devices tested that had successful results, but also had at least one warning event • **Fail**: Number of devices tested that had one or more protocol or service failures Hover over chart to view the number of devices and the percentage of all tested devices for each result category.
Sessions Tested	For BGP, chart with total number of BGP sessions included in the validation and the distribution of the overall results. For EVPN, chart with total number of BGP sessions included in the validation and the distribution of the overall results. For Interfaces, chart with total number of ports included in the validation and the distribution of the overall results. In each of these charts: • **Pass**: Number of sessions or ports tested that had successful results • **Warn**: Number of sessions or ports tested that had successful results, but also had at least one warning event • **Fail**: Number of sessions or ports tested that had one or more failure events 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. This chart does not apply to other Network Protocols and Services, and thus is not displayed for those cards.
Open <Network Protocol or Service Name> Service Card	Click to open the corresponding medium Network Services card, where available. Refer to Monitor Network Protocols and Services (see page 112) for details about these cards and workflows.

The large Validation Result card contains two tabs.

The *Summary* tab displays:

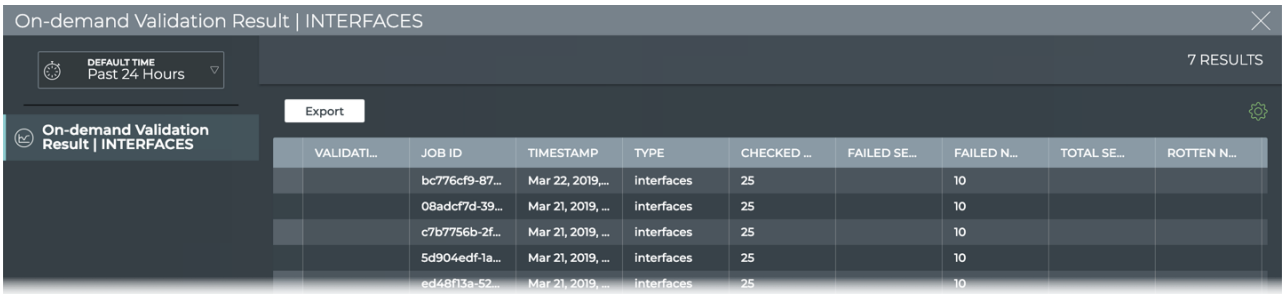
Item	Description
	Indicates an on-demand validation result
Title	On-demand Validation Result | Summary | <Network Protocol or Service Name>
Date	Day and time when the validation completed
, ,	Status of the validation job, where: • **Good**: Job ran successfully. • **Warning**: Job encountered issues, but it did complete its run. • **Failed**: Job encountered errors which prevented the job from completing.
Devices Tested	Chart with the total number of devices included in the validation and the distribution of the results. • **Pass**: Number of devices tested that had successful results • **Warn**: Number of devices tested that had successful results, but also had at least one warning event • **Fail**: Number of devices tested that had one or more protocol or service failures Hover over chart to view the number of devices and the percentage of all tested devices for each result category.
Sessions Tested	For BGP, chart with total number of BGP sessions included in the validation and the distribution of the overall results. For EVPN, chart with total number of BGP sessions included in the validation and the distribution of the overall results.

Item	Description
	For Interfaces, chart with total number of ports included in the validation and the distribution of the overall results. For OSPF, chart with total number of OSPF sessions included in the validation and the distribution of the overall results. In each of these charts: • **Pass**: Number of sessions or ports tested that had successful results • **Warn**: Number of sessions or ports tested that had successful results, but also had at least one warning event • **Fail**: Number of sessions or ports tested that had one or more failure events 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. This chart does not apply to other Network Protocols and Services, and thus is not displayed for those cards.
Open <Network Protocol or Service Name> Service Card	Click to open the corresponding medium Network Services card, when available. Refer to Monitor Network Protocols and Services (see page 112) for details about these cards and workflows.
Table/Filter options	When the **Most Active** 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. When the **Most Recent** filter option is selected, the table displays switches and hosts running the given service or protocol sorted by **timestamp**, with the device with the most recent warning or failure listed first. The table provides the following additional information: • **Hostname**: User-defined name for switch or host • **Message Type**: Network protocol or service which triggered the event • **Message**: Short description of the event • **Severity**: Indication of importance of event; values in decreasing severity include critical, warning, error, info, debug
Show All Devices	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.



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>	Displays all unscheduled validation results. By default, the results list is sorted by **Timestamp**. This tab provides the following additional data about each result: • **Validation Label**: Does not apply to on-demand validation results and can be ignored • **Job ID**: Internal identifier of the validation job that produced the given results • **Timestamp**: Date and time the validation completed • **Type**: Network protocol or service type • **Total Node Count**: Total number of nodes running the given network protocol or service • **Checked Node Count**: Number of nodes on which the validation ran • **Failed Node Count**: Number of checked nodes that had protocol or service failures • **Rotten Node Count**: Number of nodes that could not be reached during the validation • **Unknown Node Count**: Applies only to the Interfaces service. Number of nodes with unknown port states. • **Total Session Count**: Total number of sessions running for the given network protocol or service • **Failed Session Count**: Number of sessions that had session failures
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

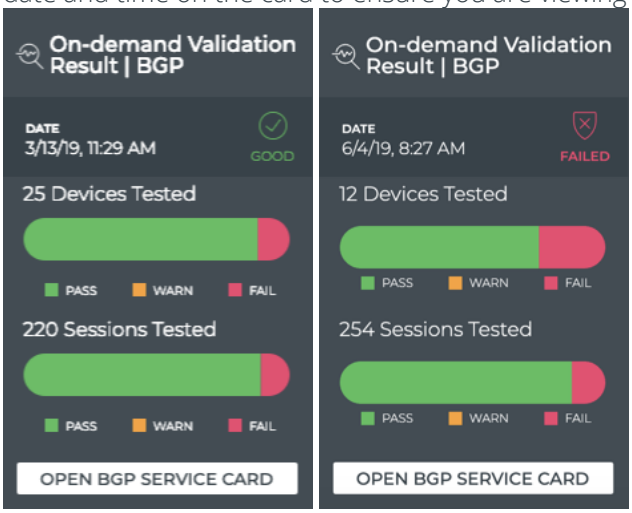
Once an on-demand validation request has completed, the results are available in the corresponding Validation Result card.

> 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.

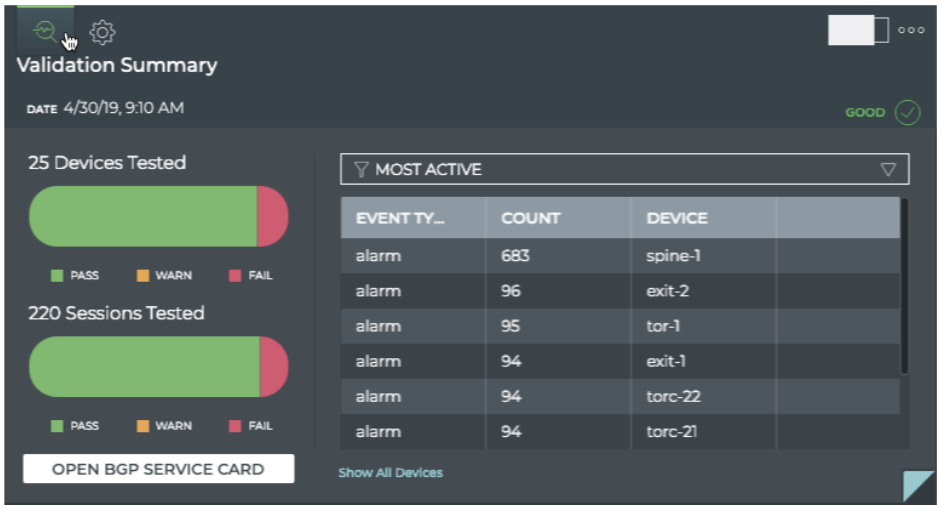
To view the results:

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.

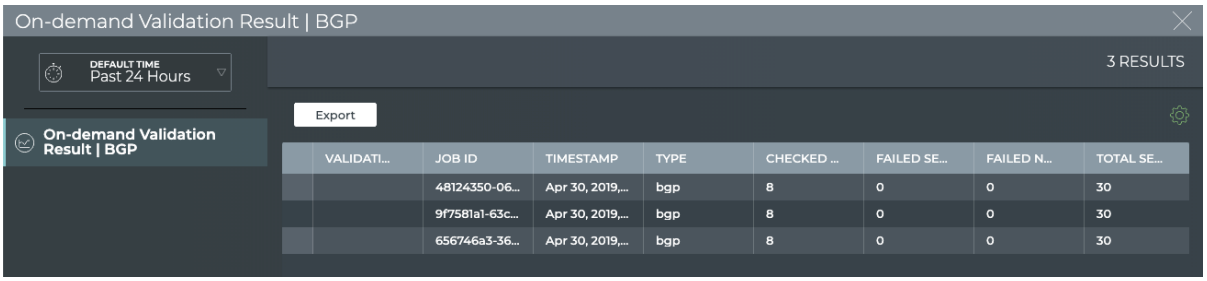
Note: You may have more than one card open for a given protocol or service, so be sure to use the date and time on the card to ensure you are viewing the correct card.



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

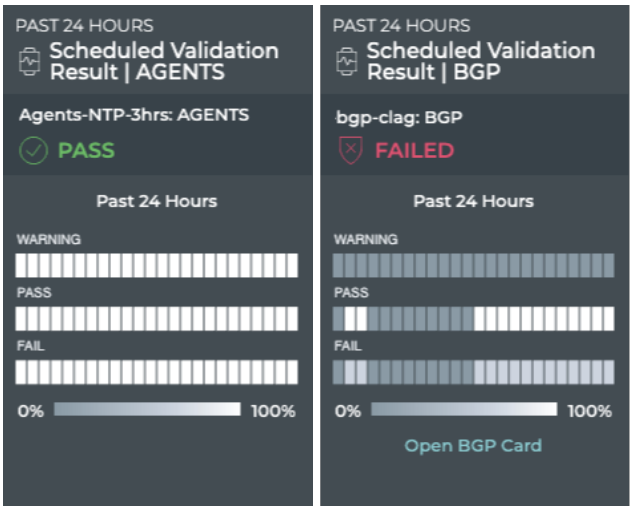
The Scheduled Validation Result card workflow enables you to view the results of scheduled validation requests. When a request has completed processing, you can access the Validation Result card from the full screen Validation Request card. Each protocol and service has its own validation result card, 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	Summary of validation results: • Number of validation runs completed in the designated time period • Number of runs with warnings • Number of runs with errors
,	Status of the validation job, where: • **Pass**: Job ran successfully. One or more warnings may have occurred during the run. • **Failed**: Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.

The medium Validation Result card displays:



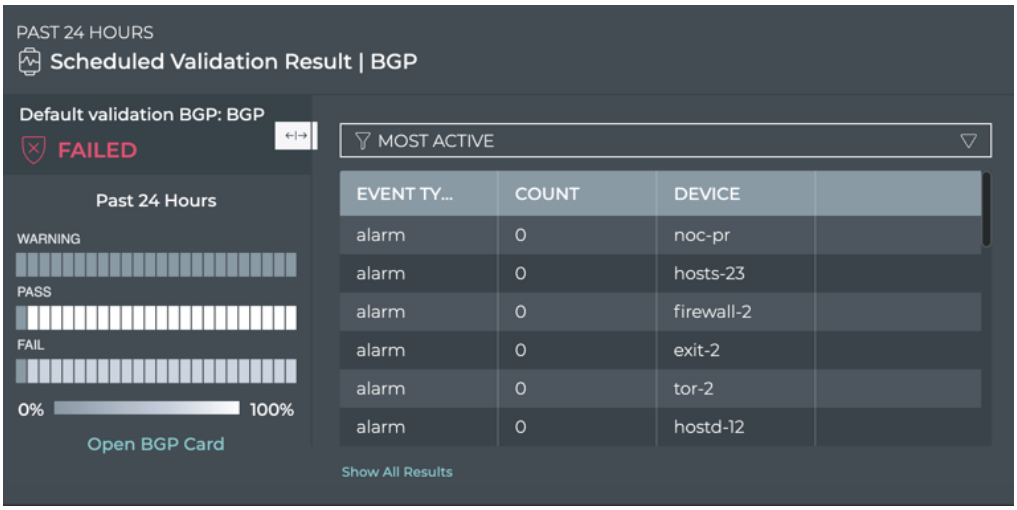
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates a scheduled validation result
Title	Scheduled Validation Result | <Network Protocol or Service Name>

Summary	Summary of validation results:
	• Name of scheduled validation
	• Status of the validation job, where:
	  • **Pass**: Job ran successfully. One or more warnings may have occurred during the run.
	  • **Failed**: Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.

Chart	Validation results, where: • **Time period:** Range of time in which the data on the heat map was collected • **Heat map: A time segmented view of the results**. For each time segment, the color represents the percentage of warning, passing, and failed results. Refer to Granularity of Data Shown Based on Time Period (see page) for details on how to interpret the results.
Open <Network Protocol or Service Name> Service Card	Click to open the corresponding medium Network Services card, when available. Refer to Monitor Network Protocols and Services (see page 112) for details about these cards and workflows.

The large Validation Result card contains two tabs.

- The *Summary* tab displays:

- 

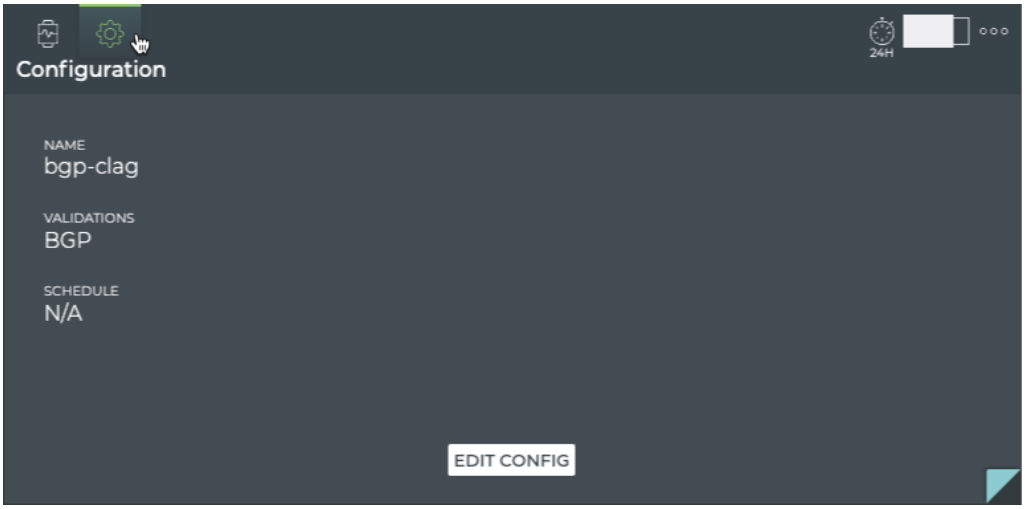
Item	Description
	Indicates a scheduled validation result
Title	Validation Summary (Scheduled Validation Result | <Network Protocol or Service Name>)

Summary	Summary of validation results:
	• Name of scheduled validation
	• Status of the validation job, where:
	  • **Pass**: Job ran successfully. One or more warnings may have occurred during the run.
	  • **Failed**: Job encountered errors which prevented the job from completing, or job ran successfully, but errors occurred during the run.
	• ←|→ : Expand the heat map to full width of card, collapse the heat map to the left

Chart	Validation results, where: • **Time period:** Range of time in which the data on the heat map was collected • **Heat map: A time segmented view of the results**. For each time segment, the color represents the percentage of warning, passing, and failed results. Refer to Granularity of Data Shown Based on Time Period (see page) for details on how to interpret the results.
Open <Network Protocol or Service Name> Service Card	Click to open the corresponding medium Network Services card, when available. Refer to Monitor Network Protocols and Services (see page 112) for details about these cards and workflows.
Table/Filter options	

Item	Description
	When the **Most Active** 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. When the **Most Recent** filter option is selected, the table displays switches and hosts running the given service or protocol sorted by **timestamp**, with the device with the most recent warning or failure listed first. The table provides the following additional information: • **Hostname**: User-defined name for switch or host • **Message Type**: Network protocol or service which triggered the event • **Message**: Short description of the event • **Severity**: Indication of importance of event; values in decreasing severity include critical, warning, error, info, debug
Show All Results	Click to open the full screen card with all scheduled validation results sorted by timestamp.

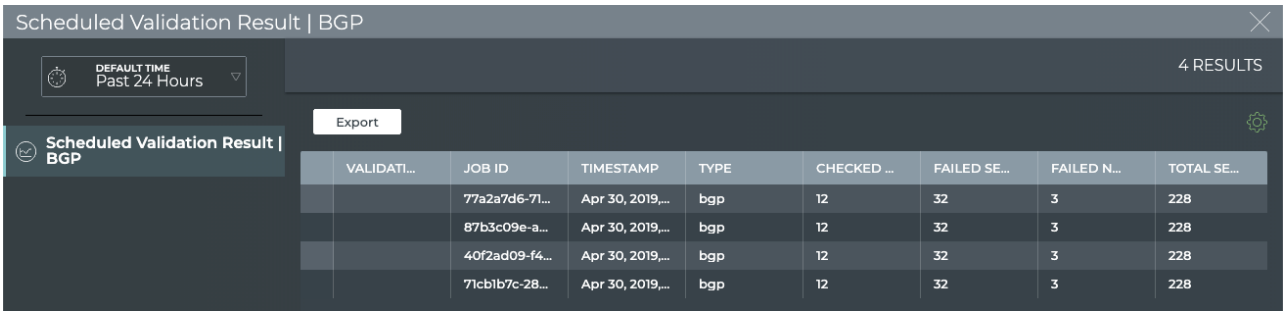
The *Configuration* tab displays:



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
Edit Config	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.

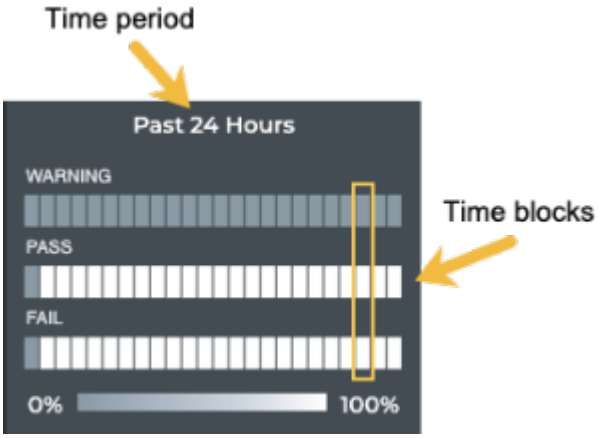


Item	Description
Title	Scheduled Validation Results | <Network Protocol or Service>
✕	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab
Scheduled Validation Result | <network protocol or service>	Displays all unscheduled validation results. By default, the results list is sorted by timestamp. This tab provides the following additional data about each result: • **Validation Label**: Does not apply to on-demand validation results and can be ignored • **Job ID**: Internal identifier of the validation job that produced the given results • **Timestamp**: Date and time the validation completed • **Type:** Protocol of Service Name • **Total Node Count**: Total number of nodes running the given network protocol or service • **Checked Node Count**: Number of nodes on which the validation ran • **Failed Node Count**: Number of checked nodes that had protocol or service failures • **Rotten Node Count**: Number of nodes that could not be reached during the validation • **Unknown Node Count**: Applies only to the Interfaces service. Number of nodes with unknown port states.

Item	Description
	• **Total Session Count**: Total number of sessions running for the given network protocol or service • **Failed Session Count**: Number of sessions that had session failures
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

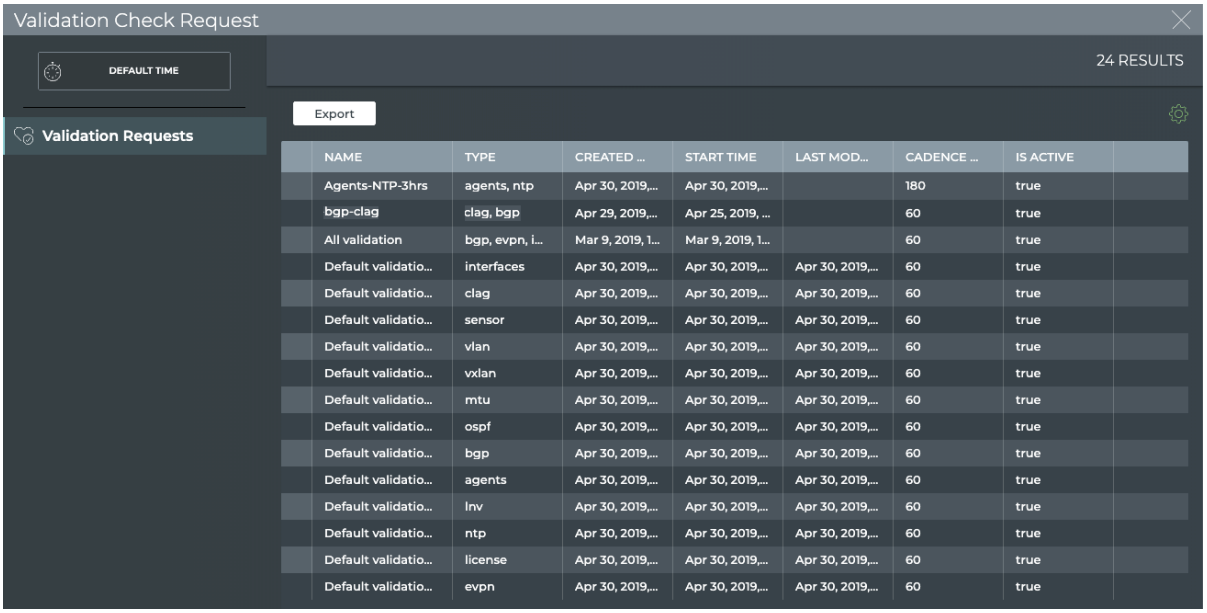
Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
1 quarter	7,000	13	1 week

View Scheduled Validation Results

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

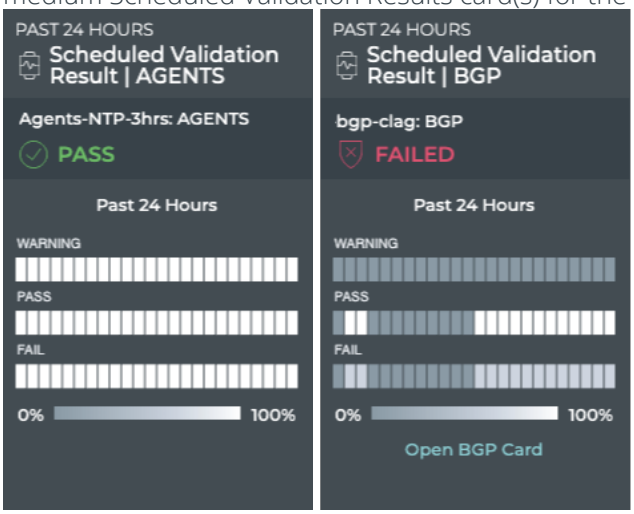
To view the results:

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

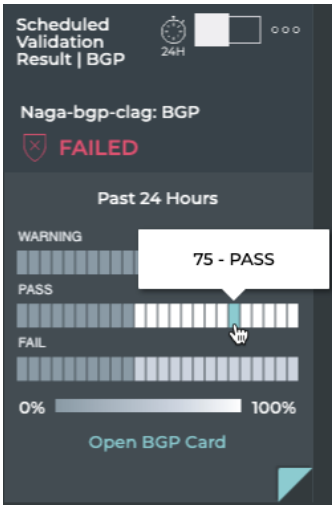


2. Select the validation results you want to view by clicking in the first column of the result and clicking the check box.

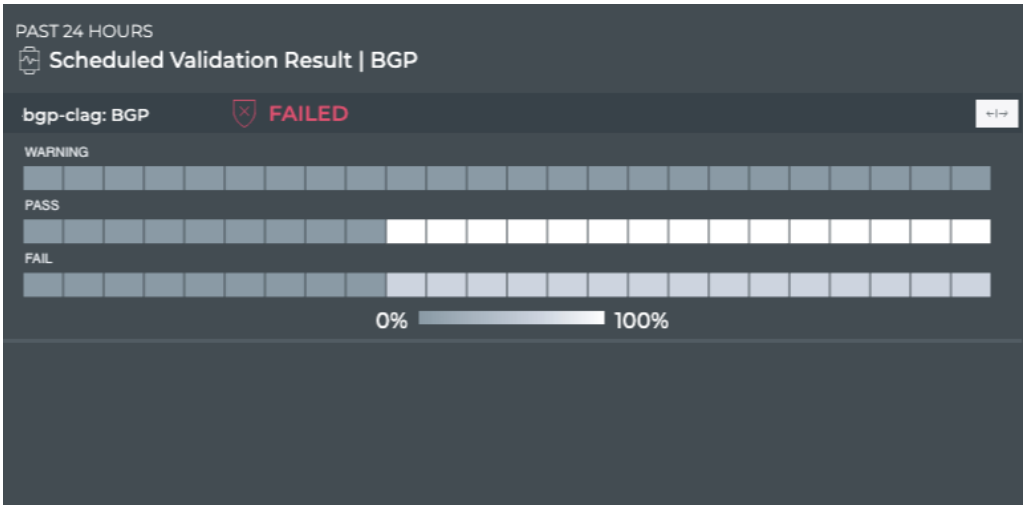
3. On the Edit Menu that appears at the bottom of the window, click (Open Cards). This opens the medium Scheduled Validation Results card(s) for the selected items.



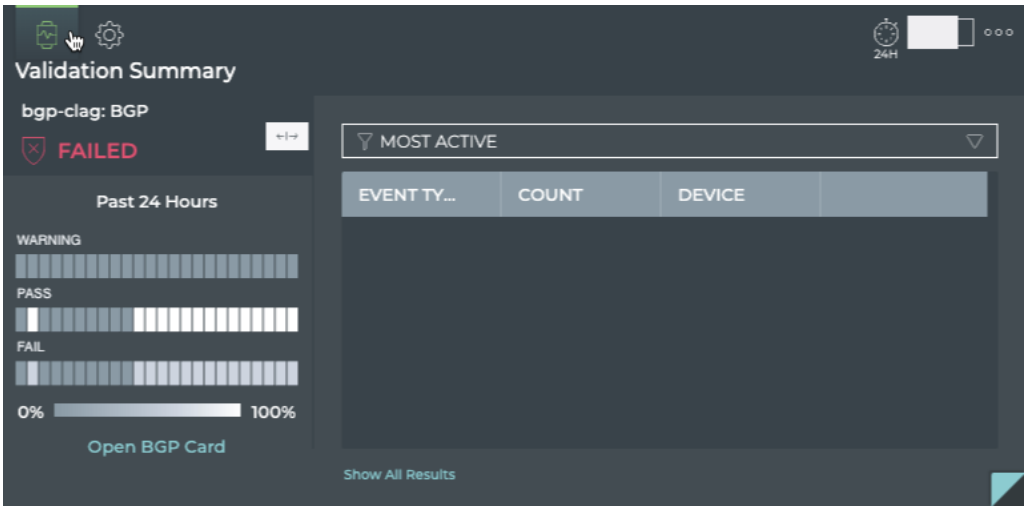
4. Note the distribution of results. Are there many failures? Are they concentrated together in time? Has the protocol or service recovered after the failures?
5. Hover over the heat maps to view the status numbers and what percentage of the total results that represents for a given region. The tooltip 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.



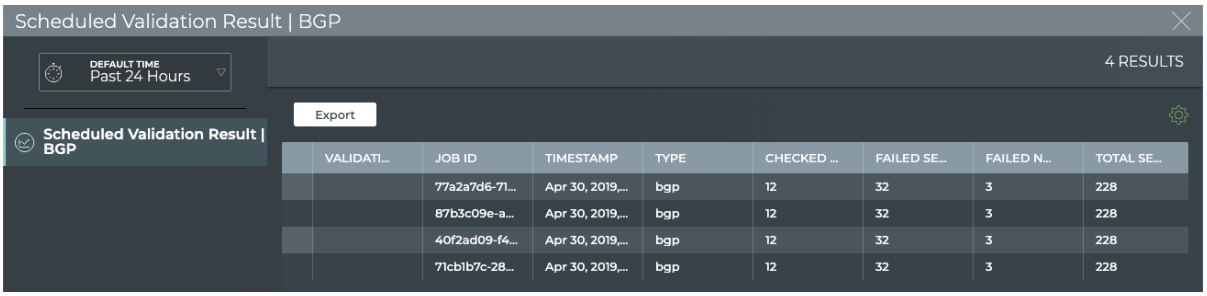
6. Optionally, click **Open**<*network service*>**Card** to open the medium individual Network Services card. Your current card is not closed.
7. Switch to the large Scheduled Validation card.
8. Click ↤↦ to expand the chart.



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 (see page) 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.



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?

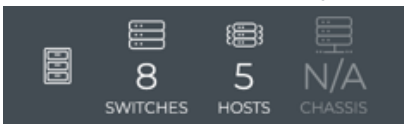
For monitoring inventory and performance on a switch-by-switch basis, refer to the Monitor Switches (see page 258) topic .

Contents

This topic describes how to...

Devices Inventory Card Workflow Summary

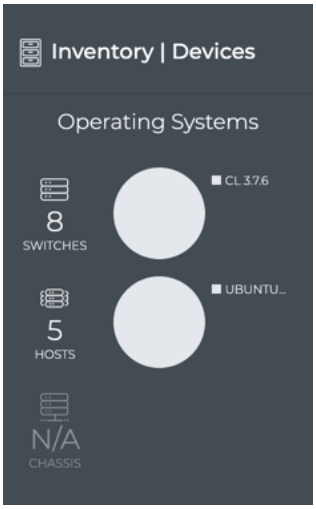
The small Devices Inventory card displays:



Item	Description
	Indicates data is for device inventory
	Total number of switches in inventory during the designated time period

Item	Description
	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
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
	Total number of chassis in inventory during the designated time period. Not monitored in this release.
Charts	Distribution of operating systems deployed on switches and hosts, respectively

The large Devices Inventory card has one tab.

The *Switches* tab displays:

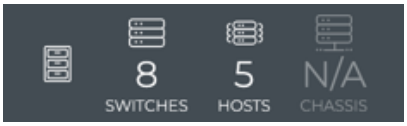
Item	Description
Time period	Always Now for inventory by default
	Indicates data is for device inventory
Title	Inventory | Devices
	Total number of switches in inventory during the designated time period
	Link to full screen listing of all switches
Component	Switch components monitored–ASIC, Operating 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.

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, o pen the small Devices Inventory card.

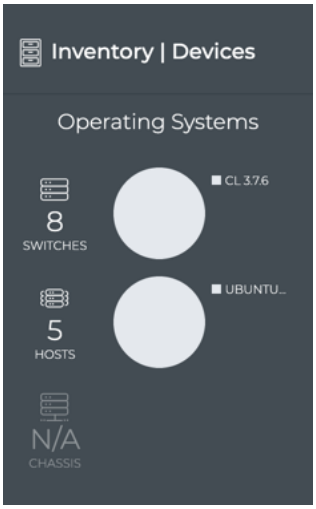


Chassis are not monitored in this release, so an N/A (not applicable) value is displayed for these devices, even if you have chassis in your network.

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.



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.

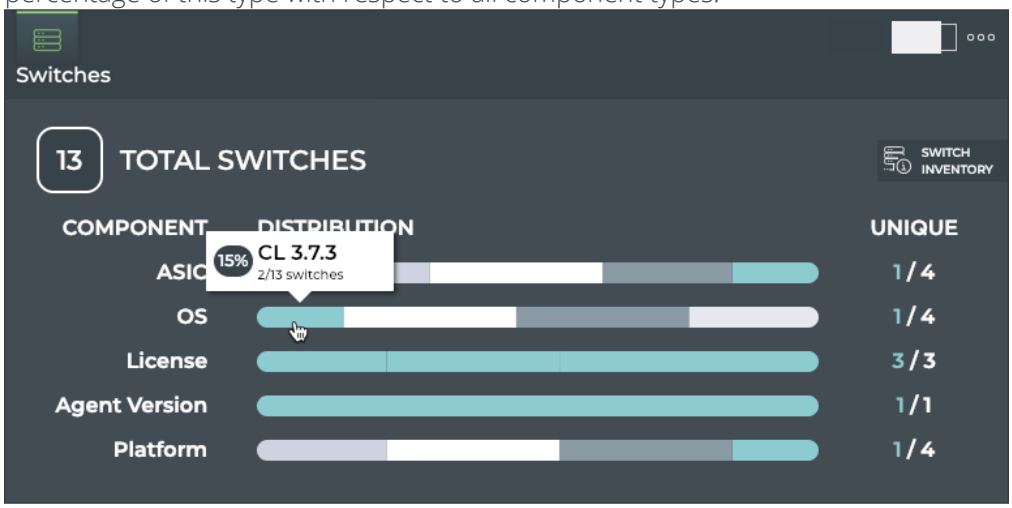
View Switch Components

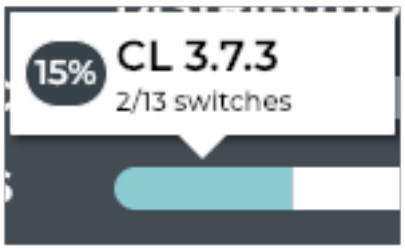
To view switch components, open the large Devices Inventory card. By default the Switches tab is shown displaying the total number of switches, ASIC vendor, OS versions, license status, NetQ Agent versions, and specific platforms deployed on all of your switches.

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.





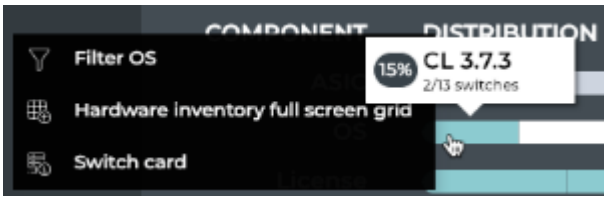
Additionally, sympathetic highlighting is used to show the related component types relevant to the highlighted segment and the number of unique component types associated with this type (shown in blue here).

Focus on a Selected Component Type

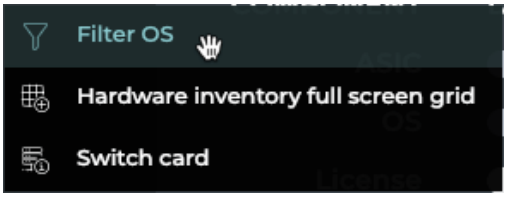
To dig deeper on a particular component type, you can filter the card data by that type. In this procedure, the result of filtering on the OS is shown.

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.

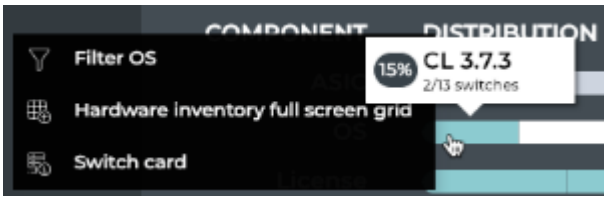
4. To return to the full complement of components, click the ✕ in the filter tag.

Navigate to Related Cards

The large Switches card provides quick links to full-screen cards in the Device Inventory workflow.

To navigate to a related card:

1. Click the component name or a segment of a component on the distribution chart.
2. Select the desired card from the dropdown list.

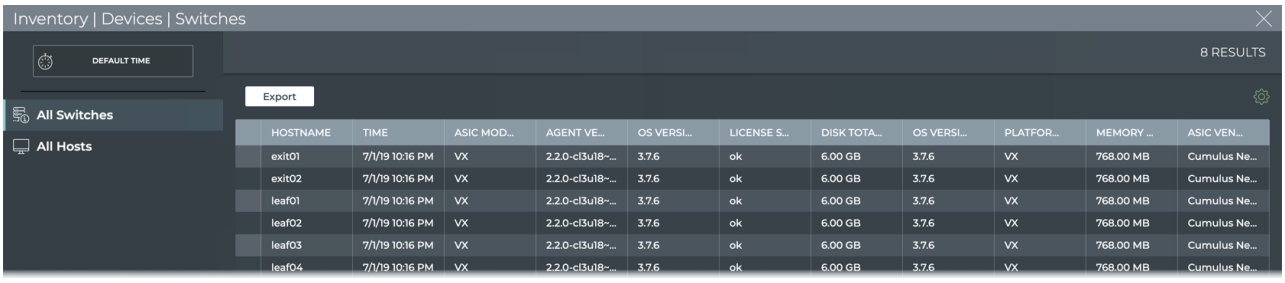


Navigate to the Switch Inventory Workflow

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.



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.

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 (see page 258) .

Contents

This topic describes how to...

Monitor Alarms

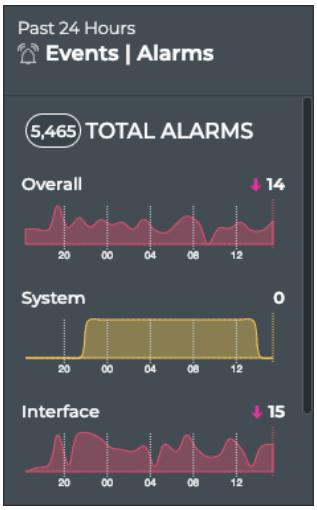
You can easily monitor critical events occurring across your network using the Alarms card. You can determine the number of events for the various system, interface, and network protocols and services components in the network. The content of the cards in the workflow is described first, and then followed 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
Alarm trend	Trend of alarm count, represented by an arrow: • **Pointing upward and bright pink**: alarm count is higher than the last two time periods, an increasing trend • **Pointing downward and green**: alarm count is lower than the last two time periods, a decreasing trend • **No arrow**: alarm count is unchanged over the last two time periods, trend is steady
Alarm score	Current count of alarms during the designated time period
Alarm rating	Count of alarms relative to the average count of alarms during the designated time period: • **Low**: Count of alarms is below the average count; a nominal count • **Med**: Count of alarms is in range of the average count; some room for improvement • **High**: Count of alarms is above the average count; user intervention recommended ***Performance rating*** **Low** **Med** **High** ***Alarm count*** **Minimum** **Average** **Maximum**
Chart	Distribution of all alarms received during the designated time period

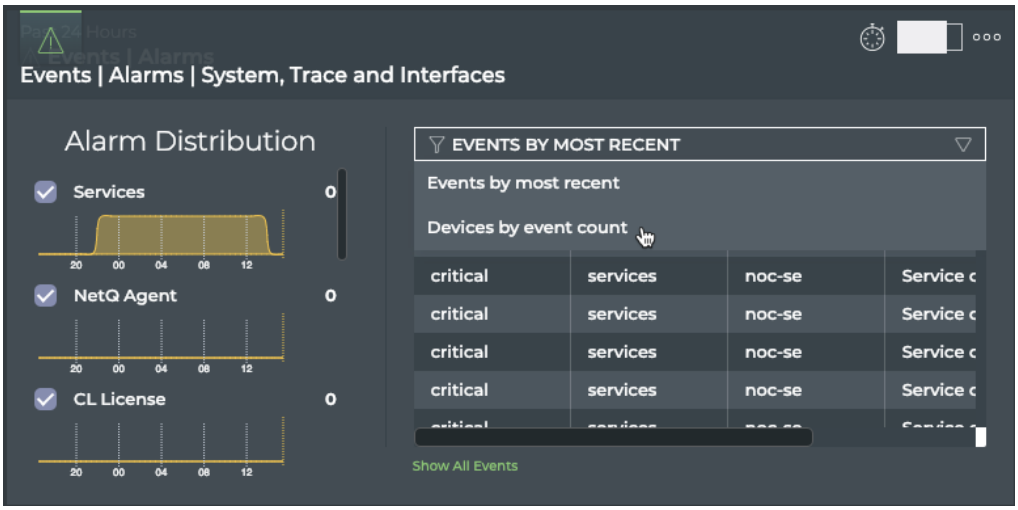
The medium Alarms card displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
🔔	Indicates data is for all 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: • **Pointing upward and bright pink**: alarm count is higher than the last two time periods, an increasing trend • **Pointing downward and green**: alarm count is lower than the last two time periods, a decreasing trend • **No arrow**: alarm count is unchanged over the last two time periods, trend is steady
Alarm score	Current count of alarms received from each category (overall, system, interface, and network services) during the designated time period
Chart	Distribution of all alarms received from each category during the designated time period

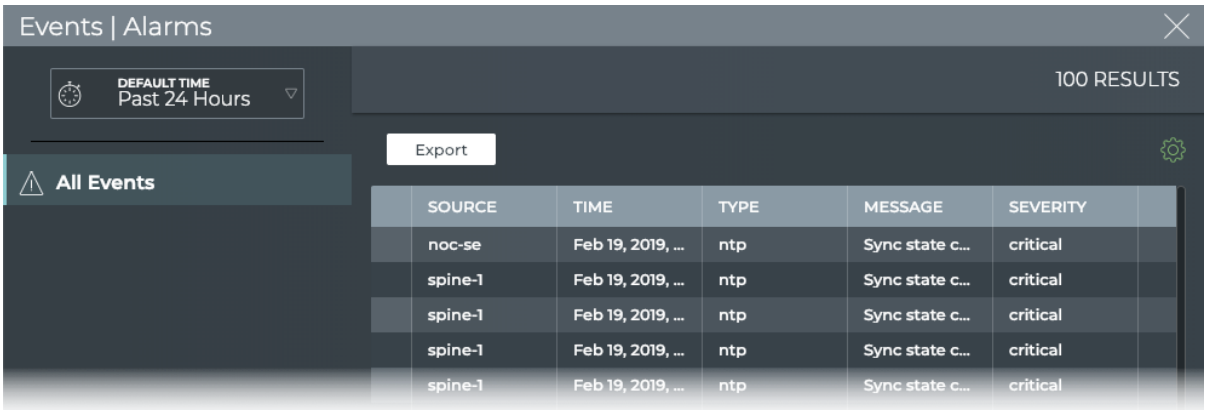
The large Alarms card has one tab.

The *System, Trace and Interfaces* 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
Alarm Distribution	Chart: Distribution of all alarms received from each category (services, NetQ Agents, Cumulus Linux licenses, sensors, ports, links, MTU, LLDP and configuration changes) during the designated time period Count: Total number of alarms received from each category during the designated time period
Table	Listing of items that match the filter selection for the selected alarm categories: • **Events by Most Recent**: Most recent event are listed at the top • **Devices by Event Count**: Devices with the most events are listed at the top
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.

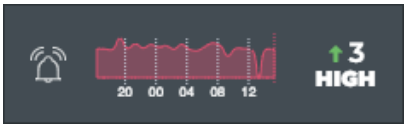


Item	Description
Title	Events | Alarms
✕	Closes full screen card and returns to workbench
Default Time	Range of time in which the displayed data was collected
Results	Number of results found for the selected tab
All Events	Displays all events (both alarms and info) received in the time period. By default, the requests list is sorted by the date and time that the event occurred (**Time**). This tab provides the following additional data about each request: • **Source**: Hostname of the given event • **Type**: Name of network protocol and/or service that triggered the given event • **Message**: Text describing the alarm or info event that occurred • **Severity**: Importance of the event–critical, warning, info, or debug
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.

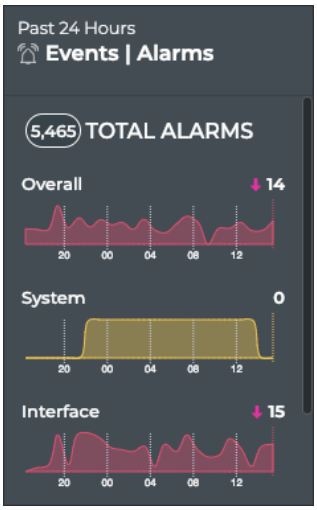


In this example, there are a small number of alarms (3), the number of alarms is increasing, and there are more alarms right now than the average number of alarms during this time period. This would indicate a need to investigate further. Note that with such a small number of alarms, the rating may be 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.



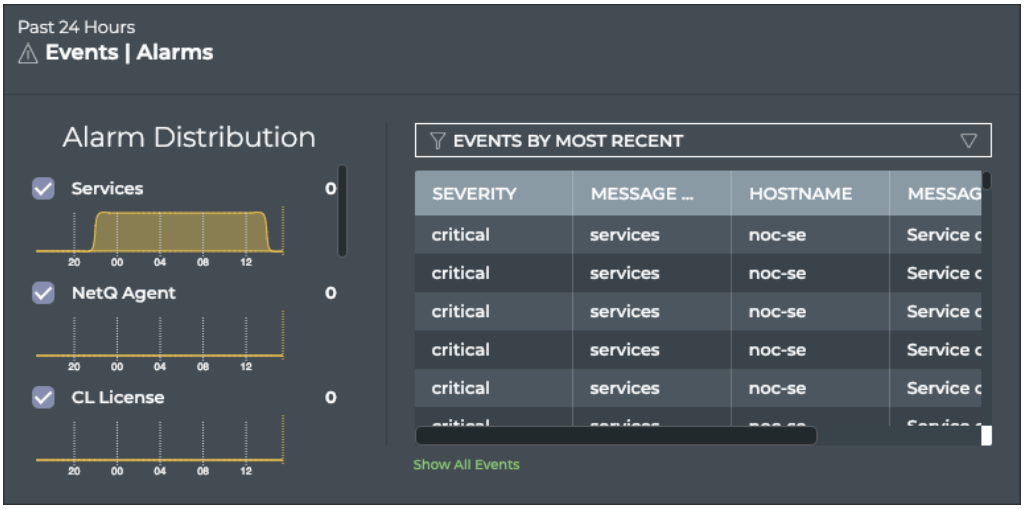
Monitor System and Interface Alarm Details

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

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.



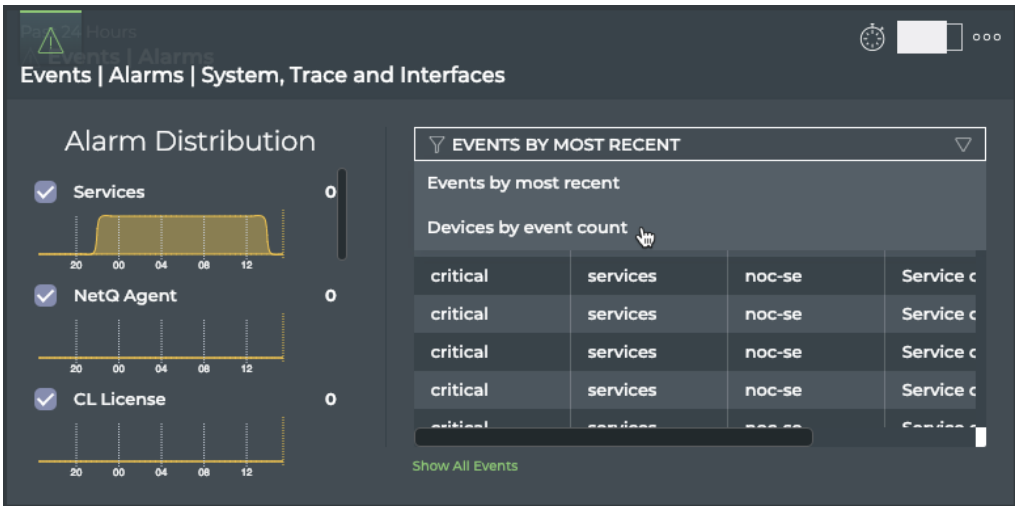
From this card, you can view the distribution of alarms for each of the categories over time. Scroll down to view any hidden charts. A list of the associated alarms is also displayed.

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.



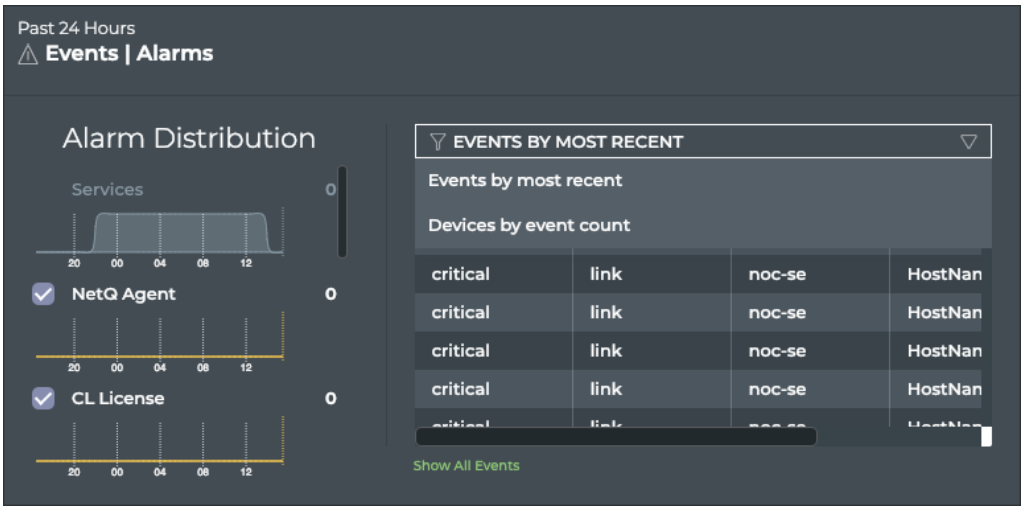
Filter Alarms by System or Interface

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 those 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.

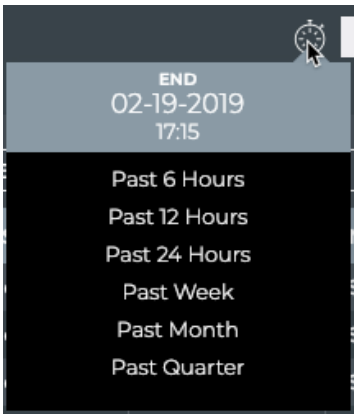


Compare Alarms with a Prior Time

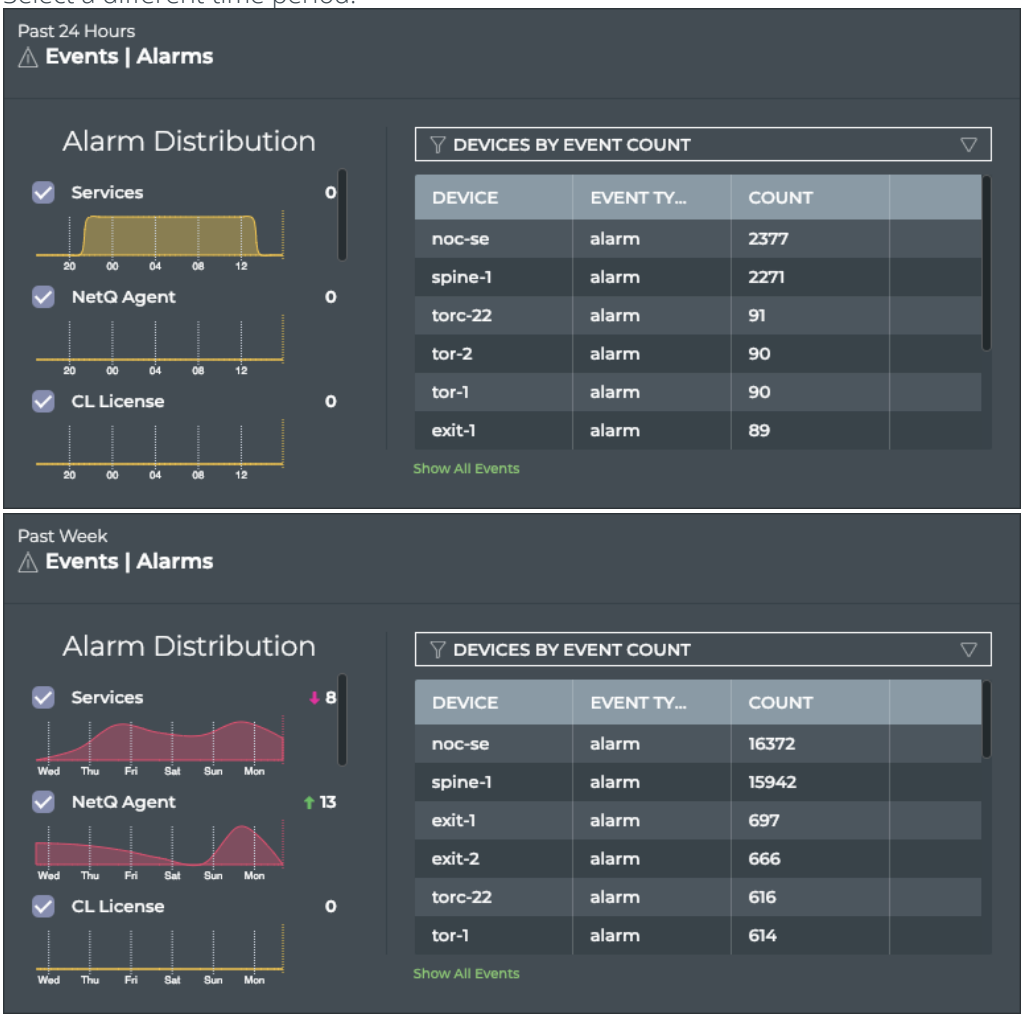
You can change the time period for the data to compare with a prior time. If the same devices are consistently indicating the most alarms, you might want to look more carefully at those devices using the Switches card workflow.

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 ⏱ .



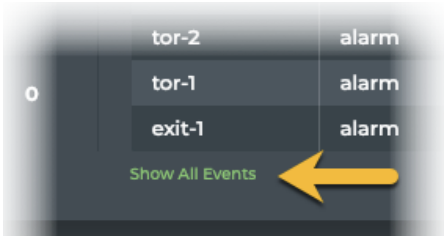
5. Select a different time period.



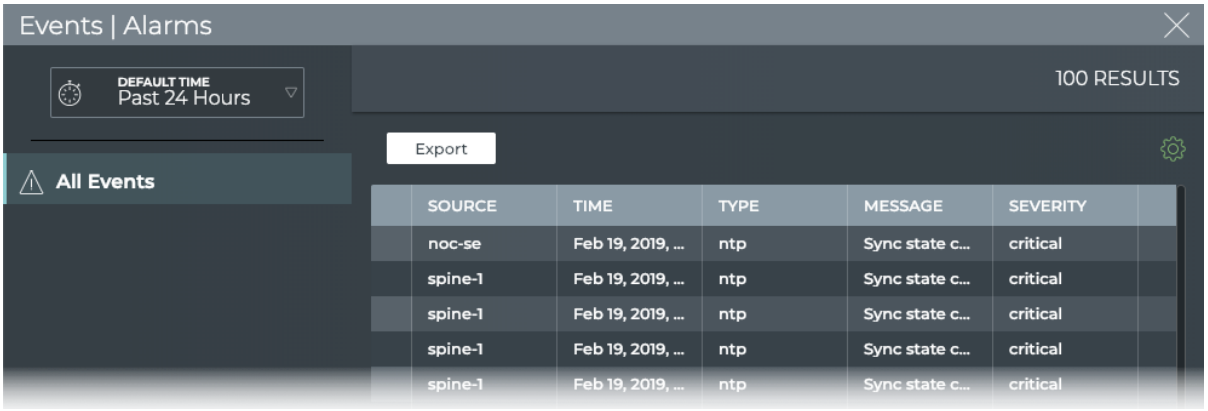
6. Compare the two cards with the **Devices by event count** filter applied.
   In this example, the total alarm count is down, but the same device has the most alarms in each time period, so it might be worth investigating this device in more detail.

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.



OR



To return to your workbench, click

in the top right corner of the card.

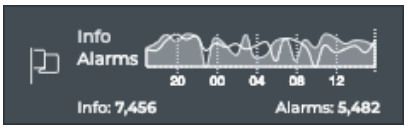
Monitor Info Events

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.

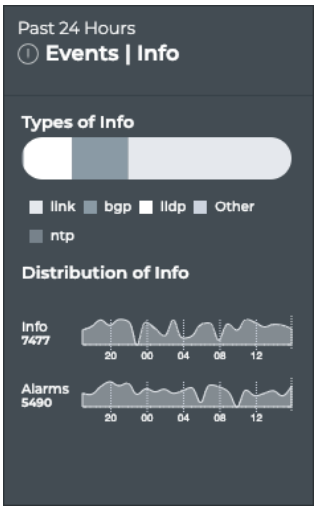
The small Info card displays:



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

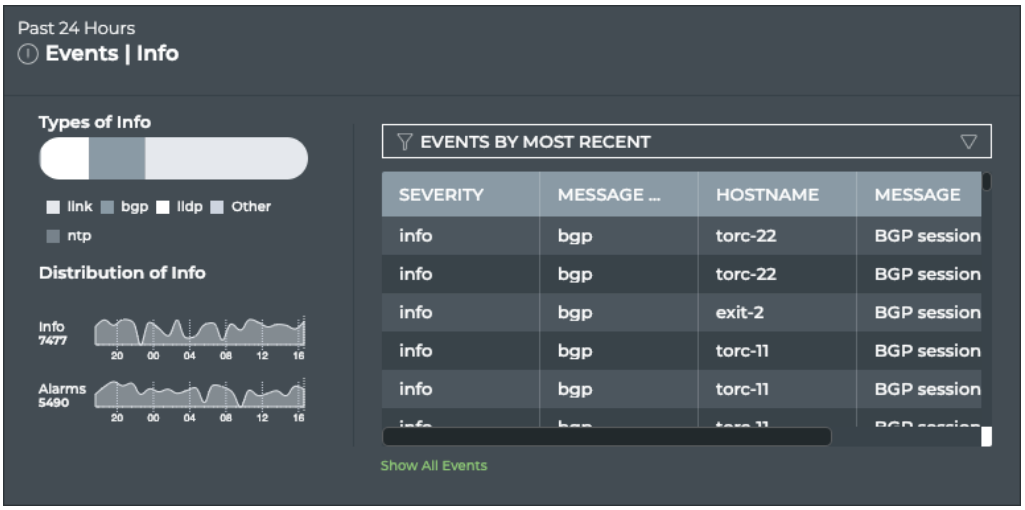
Item	Description
Chart	Distribution of all info events and alarms received during the designated time period

The medium Info card displays:



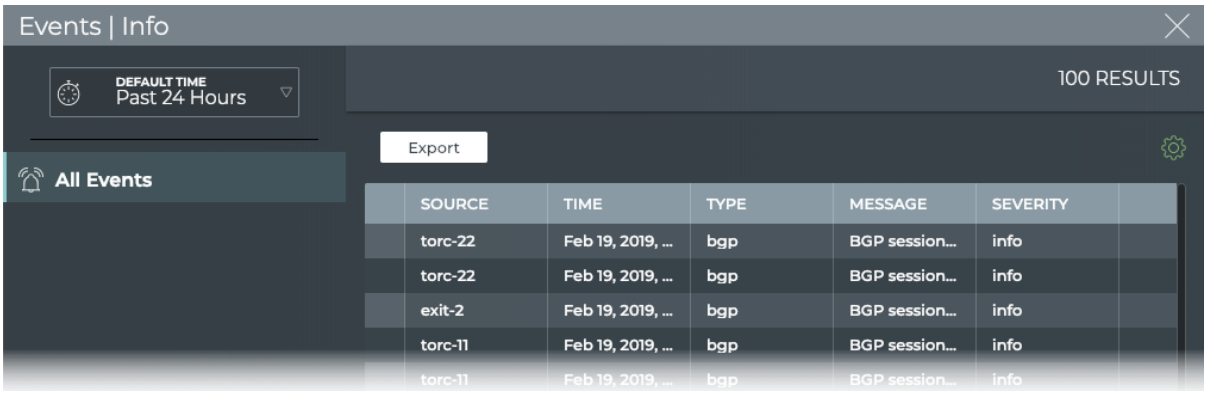
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all warning, info, and debug severity events in the network
Types of Info	Chart which displays the services that have triggered events during the designated time period. Hover over chart to view a count for each type.
Distribution of Info	Info Status • **Count**: Number of info events received during the designated time period • **Chart**: Distribution of all info events received during the designated time period Alarms Status • **Count**: Number of alarm events received during the designated time period • **Chart**: Distribution of all alarm events received during the designated time period

The large Alarms 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	Info Status • **Count**: Current number of info events received during the designated time period • **Chart**: Distribution of all info events received during the designated time period Alarms Status • **Count**: Current number of alarm events received during the designated time period • **Chart**: Distribution of all alarm events received during the designated time period
Table	Listing of items that match the filter selection: • **Events by Most Recent**: Most recent event are listed at the top • **Devices by Event Count**: Devices with the most events are listed at the top
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.

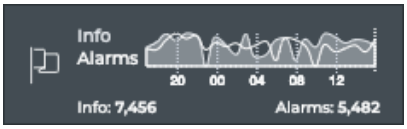


Item	Description
Title	Events | Info
✕	Closes full screen card and returns to workbench
Default Time	Range of time in which the displayed data was collected
Results	Number of results found for the selected tab
All Events	Displays all events (both alarms and info) received in the time period. By default, the requests list is sorted by the date and time that the event occurred (**Time**). This tab provides the following additional data about each request: • **Source**: Hostname of the given event • **Type**: Name of network protocol and/or service that triggered the given event • **Message**: Text describing the alarm or info event that occurred • **Severity**: Importance of the event–critical, warning, info, or debug
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

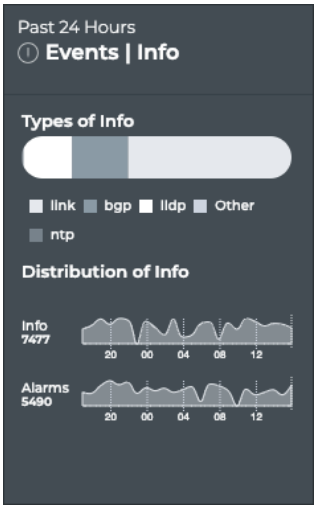
View Info Status Summary

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.

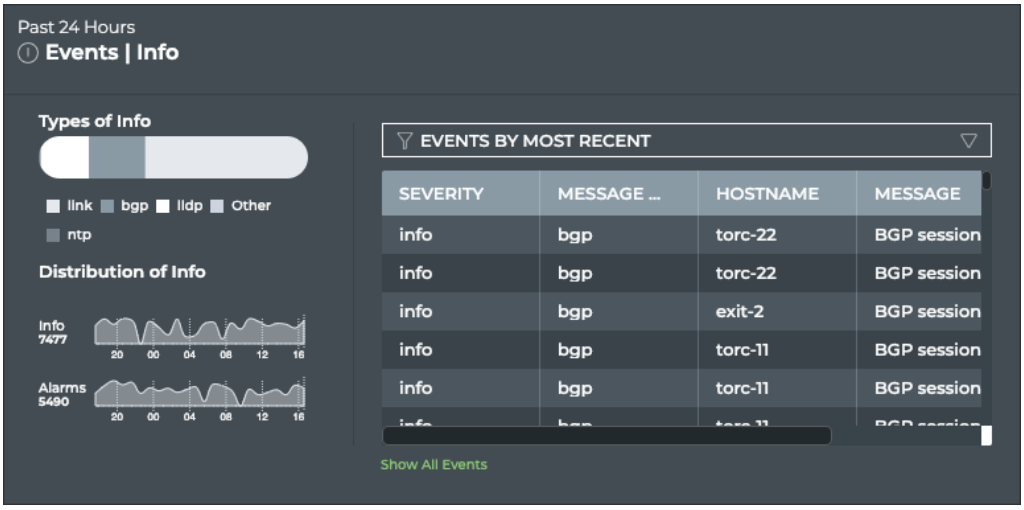
To view the summary with the *small* Info card, simply open the card. This card gives you a high-level view in a condensed visual, including the number and distribution of the info events along with the alarms that have occurred during the same time period.



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 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

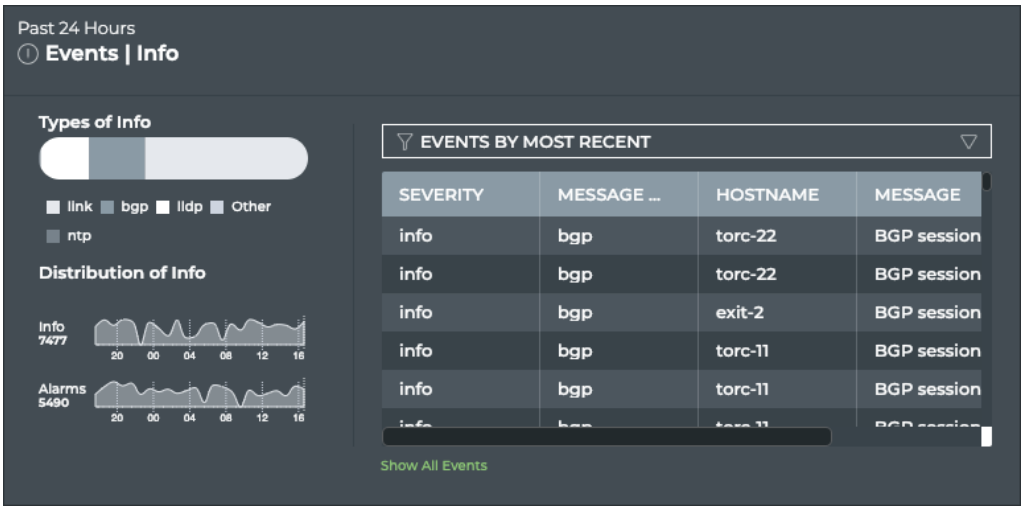
While you can see the relative relationship between info and alarm events on the small Info card, the medium and large cards provide considerably more information. Open either of these to view individual line charts for the events. Generally, alarms have some corollary info events. For example, when 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.

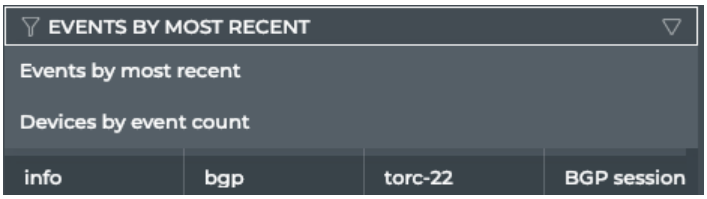
View All Info Events Sorted by Time of Occurrence

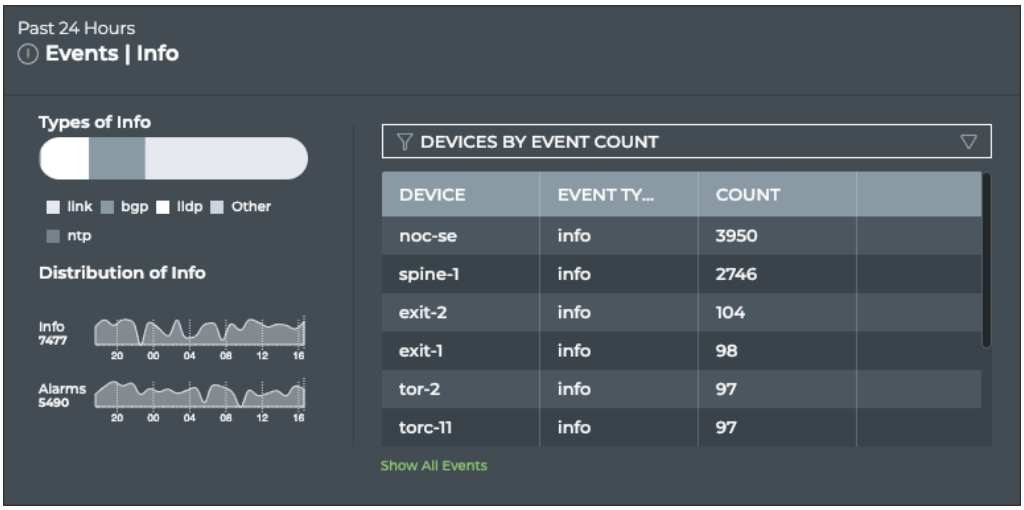
You can view all info events using the large Info card. Open the large card and confirm the **Events By Most Recent** option is selected in the filter above the table on the right. When this option is selected, all of the info events are listed with the most recently occurring event at the top. Scrolling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



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.

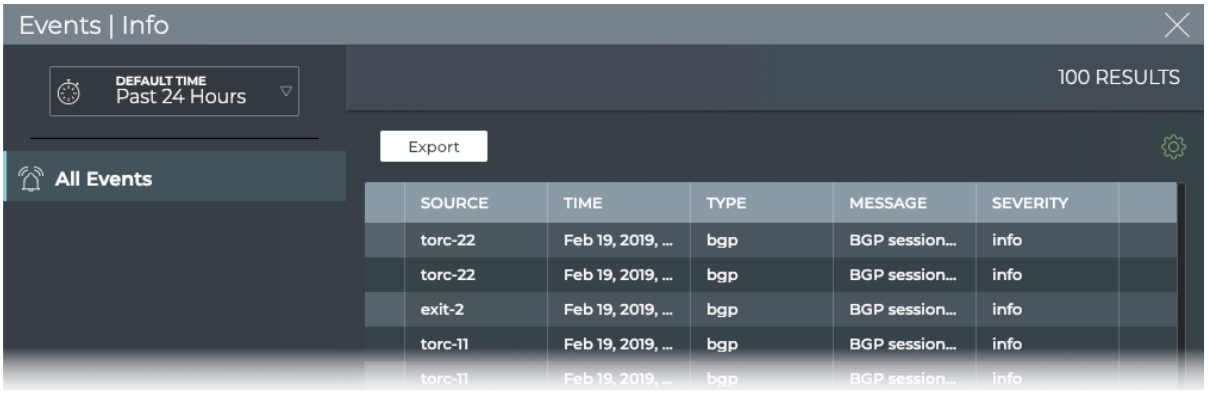




View All Events

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



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, by default. Click the column header to sort the list by that characteristic. Click in any column header to toggle the sort order between A-Z and Z-A.

The messages can be viewed through third-party notification applications. For details about configuring notifications using the NetQ CLI, refer to Integrate with Third-party Software and Hardware.

Type	Trigger	Severity	Message Format	Example
agent	NetQ Agent state changed to Rotten (not heard from in over 15 seconds)	Critical	Agent state changed to rotten	Agent state changed to rotten
bgp	BGP Session state changed	Critical	BGP session with peer @peer @neighbor vrf @vrf state changed from @old_state to @new_state	BGP session with peer leaf03 leaf04 vrf mgmt state changed from Established to Failed

Type	Trigger	Severity	Message Format	Example
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	swp2 speed 10, mismatched with peer server02 swp8 speed 40
clag	CLAG remote peer state changed from up to down	Critical	Peer state changed to down	Peer state changed to down
configdiff	Configuration file deleted on a device	Critical	@hostname config file @type was deleted	spine03 config file /etc /frr/frr.conf was deleted
evpn	A VNI was configured and moved from the up state to the down state	Critical	VNI @vni state changed from up to down	VNI 36 state changed from up to down
license	License state is missing or invalid	Critical	License check failed, name @lic_name state @state	License check failed, name agent.lic state invalid
license	License state is missing or invalid on a particular device	Critical	License check failed on @hostname	License check failed on leaf03
link	Link operational state changed from up to down	Critical	HostName @hostname changed state from @old_state to @new_state Interface:@ifname	HostName leaf01 changed state from up to down Interface:swp34
lnv	VXLAN registration daemon, vxrd, is not running	Critical	vxrd service not running	vxrd service not running
ntp	NTP sync state changed from in sync to not in sync	Critical	Sync state changed from @old_state to @new_state for @hostname	Sync state changed from in sync to not sync for leaf06
ptm	Physical interface cabling does not match configuration specified in *topology. dot* file	Critical	PTM cable status failed	PTM cable status failed
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 fan state changed from up to down

Type	Trigger	Severity	Message Format	Example
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 temp max value 110 exceeds the threshold 95
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	Sensor psu min value 10 fell below threshold 25
services	A service status changed from down to up	Critical	Service @name status changed from @old_status to @new_status	Service bgp status changed from down to up
services	A service status changed from up to down	Critical	Service @name status changed from @old_status to @new_status	Service lldp status changed from up to down
agent	NetQ Agent state changed to Fresh	Info	Agent state changed to fresh	Agent state changed to fresh
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 session with peer swp5 spine02 spine03 vrf default session state changed from Failed to Established
bgp	BGP Session state changed from down to up	Info	BGP session with peer @peer @neighbor vrf @vrf state changed from down to up	BGP session with peer leaf03 leaf04 vrf mgmt state changed from down to up
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	BGP session with peer spine03 swp9 vrf vrf2 reset time changed from 1559427694 to 1559837484
cable	The speed setting for a given port changed	Info	@ifname speed changed from @old_speed to @new_speed	swp9 speed changed from 10 to 40
cable	The transceiver status for a given port changed	Info	@ifname transceiver changed from @old_transceiver to @new_transceiver	swp4 transceiver changed from disabled to enabled
cable		Info		

Type	Trigger	Severity	Message Format	Example
	The vendor of a given transceiver changed		@ifname vendor name changed from @old_vendor_name to @new_vendor_name	swp23 vendor name changed from Broadcom to Mellanox
cable	The part number of a given transceiver changed	Info	@ifname part number changed from @old_part_number to @new_part_number	swp7 part number changed from FP1ZZ5654002A to MSN2700-CS2F0
cable	The serial number of a given transceiver changed	Info	@ifname serial number changed from @old_serial_number to @new_serial_number	swp4 serial number changed from 571254X1507020 to MT1552X12041
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	swp12 supported fec changed from supported to unsupported swp12 supported fec changed from unsupported to supported
cable	The advertised support for FEC for a given port changed	Info	@ifname supported fec changed from @old_advertised_fec to @new_advertised_fec	swp24 supported FEC changed from advertised to not advertised
cable	The FEC status for a given port changed	Info	@ifname fec changed from @old_fec to @new_fec	swp15 fec changed from disabled to enabled
clag	CLAG remote peer state changed from down to up	Info	Peer state changed to up	Peer state changed to up
clag	Local CLAG host state changed from down to up	Info	Clag state changed from down to up	Clag state changed from down to up
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 conflicted bond changed from swp7 swp8 to @swp9 swp10
clag	CLAG bond changed state from protodown to up state	Info		Clag conflicted bond changed from protodown to up

Type	Trigger	Severity	Message Format	Example
			Clag conflicted bond changed from @old_state_protodownbond to @new_state_protodownbond	
configdiff	Configuration file has been modified	Info	@hostname config file @type was modified	spine03 config file /etc /frr/frr.conf was modified
configdiff	Configuration file has been created	Info	@hostname config file @type was created	leaf12 config file /etc /lldp.d/README.conf was created
evpn	A VNI was configured and moved from the down state to the up state	Info	VNI @vni state changed from down to up	VNI 36 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	VNI 3 kernel state changed from down to up
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	VNI 11 vni state changed from false to true
link	Link operational state changed from down to up	Info	HostName @hostname changed state from @old_state to @new_state Interface:@ifname	HostName leaf04 changed state from down to up Interface: swp11
lldp	Local LLDP host has new neighbor information	Info	LLDP Session with host @hostname and @ifname modified fields @changed_fields	LLDP Session with host leaf02 swp6 modified fields leaf06 swp21
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 Session with host spine01 and swp5 swp12 changed to port12
lldp	Local LLDP host has new peer hostname	Info		LLDP Session with host leaf03 and swp2 leaf07 changed to exit01

Type	Trigger	Severity	Message Format	Example
			LLDP Session with host @hostname and @ifname @old_peer_hostname changed to @new_peer_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	Sync state changed from not sync to in sync for leaf06
ptm	Physical interface cabling matches configuration specified in *topology.dot* file	Critical	PTM cable status passed	PTM cable status passed
sensor	A temperature, fan, or power supply sensor state changed	Info	Sensor @sensor state changed from @old_state to @new_state	Sensor temperature state changed from critical to ok Sensor fan state changed from absent to ok Sensor psu state changed from bad to ok
sensor	A fan or power supply sensor state changed	Info	Sensor @sensor state changed from @old_s_state to @new_s_state	Sensor fan state changed from down to up Sensor psu state changed from down to up
services	A service changed state from inactive to active	Info	Service @name changed state from inactive to active	Service bgp changed state from inactive to active Service lldp changed state from inactive to active

Monitor Network Protocols and Services

The Network Services card workflows provide a network-wide view into the routing, link, and virtual network protocols installed in your network. In this release, you can monitor the network-wide behavior (all sessions) of the BGP, EVPN, MLAG, and LLDP services. Each protocol has its own card workflow containing:

- a small card with an overall status,

- a medium card displaying key attributes of the protocol,
- a large card with detailed performance statistics, some with additional tabs, and
- full screen cards displaying attributes of all associated switches, sessions, alarms or other relevant data.

Refer to NetQ User Interface Overview (see page 8) for information about navigating the card workflows and performing common actions.

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.

Contents

This topic describes how to...

Monitor the BGP Service (All Sessions)

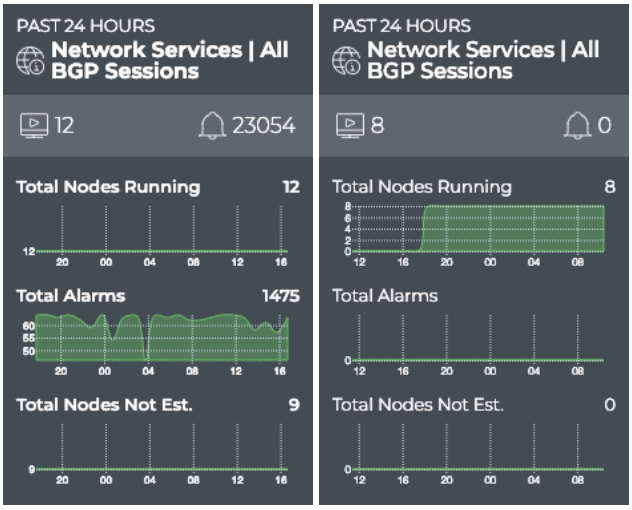
With NetQ, you can monitor the number of nodes running the BGP service, view switches with the most established and unestablished BGP sessions, and view alarms triggered by the BGP service. For an overview and how to configure BGP to run in your data center network, refer to Border Gateway Protocol - 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
	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 BGP-related alarms received during the designated time period

The medium BGP Service card displays:

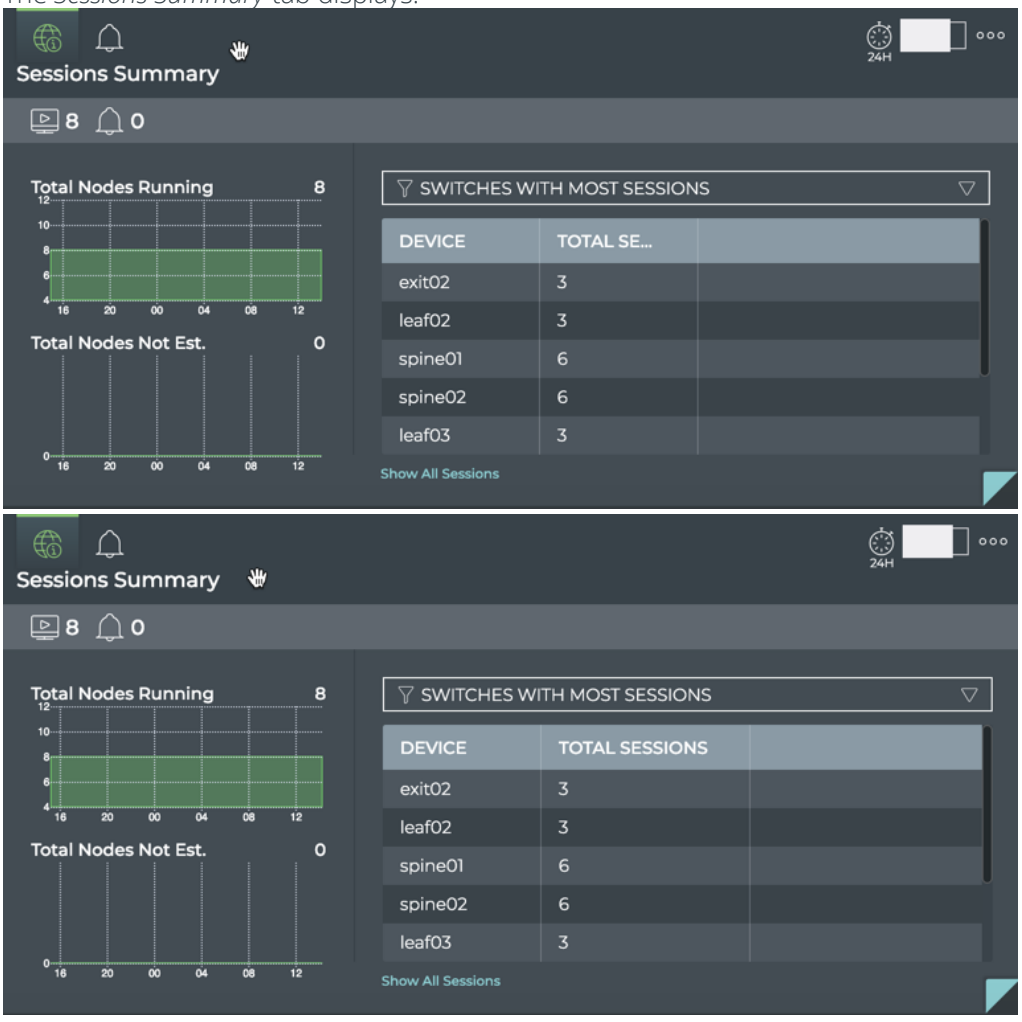


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	Network Services | All BGP Sessions
	Total number of switches and hosts with the BGP service enabled during the designated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

Item	Description
Total Nodes Running chart	Total number and distribution of switches and hosts with the BGP service enabled during the designated time period
Total Alarms chart	Total number and distribution of BGP-related alarms received during the designated time period
Total Nodes Not Est. chart	Total number and distribution of switches and hosts with unestablished BGP sessions during the designated time period

The large BGP service card contains two tabs.

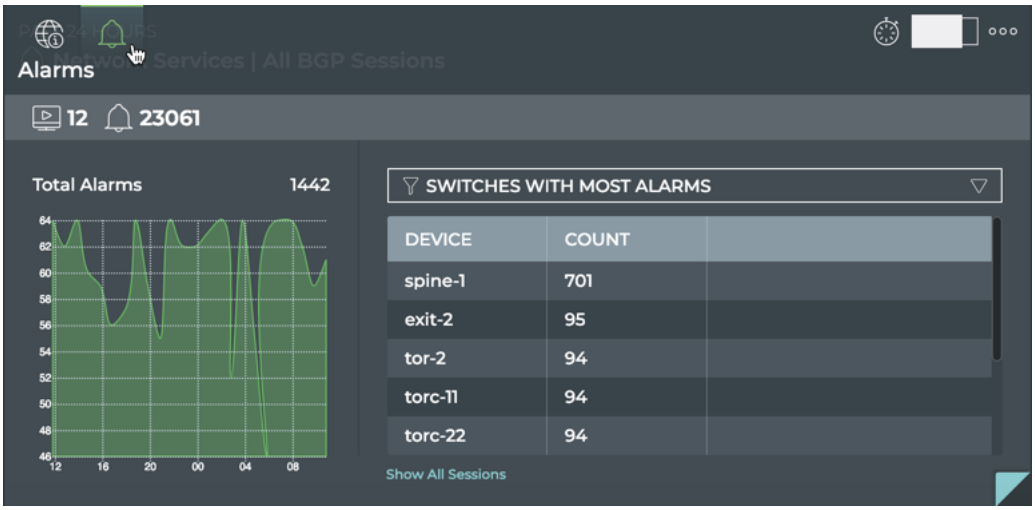
The *Sessions Summary* tab displays:



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)
	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	Total number and distribution of switches and hosts with the BGP service enabled
Total Nodes Not Est. chart	Total number and distribution of switches and hosts with unestablished BGP sessions during the designated time period
Table /Filter options	When the **Switches with Most Sessions** 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 When the **Switches with Most Unestablished Sessions** 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
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
	Indicates data is 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 BGP service enabled during the designated time period
	Total number of BGP-related alarms received during the designated time period
Total Alarms chart	Total number and distribution of BGP-related alarms received during the designated time period
Table /Filter options	When the selected filter option is **Switches with Most Alarms**, 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.

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	Displays all switches and hosts running the BGP service. By default, the device list is sorted by **hostname**. This tab provides the following additional data about each device:
	• **Agent**
	  • State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).
	  • 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.
	• **ASIC**
	  • Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.
	  • Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.
	  • Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.
	  • Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.
	  • Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.
	• **CPU**
	  • Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.
	  • Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.
	  • Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.
	  • Nos: Number of cores. Example values include 2, 4, and 8.
	• **Disk Total Size**: Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.
	• **License State**: Indicator of validity. Values include ok and bad.
	• **Memory Size**: Total amount of local RAM. Example values include 8192 MB and 2048 MB.
	• **OS**
	  • Vendor: Operating System manufacturer. Values include Cumulus Networks, RedHat, Ubuntu, and CentOS.
	  • Version: Software version number of the OS. Example values include 3.7.3, 2.5.x, 16.04, 7.1.
	  • Version Id: Identifier of the OS version. For Cumulus, this is the same as the *Version* (3.7.x).

Item	Description

	• **Platform**
	  • Date: Date and time the platform was manufactured. Example values include 7 /12/18 and 10/29/2015.
	  • MAC: System MAC address. Example value: 17:01:AB:EE:C3:F5.
	  • Model: Manufacturer's model name. Examples values include AS7712-32X and S4048-ON.
	  • Number: Manufacturer part number. Examples values include FP3ZZ7632014A, 0J09D3.
	  • Revision: Release version of the platform
	  • Series: Manufacturer serial number. Example values include D2060B2F044919GD000060, CN046MRJCES0085E0004.
	  • Vendor: Manufacturer of the platform. Example values include Cumulus Express, Dell, EdgeCore, Lenovo, Mellanox.
	• **Time:** Date and time the data was collected from device.

All Sessions tab	Displays all BGP sessions network-wide. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session:
	• **ASN**: Autonomous System Number, identifier for a collection of IP networks and routers. Example values include 633284,655435.
	• **Conn Dropped**: Number of dropped connections for a given session
	• **Conn Estd**: Number of connections established for a given session
	• **DB State**: Session state of DB
	• **Evpn Pfx Rcvd**: Address prefix received for EVPN traffic. Examples include 115, 35.
	• **Ipv4, and Ipv6 Pfx Rcvd**: Address prefix received for IPv4 or IPv6 traffic. Examples include 31, 14, 12.
	• **Last Reset Time**: Date and time at which the session was last established or reset
	• **Objid**: Object identifier for service
	• **OPID**: Customer identifier. This is always zero.
	• **Peer**
	  • ASN: Autonomous System Number for peer device
	  • Hostname: User-defined name for peer device
	  • Name: Interface name or hostname of peer device
	  • Router Id: IP address of router with access to the peer device
	• **Reason**: Text describing the cause of, or trigger for, an event
	• **Rx and Tx Families**: Address families supported for the receive and transmit session channels. Values include ipv4, ipv6, and evpn.
	• **State**: Current state of the session. Values include Established and NotEstd (not established).
	• **Timestamp**: Date and time session was started, deleted, updated or marked dead (device is down)

Item	Description
	• **Upd8 Rx:** Count of protocol messages received • **Upd8 Tx**: Count of protocol messages transmitted • **Up Time**: Number of seconds the session has been established, in EPOCH notation. Example: 1550147910000 • **Vrf**: Name of the Virtual Route Forwarding interface. Examples: default, mgmt, DataVrf1081 • **Vrfid**: Integer identifier of the VRF interface when used. Examples: 14, 25, 37
All Alarms tab	Displays all BGP 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: • **Message**: Text description of a BGP-related event. Example: BGP session with peer tor-1 swp7 vrf default state changed from failed to Established • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *bgp* in this card workflow.
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.

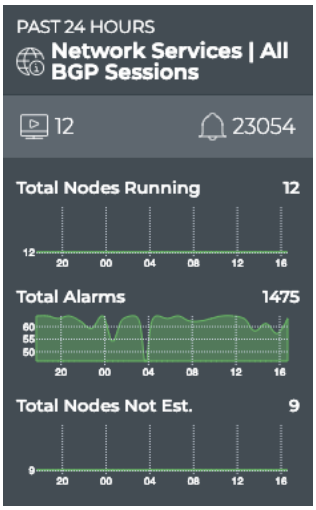
To view the summary, open the small BGP Service card.

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

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.



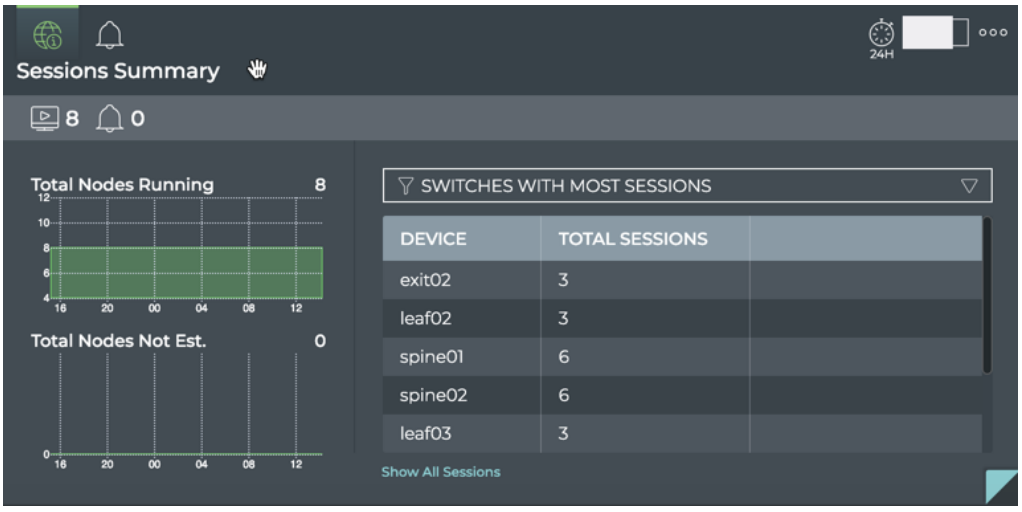
If a visual correlation is apparent, you can dig a little deeper with the large BGP Service card tabs.

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.

To view switches and hosts with the most BGP sessions:

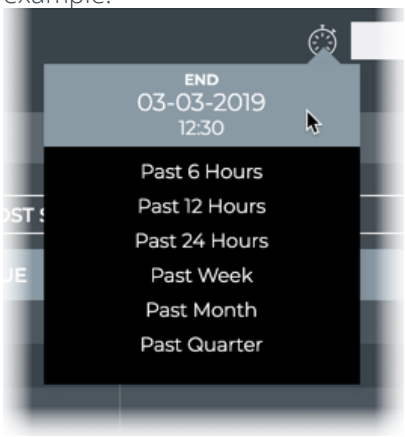
1. Open the large BGP Service card.
2. Select **SWITCHES WITH MOST SESSIONS** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most BGP sessions at the top. Scroll down to view those with the fewest sessions.

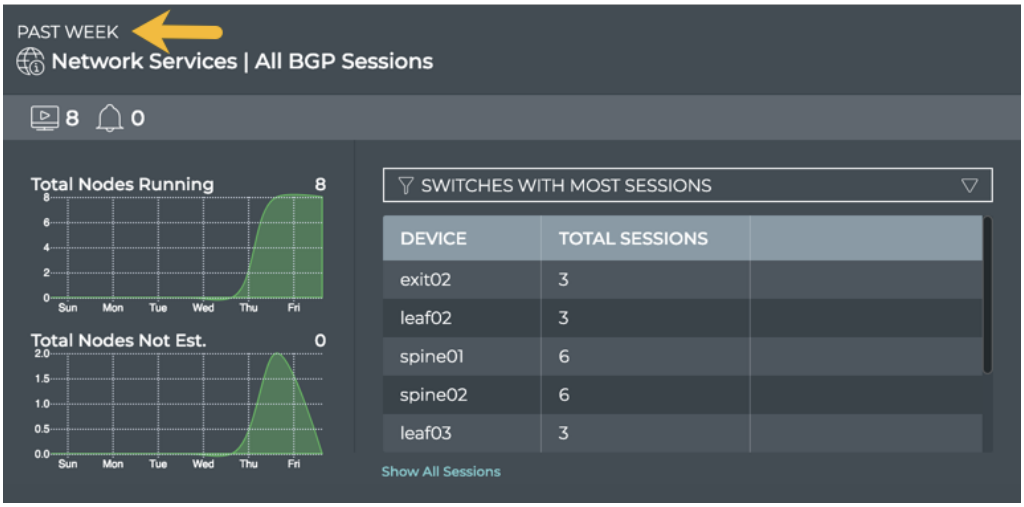


To compare this data with the same data at a previous time:

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.





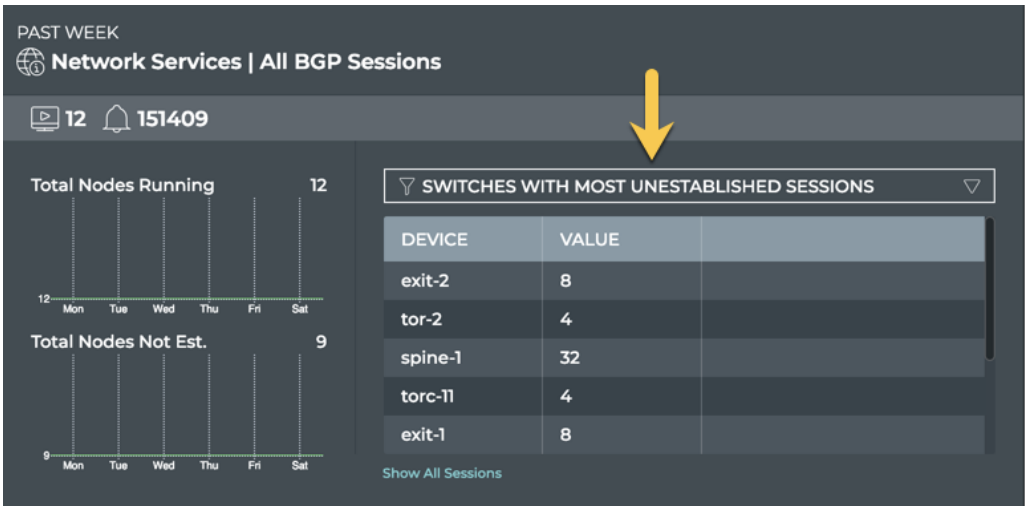
You can now see whether there are significant differences between this time and the original time. If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running BGP than previously, looking for changes in the topology, and so forth.

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.

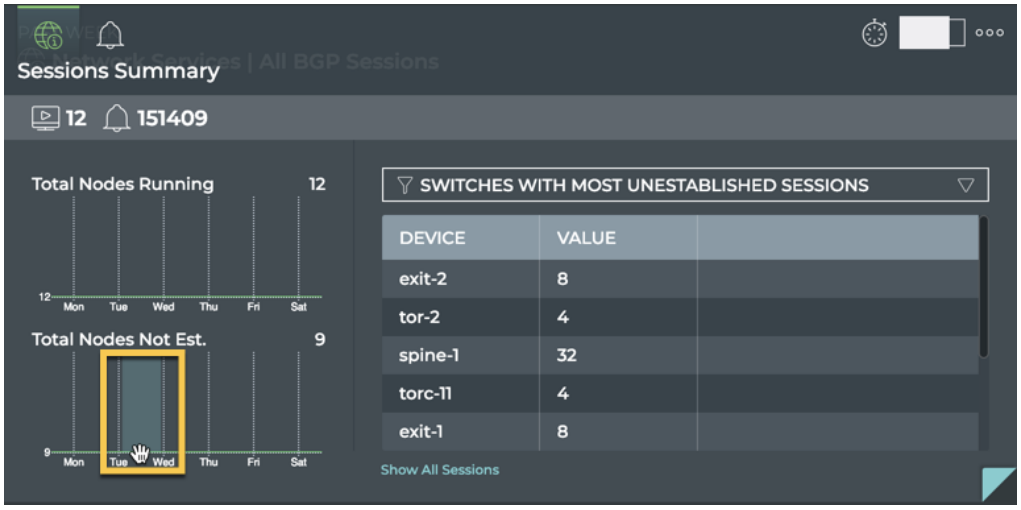
To view switches with the most unestablished BGP sessions:

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

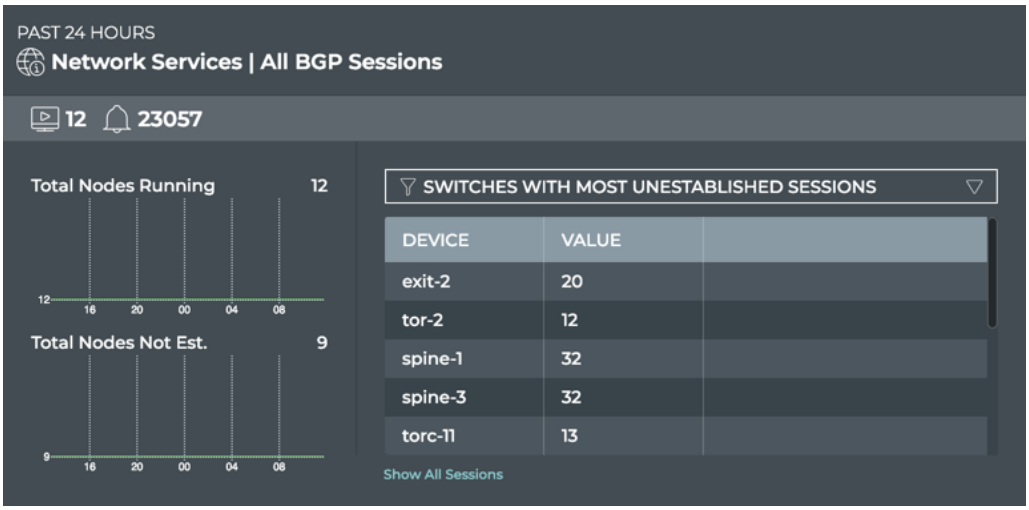


Where to go next depends on what data you see, but a couple of options include:

- Hover over the **Total Nodes Not Est.** chart to focus on the switches and hosts with the most unestablished sessions 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 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 (see page 258).

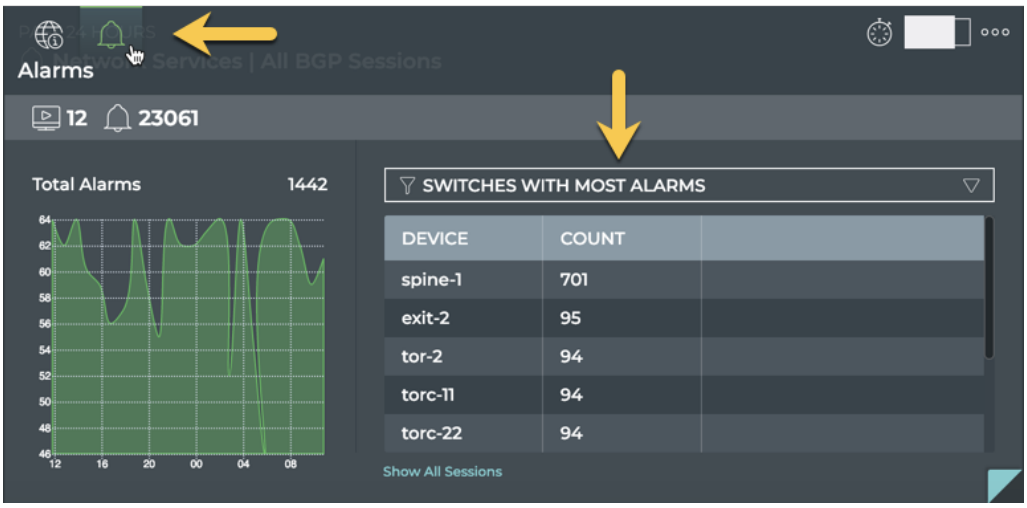
- Click **Show All Sessions** to investigate all BGP sessions with events in the full screen card.

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.

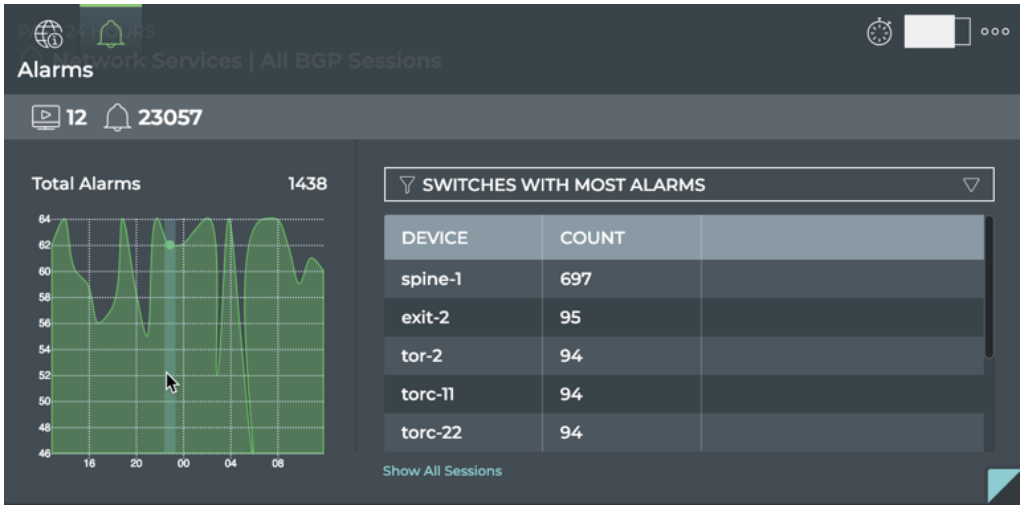
To view switches with the most BGP alarms:

1. Open the large BGP Service card.
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.

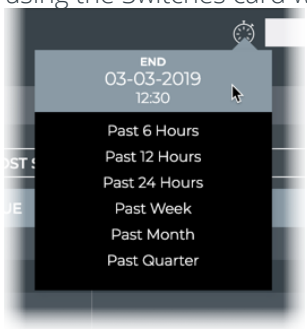


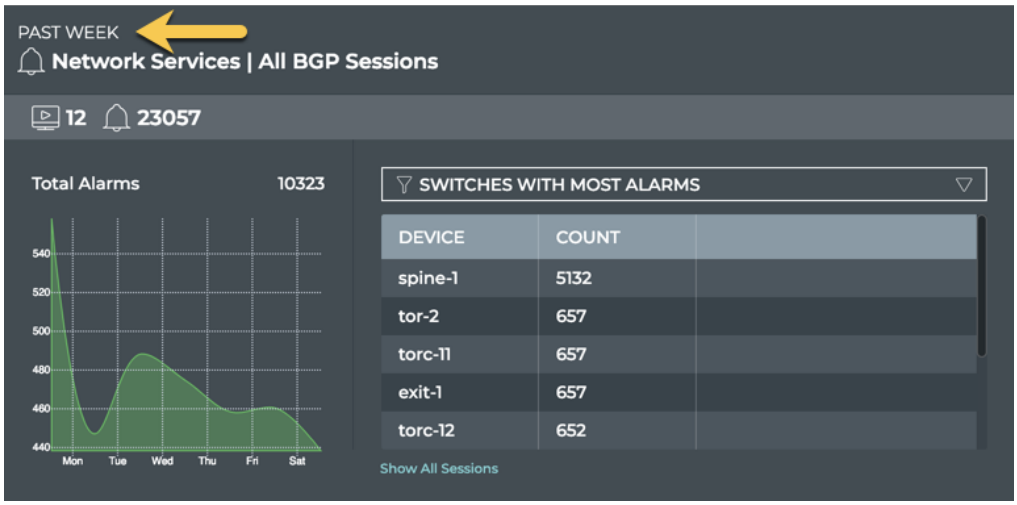
Where to go next depends on what data you see, but a few options include:

- 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.





  In this example, the total alarm count has reduced significantly from one week ago.

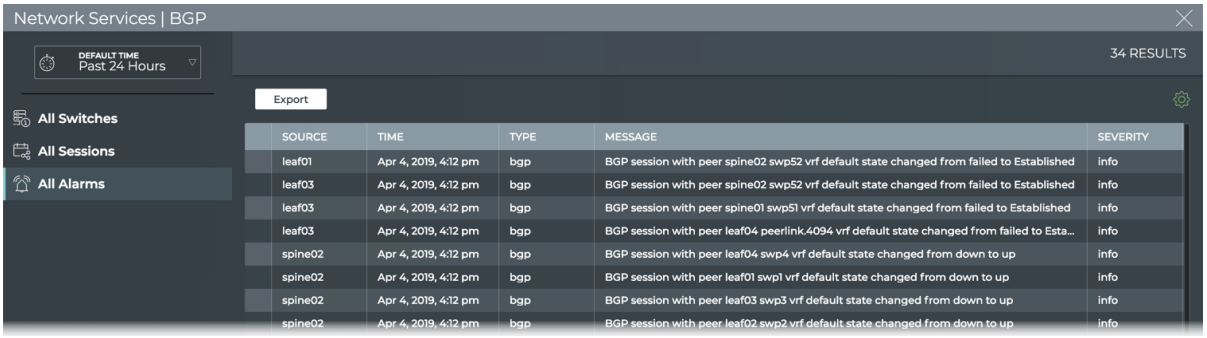
- Click **Show All Sessions** to investigate all BGP sessions with events in the full screen card.

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.
2. Click **All Alarms** tab in the navigation panel.
   By default, events are listed in most recent to least recent order.



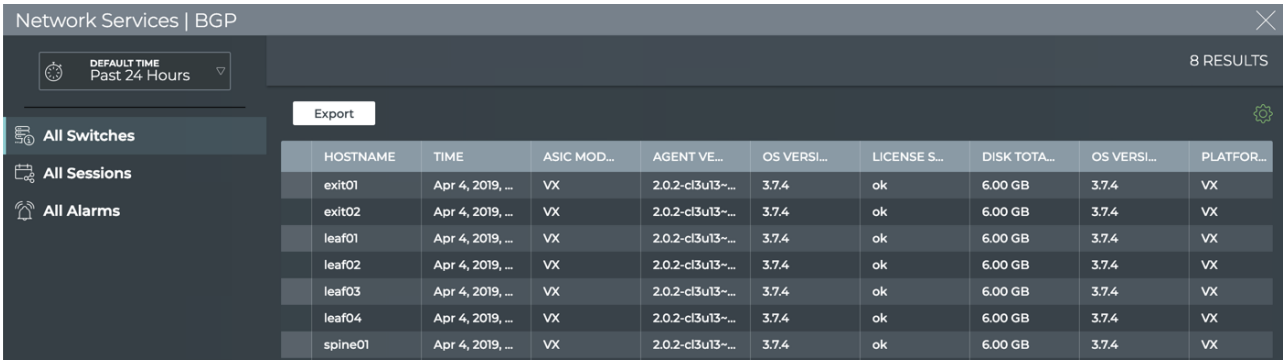
Where to go next depends on what data you see, but a couple of options include:

- 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 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.

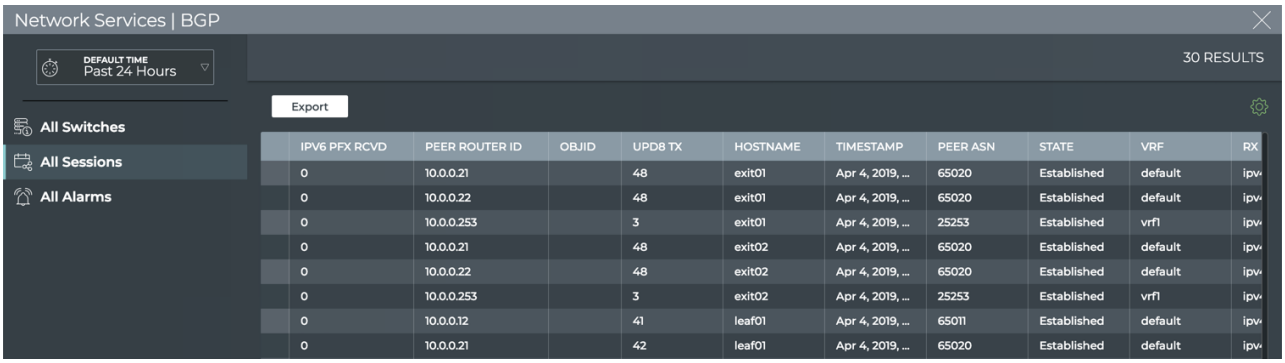


To return to your workbench, click ✕ in the top right corner.

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.

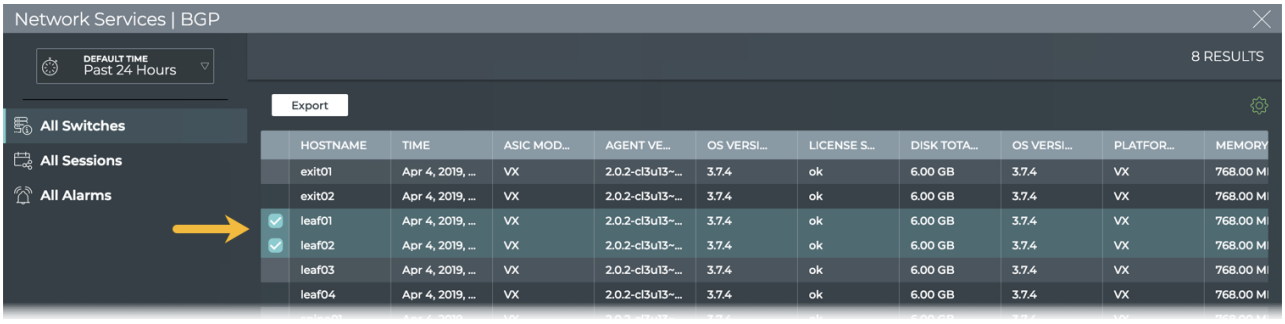


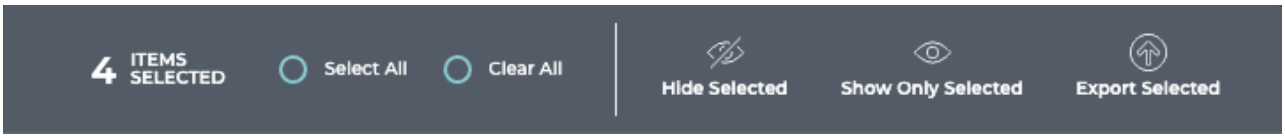
To return to your workbench, click ✕ in the top right corner.

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).





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.

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 **Export** button.

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

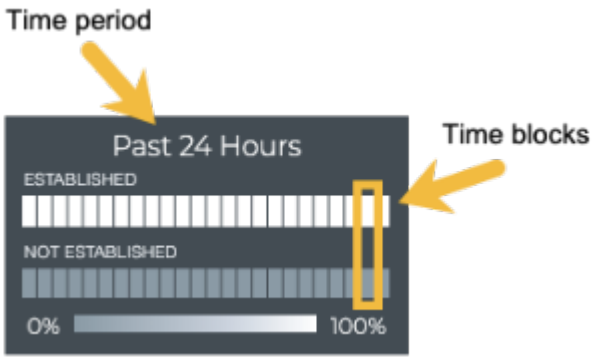
Monitor a Single BGP Session

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.

> To access the single session cards, you must open the full screen BGP Service (all sessions) card, click the All Sessions tab, and double-click on a session. The full screen card automatically closes so you can view the medium single session card.

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.

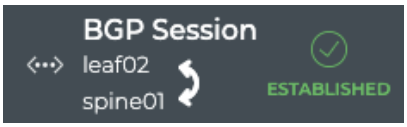


Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour

Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
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

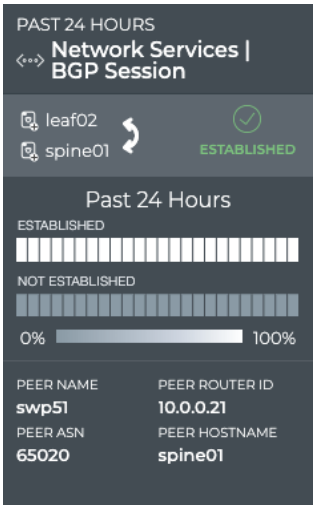
BGP Session Card Workflow Summary

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

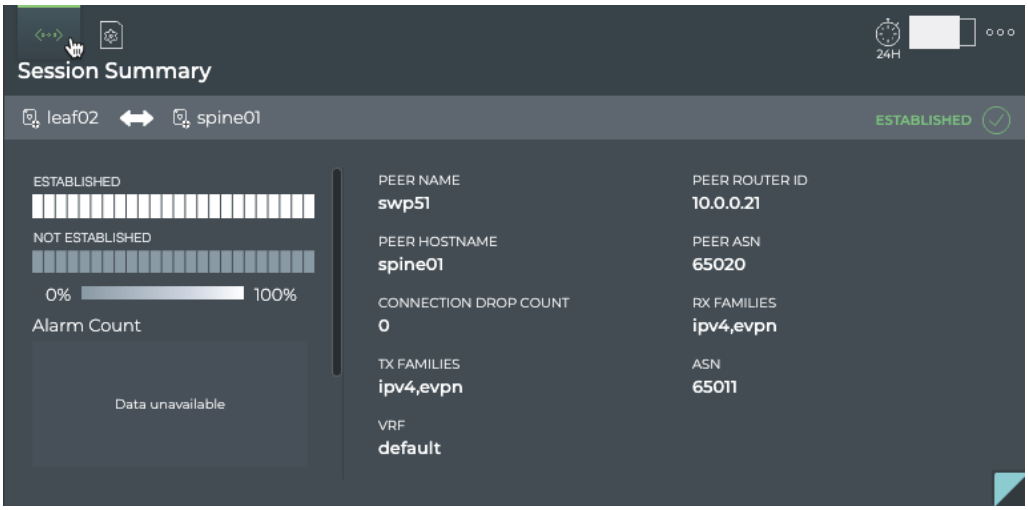
The medium BGP Session card displays:



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
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 Granularity of Data Shown Based on Time Period (see page).
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.

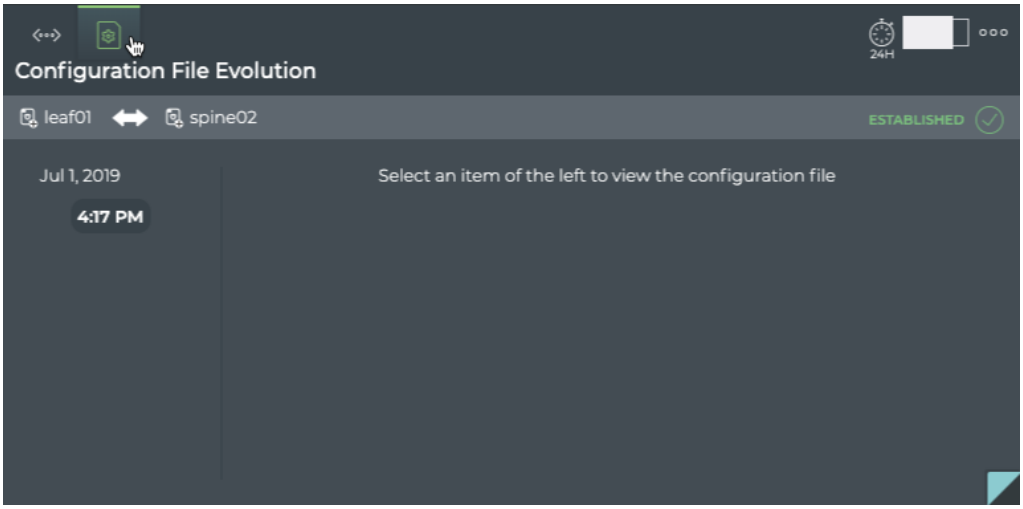
The *Session Summary* tab displays:



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	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 ⓧ
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 Granularity of Data Shown Based on Time Period (see page) .
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
	Receive and Transmit address types supported. Values include IPv4, IPv6, and EVPN.

Item	Description
RX/TX Families	
Peer Hostname	User-defined name for peer device
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

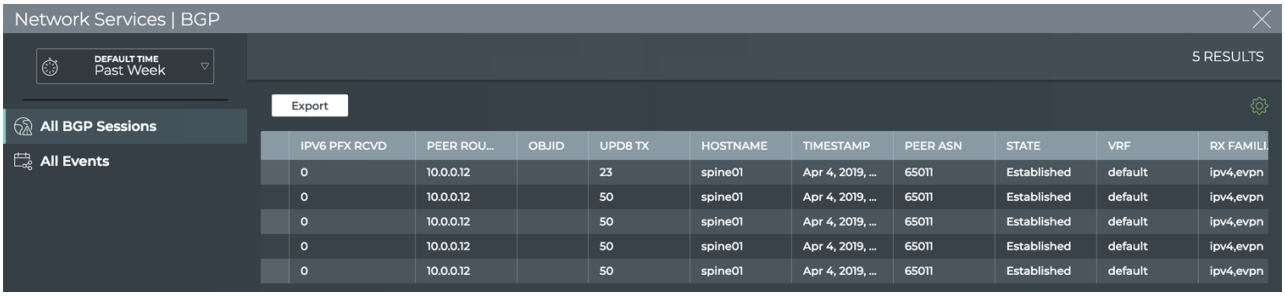
The *Configuration File Evolution* tab displays:



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

Item	Description
	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 **File** is selected, the configuration file as it was at the selected time is shown. When **Diff** 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. **Note**: If no configuration file changes have been made, the card shows no results at all.

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



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	Displays all BGP sessions running on the host device. This tab provides the following additional data about each session:
	• **ASN**: Autonomous System Number, identifier for a collection of IP networks and routers. Example values include 633284,655435.
	• **Conn Dropped**: Number of dropped connections for a given session
	• **Conn Estd**: Number of connections established for a given session
	• **DB State**: Session state of DB
	• **Evpn Pfx Rcvd**: Address prefix for EVPN traffic. Examples include 115, 35.
	• **Ipv4, and Ipv6 Pfx Rcvd**: Address prefix for IPv4 or IPv6 traffic. Examples include 31, 14, 12.
	• **Last Reset Time**: Time at which the session was last established or reset
	  • **Objid**: Object identifier for service
	OPID: Customer identifier. This is always zero.**Peer**
	  • ASN: Autonomous System Number for peer device
	  • Hostname: User-defined name for peer device
	  • Name: Interface name or hostname of peer device

Item	Description
	• Router Id: IP address of router with access to the peer device • **Reason**: Event or cause of failure • **Rx and Tx Families**: Address families supported for the receive and transmit session channels. Values include ipv4, ipv6, and evpn. • **State**: Current state of the session. Values include Established and NotEstd (not established). • **Timestamp**: Date and time session was started, deleted, updated or marked dead (device is down) • **Upd8 Rx:** Count of protocol messages received • **Upd8 Tx**: Count of protocol messages transmitted • **Up Time**: Number of seconds the session has be established, in EPOC notation. Example: 1550147910000 • **Vrf**: Name of the Virtual Route Forwarding interface. Examples: default, mgmt, DataVrf1081 • **Vrfid**: Integer identifier of the VRF interface when used. Examples: 14, 25, 37
All Events tab	Displays all 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: • **Message**: Text description of a BGP-related event. Example: BGP session with peer tor-1 swp7 vrf default state changed from failed to Established • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of bgp in this card workflow.
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

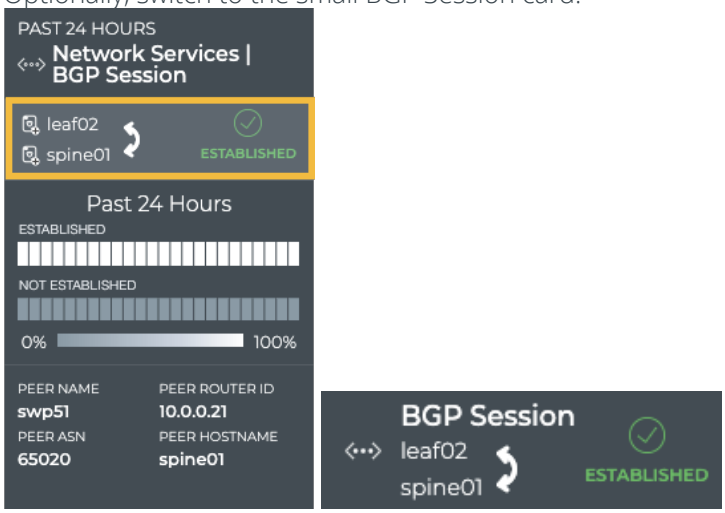
View Session Status Summary

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.

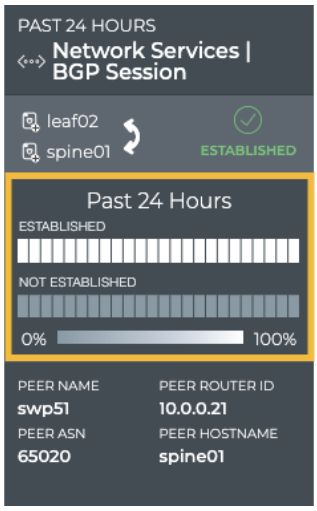


View BGP Session State Changes

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:

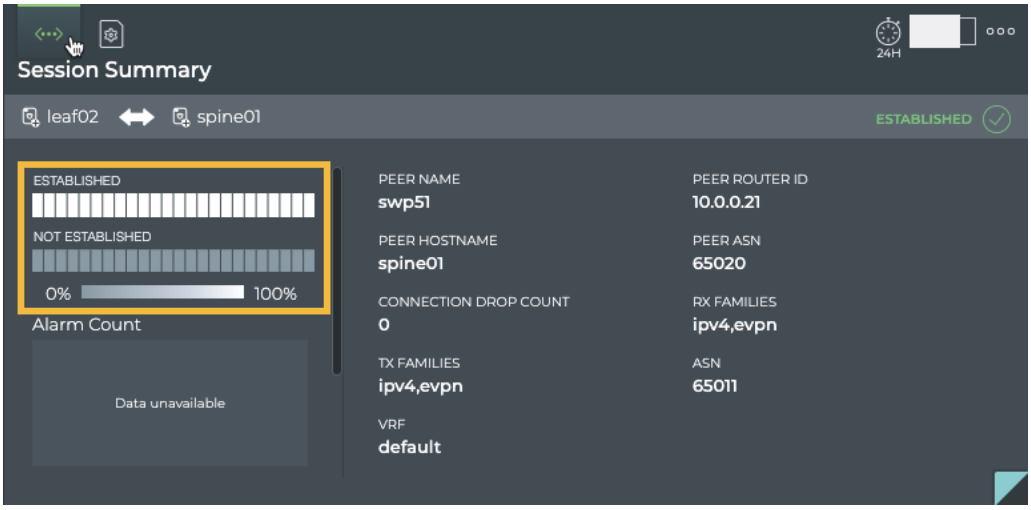
1. Add the Network Services | All BGP Sessions card.
2. Switch to the full screen card.
3. Open the large BGP Service card.
4. Click the **All Sessions** tab.
5. Double-click the session of interest. The full screen card closes automatically.



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.



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.

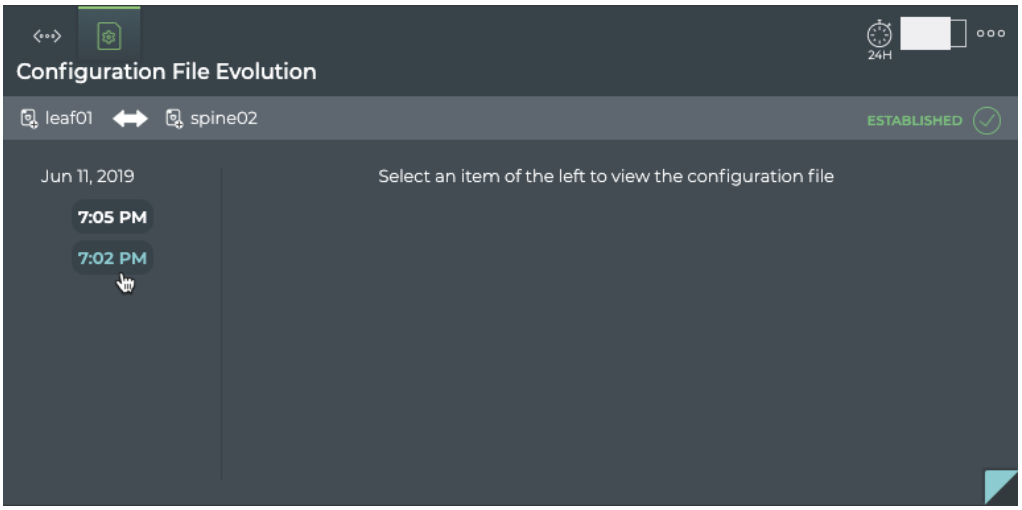
View Changes to the BGP Service Configuration File

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.

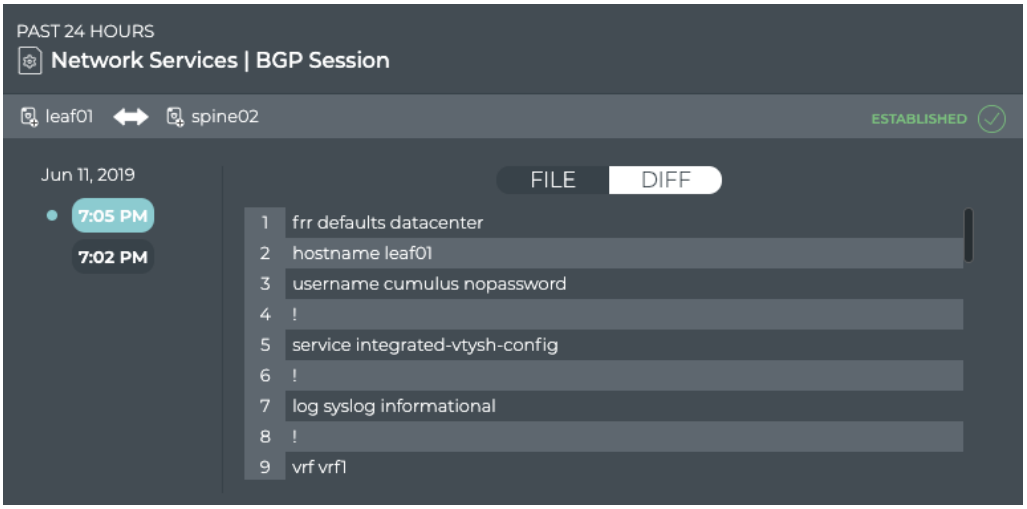
To view the configuration file changes:

1. Open the large BGP Session card.
2. Hover over the card and click

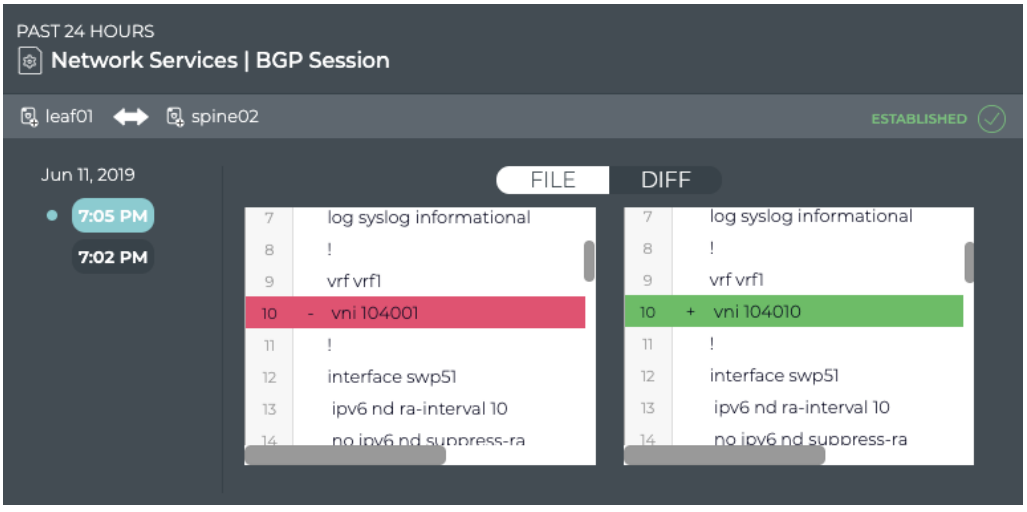
   to open the **BGP Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.



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.



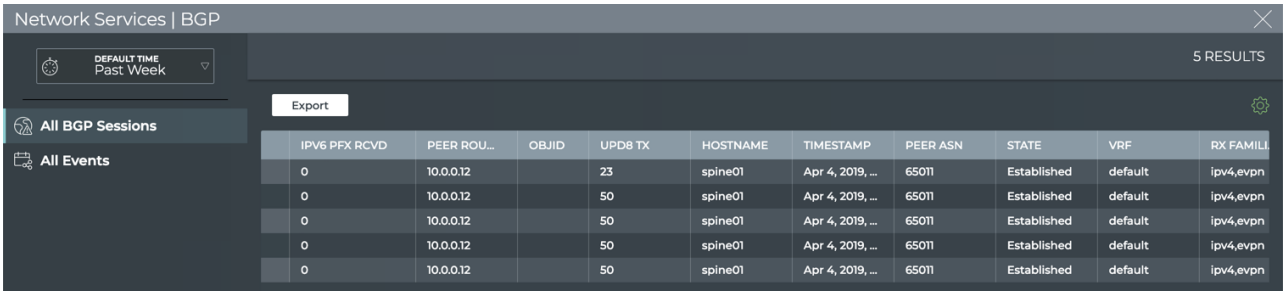
The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted, as seen in this example.



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.

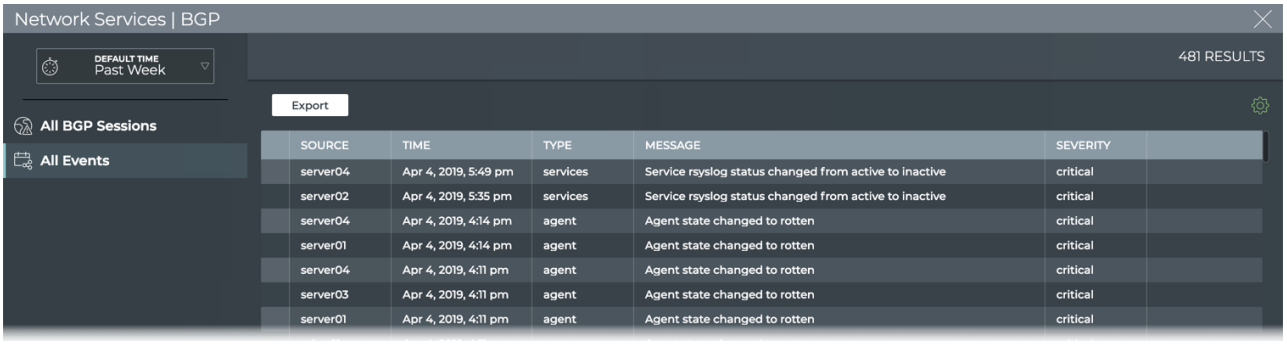


To return to your workbench, click ✕ in the top right corner.

View All Events

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

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



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.

Contents

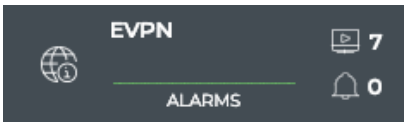
This topic describes how to...

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.

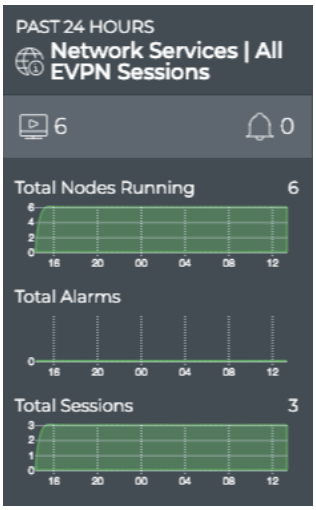
EVPN Service Card Workflow Summary

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
	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

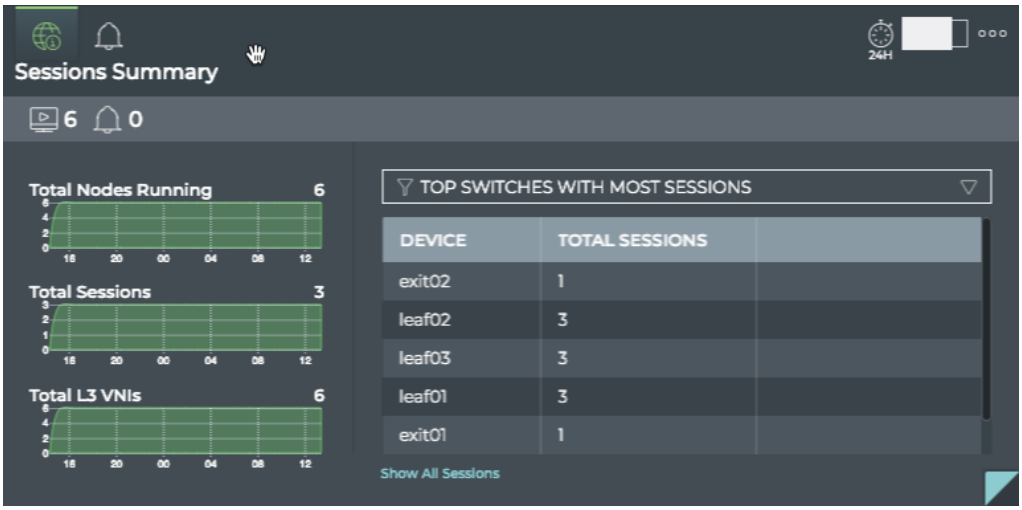
The medium EVPN Service card displays:



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
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	Total number and distribution of switches and hosts with the EVPN service enabled during the designated time period
Total Alarms chart	Total number and distribution of EVPN-related alarms received during the designated time period
Total Sessions chart	Total number and distribution of EVPN sessions network-wide during the designated time period

The large EVPN service card contains two tabs.

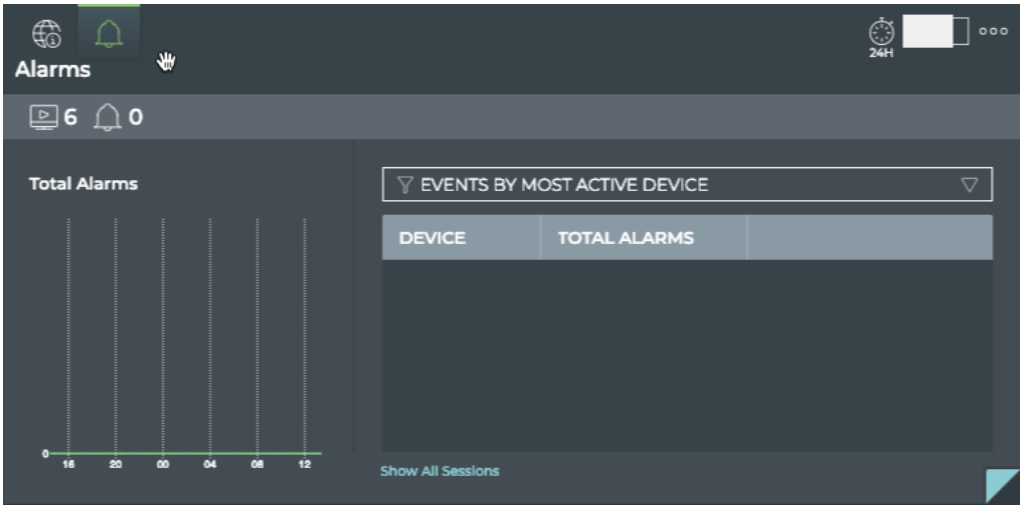
The *Sessions Summary* tab which displays:



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
Total Nodes Running chart	Total number and distribution of switches and hosts with the EVPN service enabled during the designated time period
Total Sessions chart	Total number and distribution of EVPN sessions network-wide during the designated time period
Total L3 VNIs chart	Total number and distribution of layer 3 VXLAN Network Identifiers network-wide
Table /Filter options	When the **Top Switches with Most Sessions** 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. When the **Switches with Most L2 EVPN** 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.

Item	Description
	When the **Switches with Most L3 EVPN** 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.
Show All Sessions	Link to view data for all EVPN sessions network-wide in the full screen card

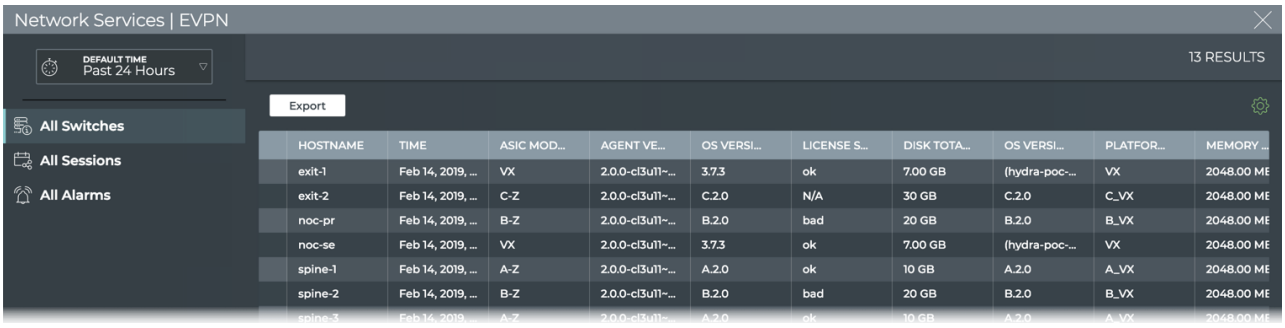
The *Alarms* tab which displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is 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
	Total number of EVPN-related alarms received during the designated time period
Total Alarms chart	Total number and distribution of EVPN-related alarms received during the designated time period
Table /Filter options	When the **Events by Most Active Device** 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

Item	Description
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.



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	Displays all switches and hosts running the EVPN service. By default, the device list is sorted by **hostname**. This tab provides the following additional data about each device:
	• **Agent**
	  • State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).
	  • 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.
	• **ASIC**
	  • Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.
	  • Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.
	  • Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.
	  • Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.

Item	Description

	• Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.
	• **CPU**
	  • Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.
	  • Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.
	  • Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.
	  • Nos: Number of cores. Example values include 2, 4, and 8.
	• **Disk Total Size**: Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.
	• **License State**: Indicator of validity. Values include ok and bad.
	• **Memory Size**: Total amount of local RAM. Example values include 8192 MB and 2048 MB.
	• **OS**
	  • Vendor: Operating System manufacturer. Values include Cumulus Networks, RedHat, Ubuntu, and CentOS.
	  • Version: Software version number of the OS. Example values include 3.7.3, 2.5.x, 16.04, 7.1.
	  • Version Id: Identifier of the OS version. For Cumulus, this is the same as the *Version* (3.7.x).
	• **Platform**
	  • Date: Date and time the platform was manufactured. Example values include 7/12/18 and 10/29/2015.
	  • MAC: System MAC address. Example value: 17:01:AB:EE:C3:F5.
	  • Model: Manufacturer's model name. Examples include AS7712-32X and S4048-ON.
	  • Number: Manufacturer part number. Examples values include FP3ZZ7632014A, 0J09D3.
	  • Revision: Release version of the platform
	  • Series: Manufacturer serial number. Example values include D2060B2F044919GD000060, CN046MRJCES0085E0004.
	  • Vendor: Manufacturer of the platform. Example values include Cumulus Express, Dell, EdgeCore, Lenovo, Mellanox.
	• **Time:** Date and time the data was collected from device.

All Sessions tab	Displays all EVPN sessions network-wide. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session: • **Adv All Vni**: Indicates whether the VNI state is advertising all VNIs (true) or not (false)

Item	Description
	• **Adv Gw Ip**: Indicates whether the host device is advertising the gateway IP address (true) or not (false) • **DB State**: Session state of the DB • **Export RT**: IP address and port of the export route target used in the filtering mechanism for BGP route exchange • **Import RT**: IP address and port of the import route target used in the filtering mechanism for BGP route exchange • **In Kernel**: Indicates whether the associated VNI is in the kernel (in kernel) or not (not in kernel) • **Is L3**: Indicates whether the session is part of a layer 3 configuration (true) or not (false) • **Origin Ip**: Host device's local VXLAN tunnel IP address for the EVPN instance • **OPID**: LLDP service identifier • **Rd**: Route distinguisher used in the filtering mechanism for BGP route exchange • **Timestamp**: Date and time the session was started, deleted, updated or marked as dead (device is down) • **Vni**: Name of the VNI where session is running
All Alarms tab	Displays all EVPN 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: • **Message**: Text description of a EVPN-related event. Example: VNI 3 kernel state changed from down to up • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *evpn* in this card workflow.
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.

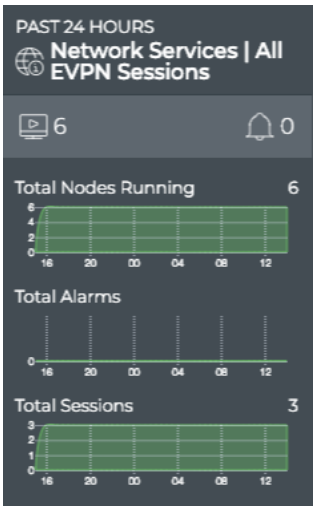
To view the summary, open the small EVPN Network Service card.

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

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.

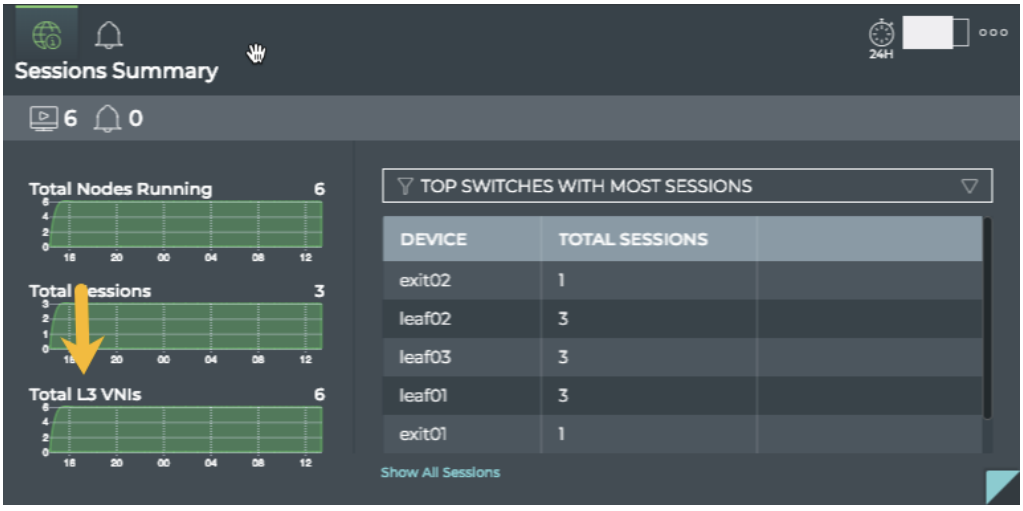


If a visual correlation is apparent, you can dig a little deeper with the large EVPN Service card tabs.

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.

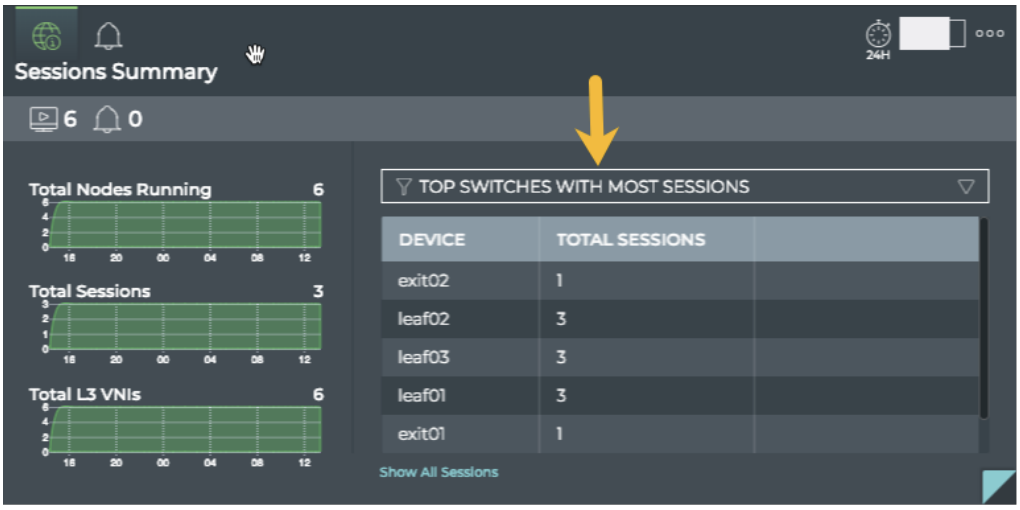


View Devices with the Most EVPN Sessions

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:

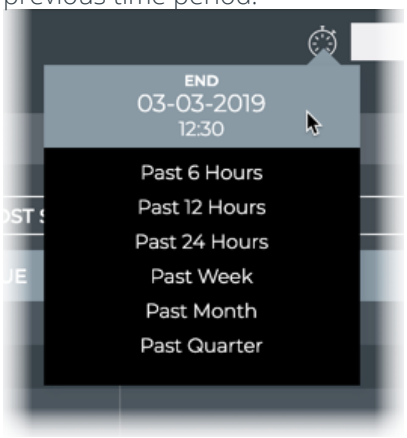
1. Open the large EVPN Service card.
2. Select **TOPSWITCHES WITH MOST SESSIONS** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most EVPN sessions at the top. Scroll down to view those with the fewest sessions.

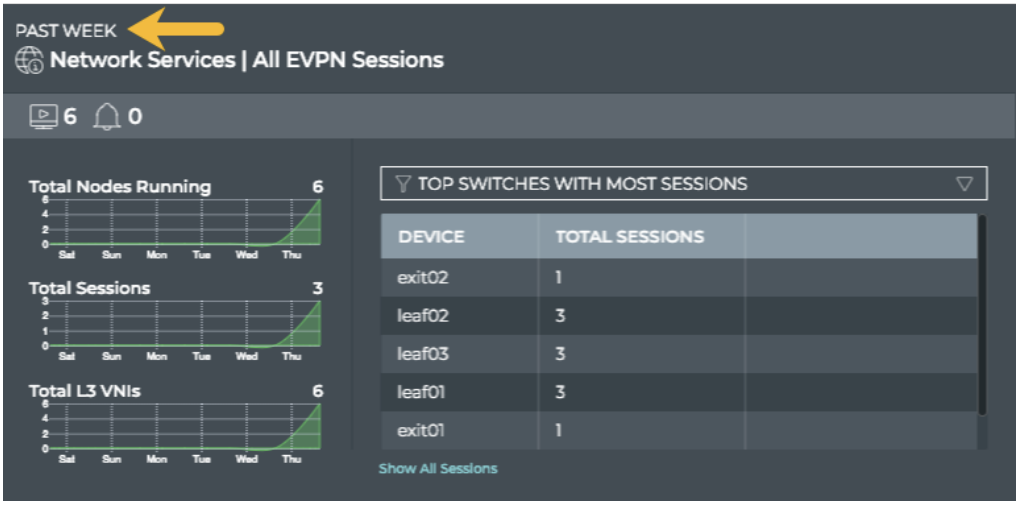


To compare this data with the same data at a previous time:

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.





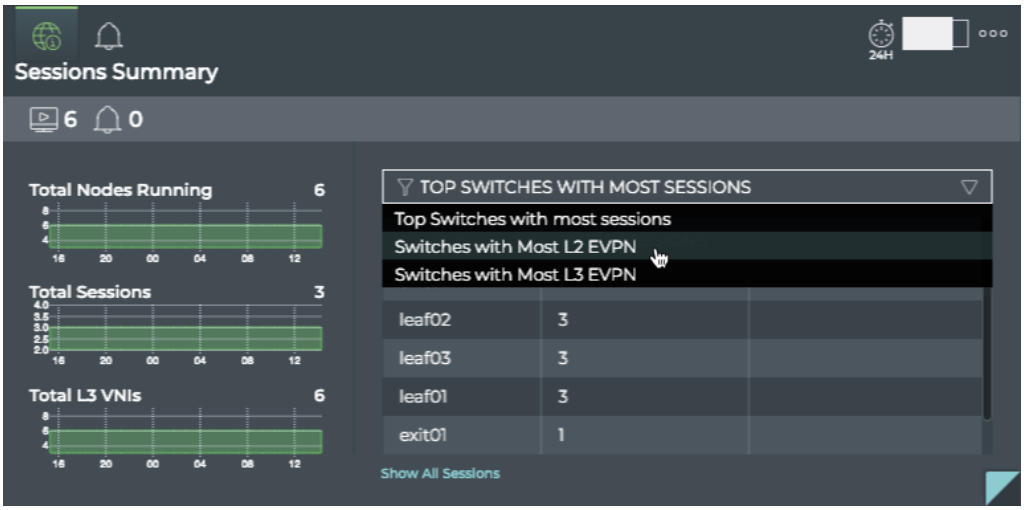
If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running EVPN than previously, looking for changes in the topology, and so forth.

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.

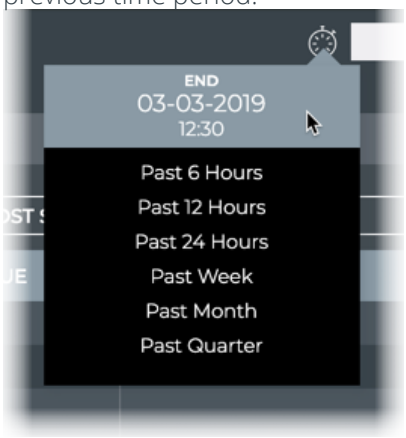
To view switches and hosts with the most layer 2 EVPN sessions:

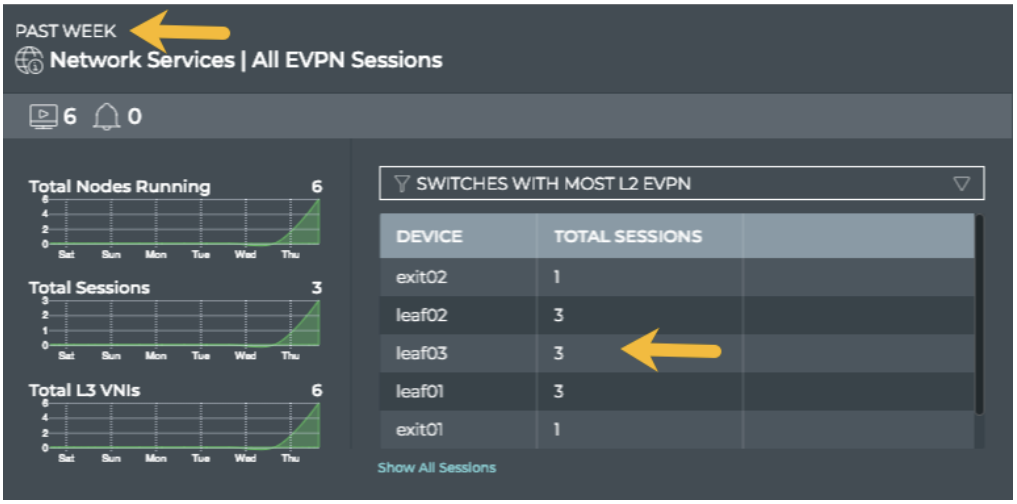
1. Open the large EVPN Service card.
2. Select **SWITCHES WITH MOST L2 EVPN** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most layer 2 EVPN sessions at the top. Scroll down to view those with the fewest sessions.



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 .
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.





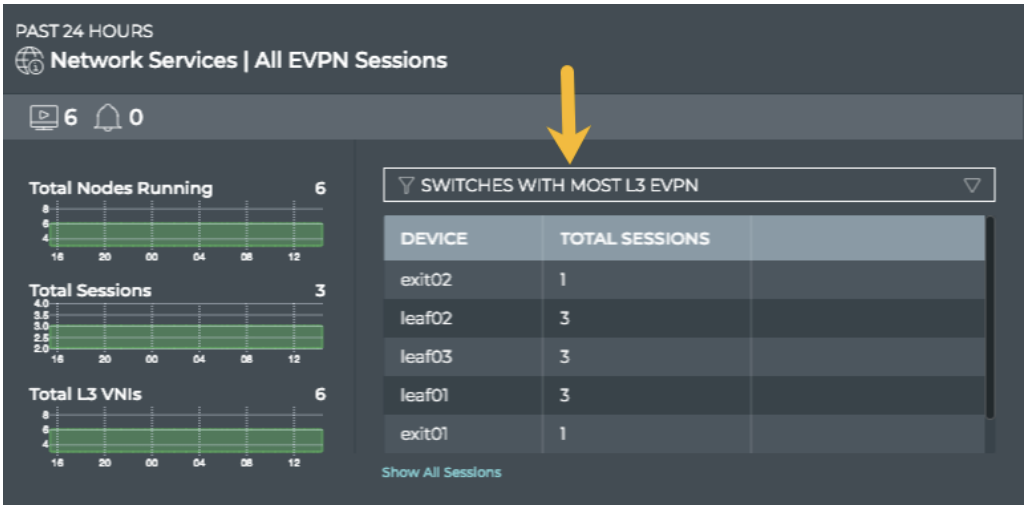
If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running EVPN than previously, looking for changes in the topology, and so forth.

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.

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

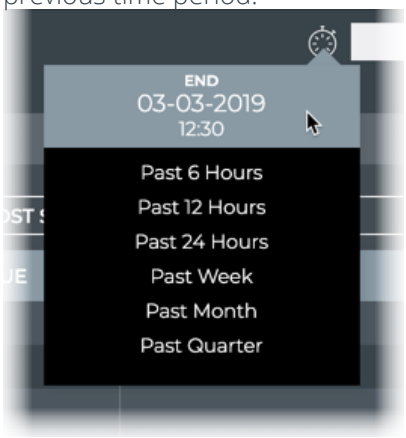
1. Open the large EVPN Service card.
2. Select **SWITCHES WITH MOST L3 EVPN** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most layer 3 EVPN sessions at the top. Scroll down to view those with the fewest sessions.

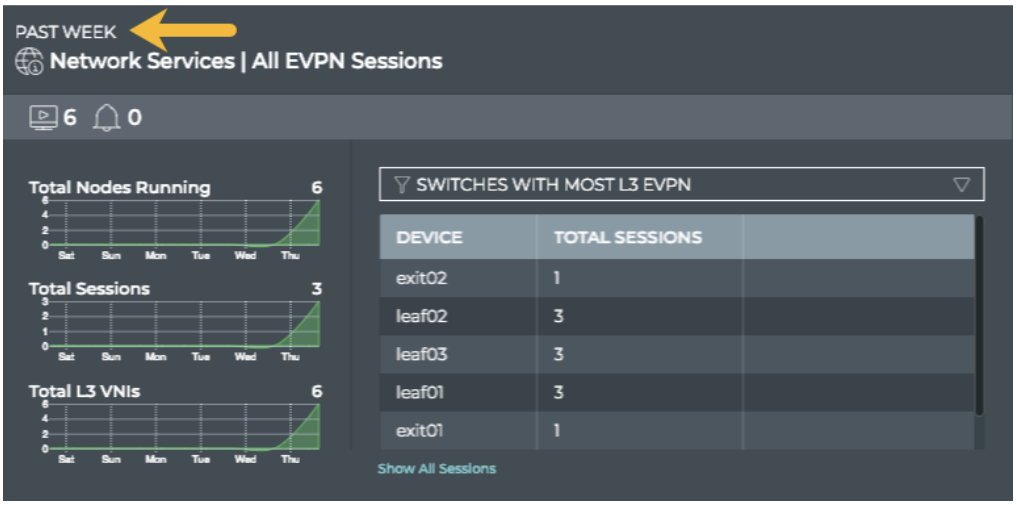


To compare this data with the same data at a previous time:

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.





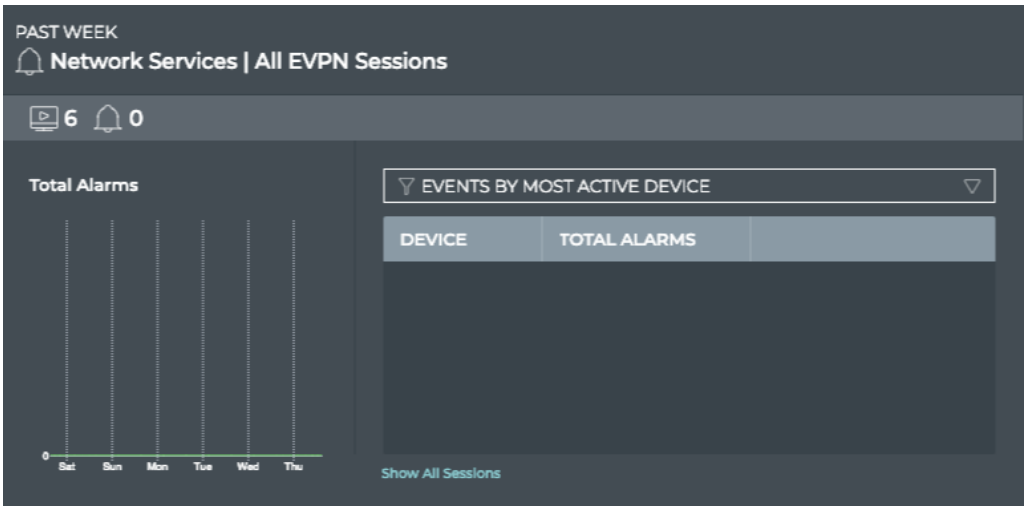
If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running EVPN than previously, looking for changes in the topology, and so forth.

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 🔔.
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:

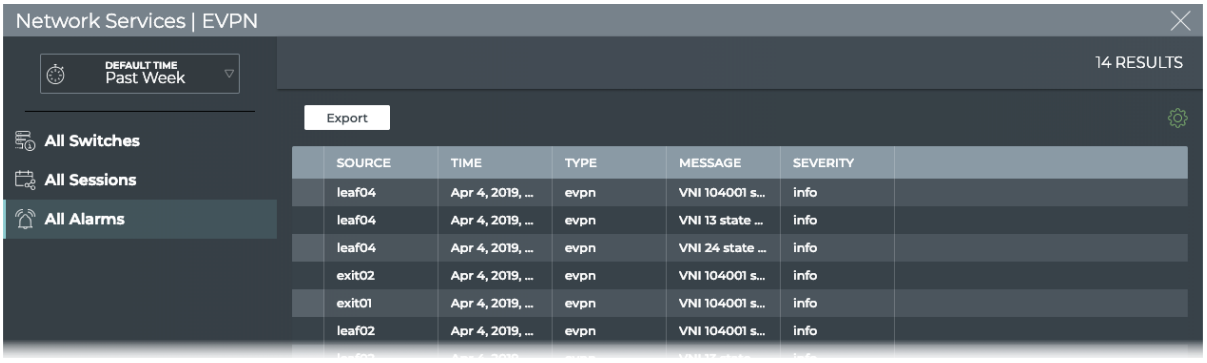
- Hover over the Total Alarms chart to focus on the switches exhibiting alarms during that smaller time slice.
  The table content changes to match the hovered content. Click on the chart to persist the table changes.
- Change the time period for the data to compare with a prior time. If the same switches 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.
2. Click **All Alarms** tab in the navigation panel. By default, events are sorted by Time, with most recent events listed first.



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

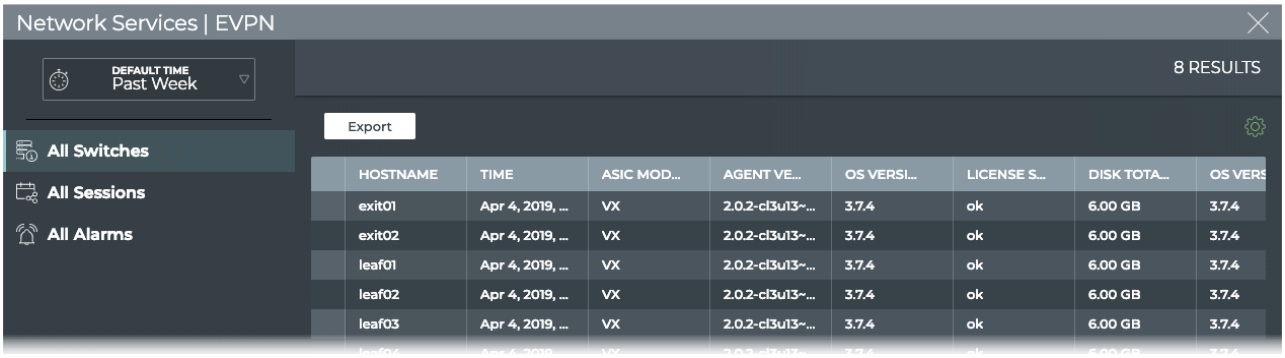
- Open one of the other full screen tabs in this flow to focus on devices or sessions.
- Sort by the **Message** or **Severity** to narrow your focus.

- 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.

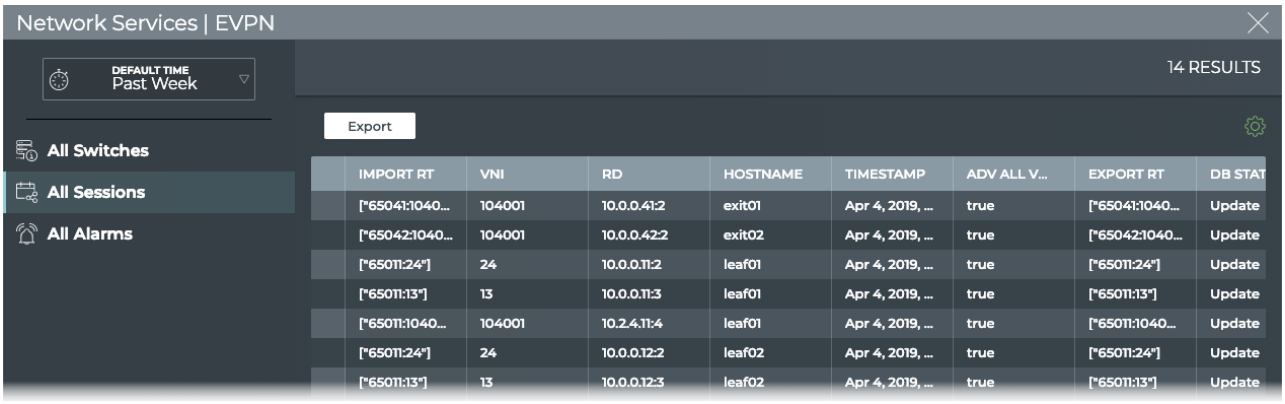


To return to your workbench, click ✕ at the top right.

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.

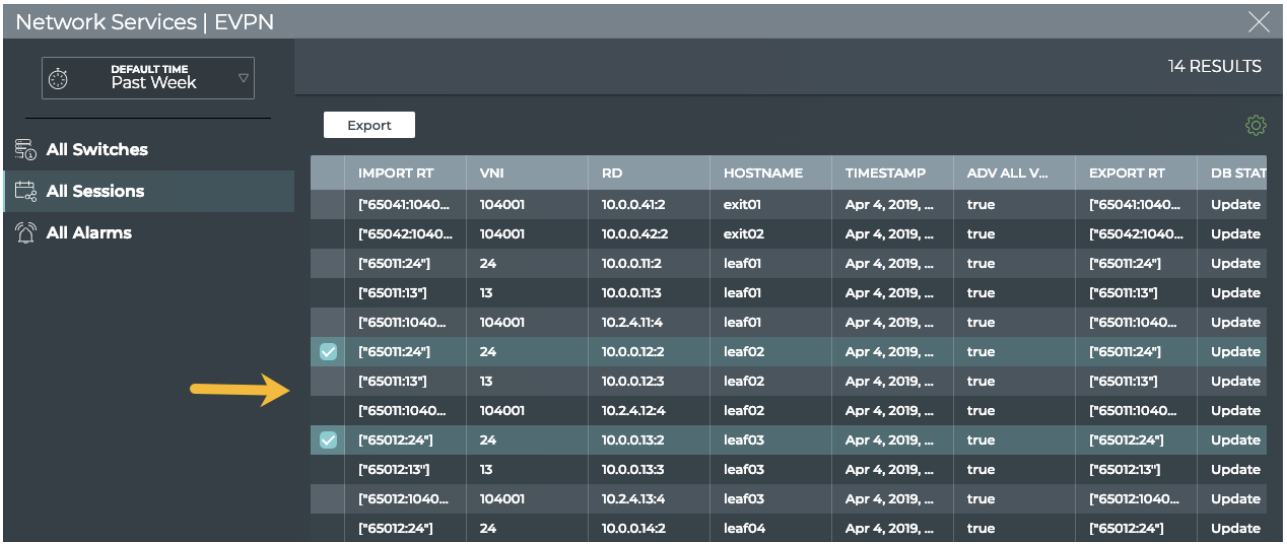


To return to your workbench, click ✕ at the top right.

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).



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 **Export** button.

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

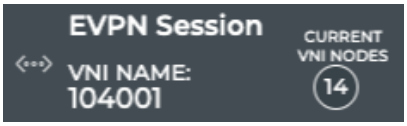
Monitor a Single EVPN Session

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.

> To access the single session cards, you must open the full screen EVPN Service (all sessions) card and click on a session. Close the full screen card to view the medium single session card.

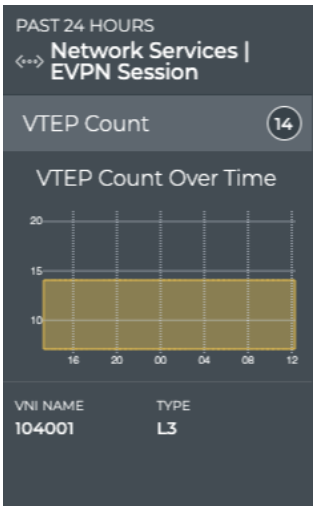
EVPN Session Card Workflow Summary

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 devices participating in the EVPN session during the designated time period

The medium EVPN Session card displays:

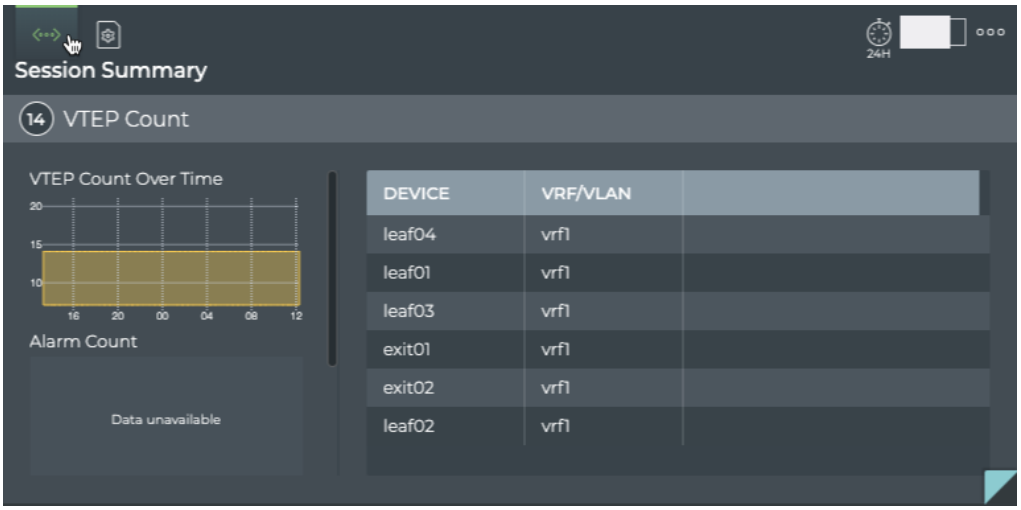


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
⟷	Indicates data is for an EVPN session
Title	Network Services | EVPN Session
Summary bar	

Item	Description
	VTEP (VXLAN Tunnel EndPoint) Count: Total number of VNI devices participating in the EVPN session during the designated time period
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
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.

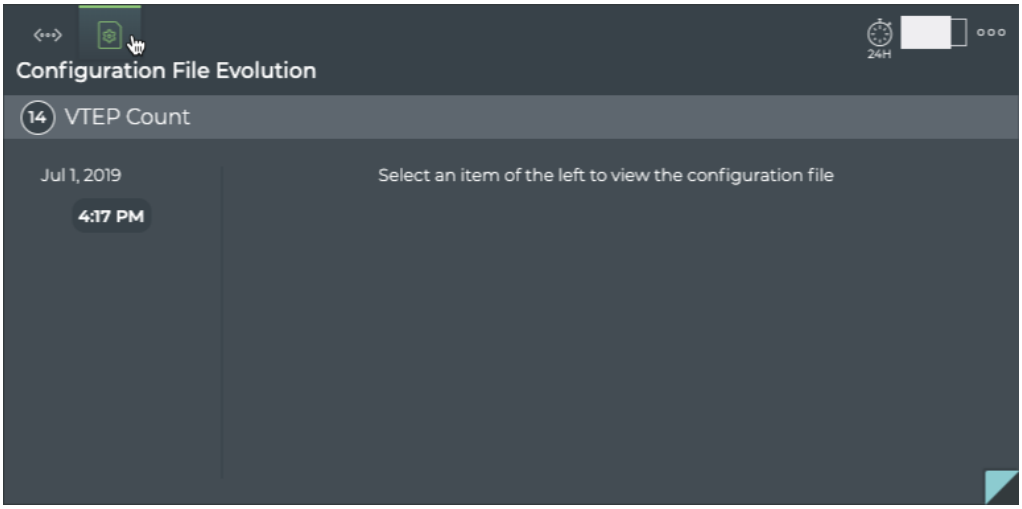
The *Session Summary* tab displays:



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 during the designated time period
VTEP Count Over Time chart	Distribution of VTEP counts during the designated time period
Alarm Count chart	Distribution of alarm event counts during the designated time period

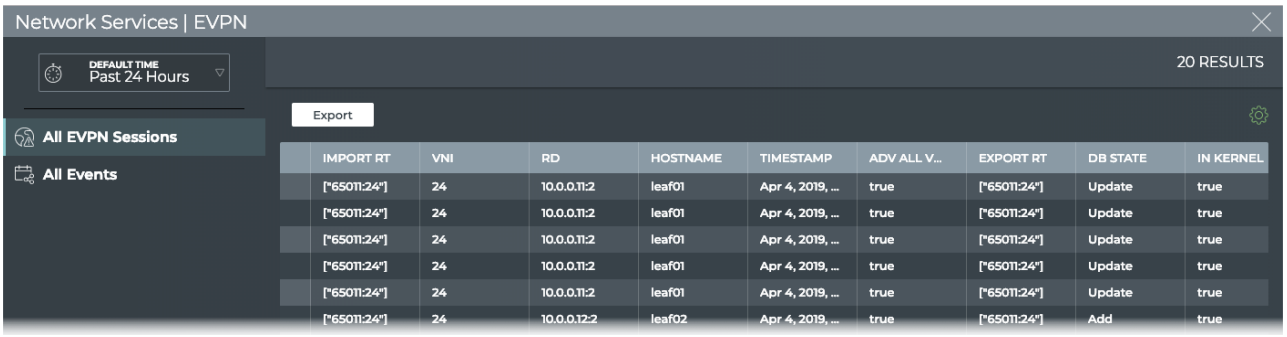
Item	Description
Info Count chart	Distribution of info event counts during the designated time period
Table	VRF (for layer 3) or VLAN (for layer 2) identifiers by device

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
⟷	Indicates data is for a single session of a Network Service or Protocol
Title	(Network Services | EVPN Session) **Configuration File Evolution**
14	VTEP count
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 **File** is selected, the configuration file as it was at the selected time is shown. When **Diff** 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. **Note**: If no configuration file changes have been made, the card shows no results at all.

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



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 EVPN Sessions tab	Displays all EVPN sessions network-wide. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session: • **Adv All Vni**: Indicates whether the VNI state is advertising all VNIs (true) or not (false) • **Adv Gw Ip**: Indicates whether the host device is advertising the gateway IP address (true) or not (false) • **DB State**: Session state of the DB • **Export RT**: IP address and port of the export route target used in the filtering mechanism for BGP route exchange • **Import RT**: IP address and port of the import route target used in the filtering mechanism for BGP route exchange • **In Kernel**: Indicates whether the associated VNI is in the kernel (in kernel) or not (not in kernel) • **Is L3**: Indicates whether the session is part of a layer 3 configuration (true) or not (false) • **Origin Ip**: Host device's local VXLAN tunnel IP address for the EVPN instance • **OPID**: LLDP service identifier • **Rd**: Route distinguisher used in the filtering mechanism for BGP route exchange • **Timestamp**: Date and time the session was started, deleted, updated or marked as dead (device is down) • **Vni**: Name of the VNI where session is running
All Events tab	Displays all 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:

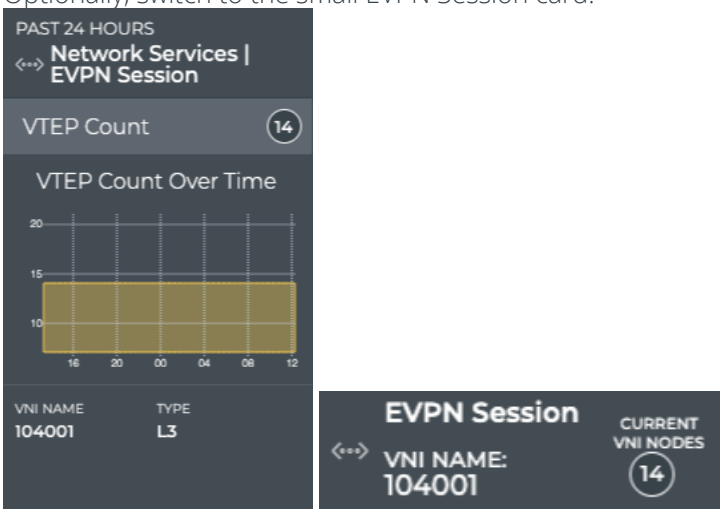
Item	Description
	• **Message**: Text description of a EVPN-related event. Example: VNI 3 kernel state changed from down to up • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *evpn* in this card workflow.
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.



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

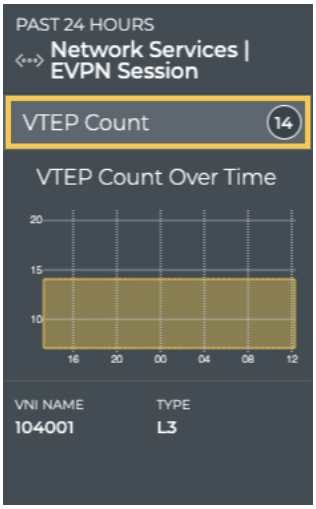
View VTEP Count

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

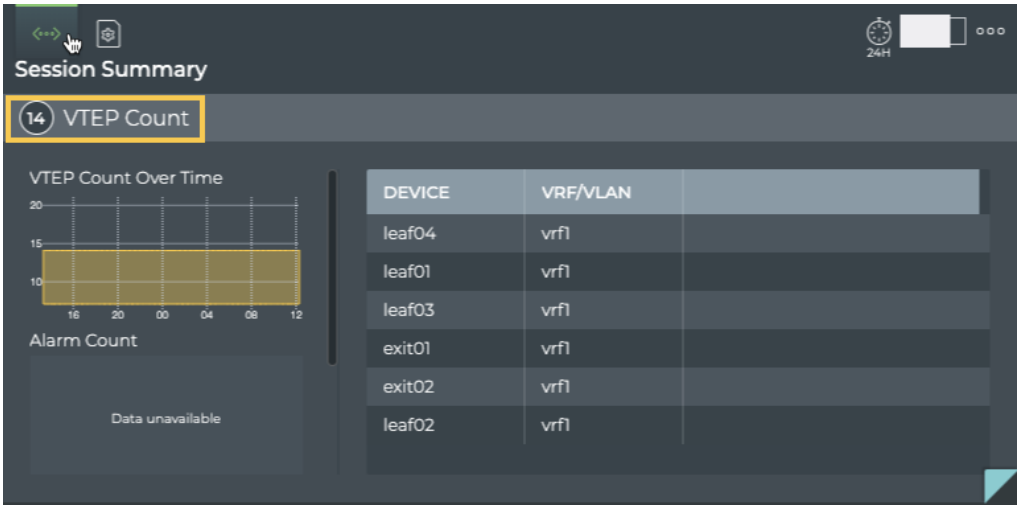
To view the count for a given EVPN session, on the *medium* EVPN Session card:

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.



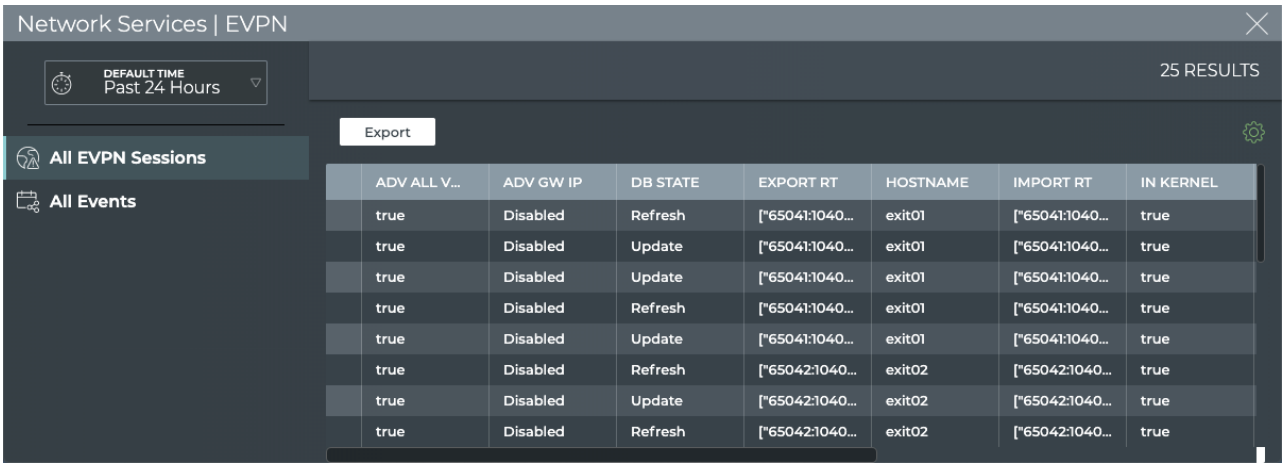
To view the count for a given EVPN session on the *large* EVPN Session card, follow the same steps as for the medium card and then switch to the large card.



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.



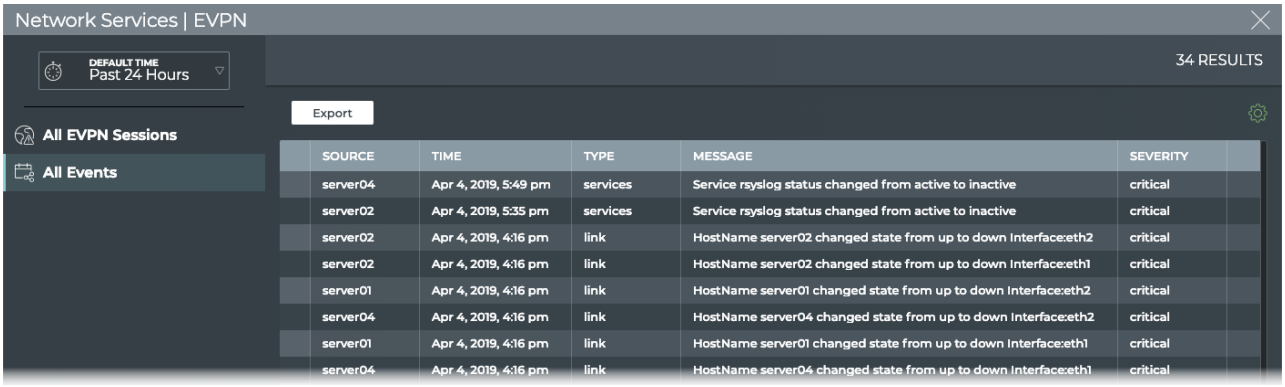
To return to your workbench, click


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, o pen the full screen EVPN Session card and click the **All Events** tab.



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.

Contents

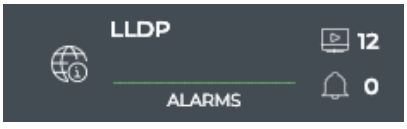
This topic describes how to...

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

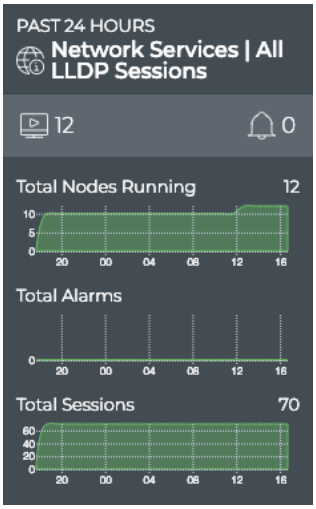
The small LLDP Service card displays:



Item	Description
	Indicates data is for all sessions of a Network Service or Protocol

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
Chart	Distribution of LLDP-related alarms received during the designated time period

The medium LLDP Service card displays:

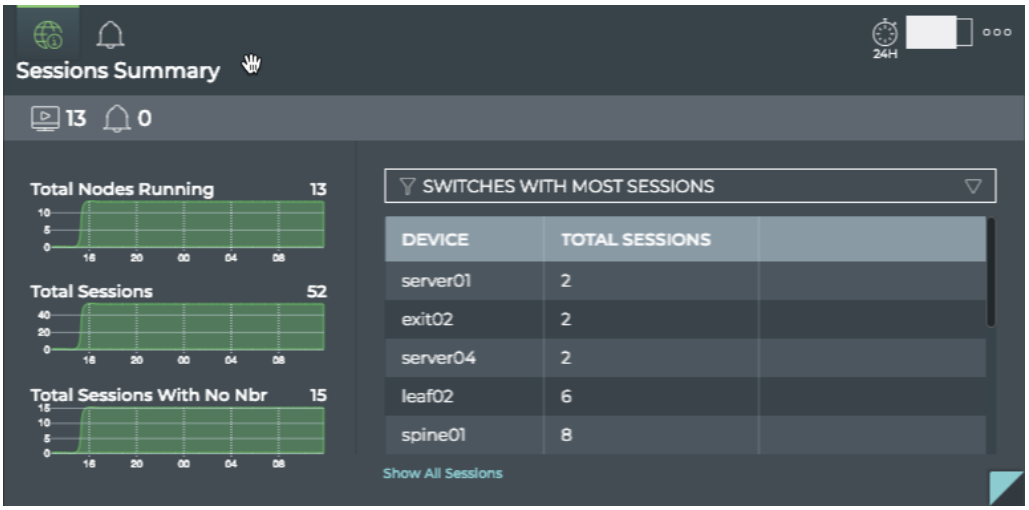


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates data is for all sessions of a Network Service or Protocol
Title	**LLDP**: All LLDP Sessions, or the LLDP Service
	Total number of switches with the LLDP service enabled during the designated time period
	Total number of LLDP-related alarms received during the designated time period
Total Nodes Running chart	Total number and distribution of switches and hosts with LLDP enabled during the designated time period
Total Alarms chart	Total number and distribution of LLDP-related alarms received during the designated time period

Item	Description
Total Sessions chart	Total number and distribution of LLDP sessions running during the designated time period

The large LLDP service card contains two tabs.

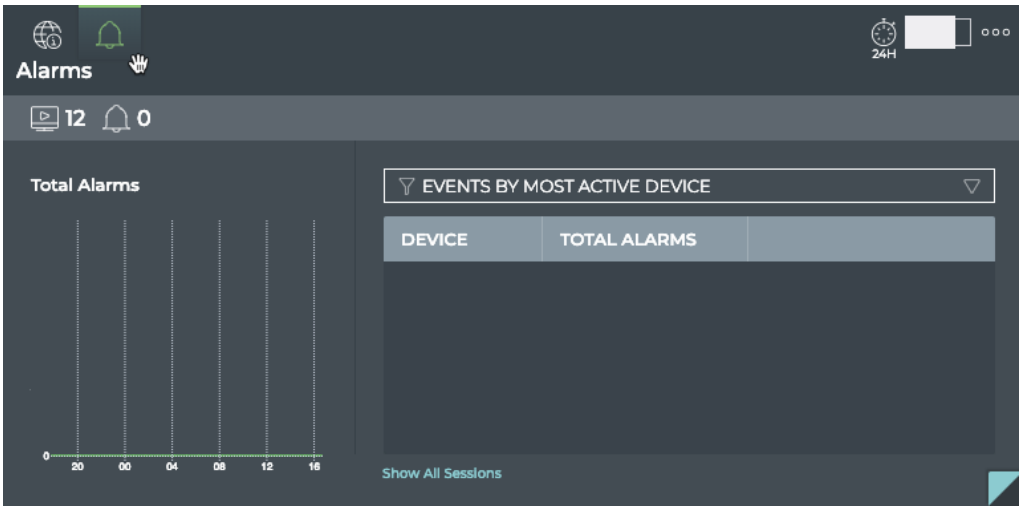
The *Sessions Summary* tab which displays:



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
Total Nodes Running chart	Total number and distribution of switches and hosts with LLDP enabled during the designated time period
Total Sessions chart	Total number and distribution of LLDP sessions running during the designated time period

Item	Description
Total Sessions with No Nbr chart	Total number and distribution of LLDP sessions missing neighbor information during the designated time period
Table /Filter options	When the **SWITCHES WITH MOST SESSIONS** 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 When the **SWITCHES WITH MOST UNESTABLISHED SESSIONS** 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
Show All Sessions	Link to view all LLDP sessions in the full screen card

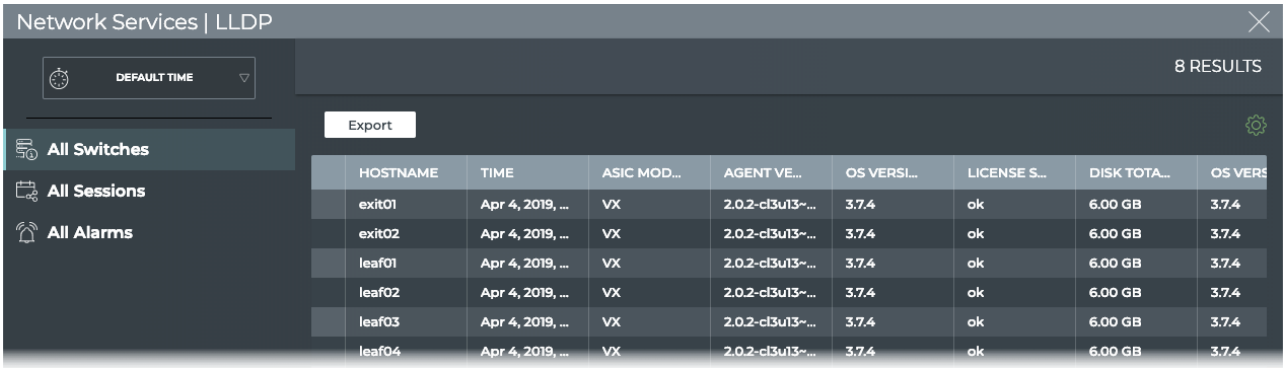
The *Alarms* tab which displays:



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

Item	Description
Total Alarms chart	Total number and distribution of LLDP-related alarms received during the designated time period
Table /Filter options	When the **EVENTS BY MOST ACTIVE DEVICE** 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
Show All Sessions	Link to view all LLDP sessions in the full screen card

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



Item	Description
Title	Network Services | LLDP
✕	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	Displays all switches and hosts running the LLDP service. By default, the device list is sorted by **hostname**. This tab provides the following additional data about each device:
	• **Agent**
	  • State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).
	  • 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.**ASIC**

Item	Description
	• Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G. • Model: Chip family. Example values include Tomahawk, Trident, and Spectrum. • Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854. • Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+. • Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox. **CPU** • Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC. • Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz. • Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338. • Nos: Number of cores. Example values include 2, 4, and 8. • **Disk Total Size**: Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB. • **License State**: Indicator of validity. Values include ok and bad. • **Memory Size**: Total amount of local RAM. Example values include 8192 MB and 2048 MB. • **OS** • Vendor: Operating System manufacturer. Values include Cumulus Networks, RedHat, Ubuntu, and CentOS. • Version: Software version number of the OS. Example values include 3.7.3, 2.5.x, 16.04, 7.1. • Version Id: Identifier of the OS version. For Cumulus, this is the same as the *Version* (3.7.x). • **Platform** • Date: Date and time the platform was manufactured. Example values include 7/12/18 and 10/29/2015. • MAC: System MAC address. Example value: 17:01:AB:EE:C3:F5. • Model: Manufacturer's model name. Examples values include AS7712-32X and S4048-ON. • Number: Manufacturer part number. Examples values include FP3ZZ7632014A, 0J09D3. • Revision: Release version of the platform • Series: Manufacturer serial number. Example values include D2060B2F044919GD000060, CN046MRJCES0085E0004.

Item	Description
	• Vendor: Manufacturer of the platform. Example values include Cumulus Express, Dell, EdgeCore, Lenovo, Mellanox. • **Time:** Date and time the data was collected from device.

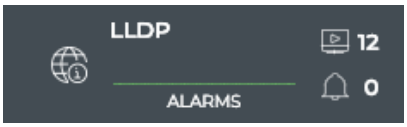
All Sessions tab	Displays all LLDP sessions network-wide. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session:
	• **DB State**: Session state of the DB.
	• **Ifname**: Name of the host interface where LLDP session is running
	• **LLDP Peer**:
	  • Os: Operating system (OS) used by peer device. Values include Cumulus Linux, RedHat, Ubuntu, and CentOS.
	  • Osv: Version of the OS used by peer device. Example values include 3.7.3, 2.5.x, 16.04, 7.1.
	  • Bridge: Indicates whether the peer device is a bridge (true) or not (false)
	  • Router: Indicates whether the peer device is a router (true) or not (false)
	  • Station: Indicates whether the peer device is a station (true) or not (false)
	• **OPID**: LLDP service identifier
	• **Peer**:
	  • Hostname: User-defined name for the peer device
	  • Ifname: Name of the peer interface where the session is running
	• **Timestamp**: Date and time that the session was started, deleted, updated, or marked dead (device is down)

All Alarms tab	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: • **Message**: Text description of a LLDP-related event. Example: LLDP Session with host leaf02 swp6 modified fields leaf06 swp21 • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *lldp* in this card workflow.
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.



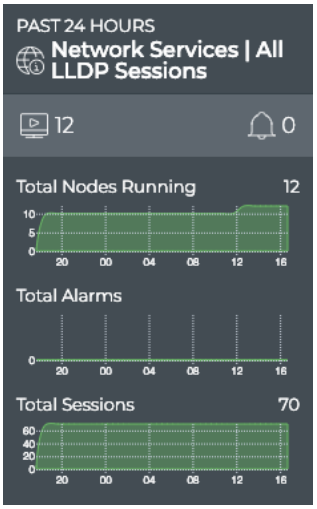
In this example, there are no LLDP alarms present on the network of twelve devices.

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

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.

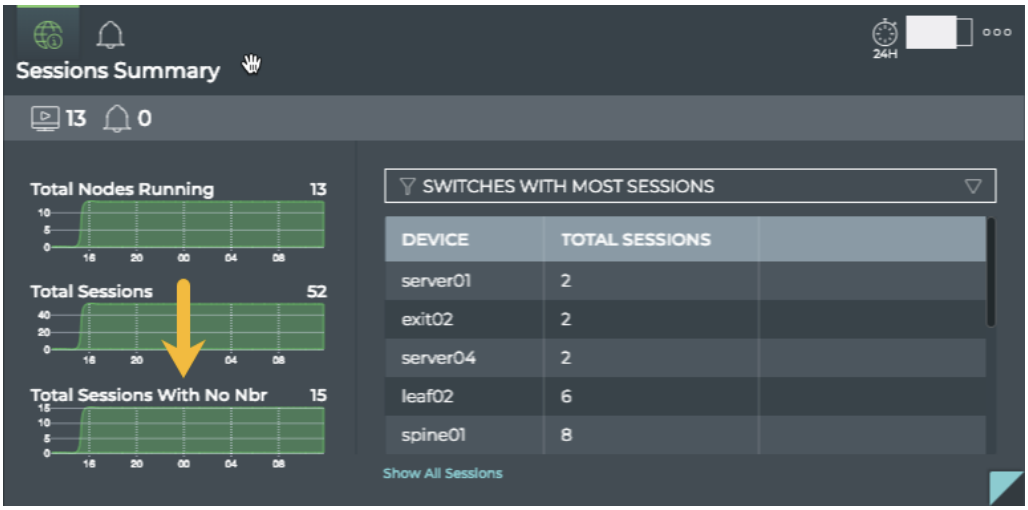


In this example, we see that twelve nodes are running the LLDP protocol, that there are 70 sessions established, and that no LLDP-related alarms have occurred in the last 24 hours.

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**.



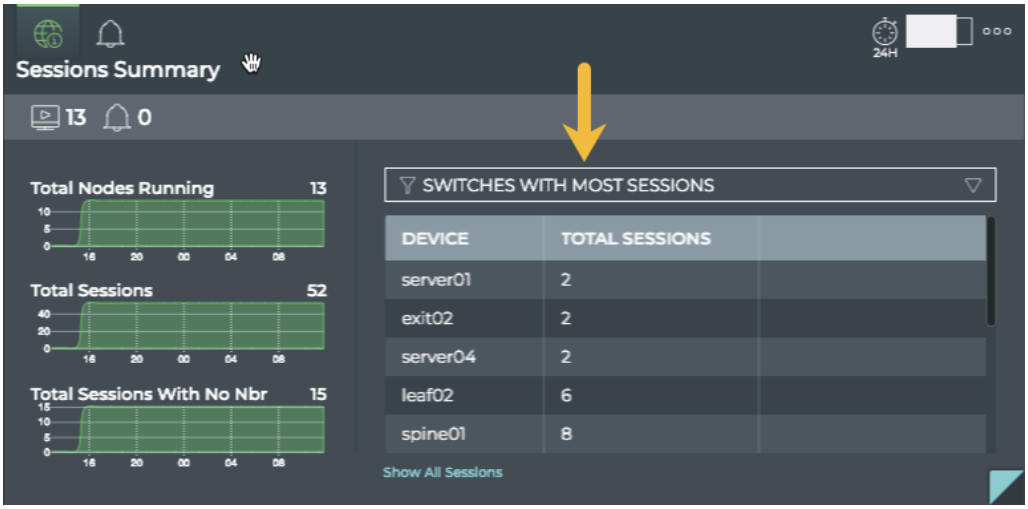
In this example, we see that 18 of the 52 sessions are missing the neighbor (peer) device.

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:

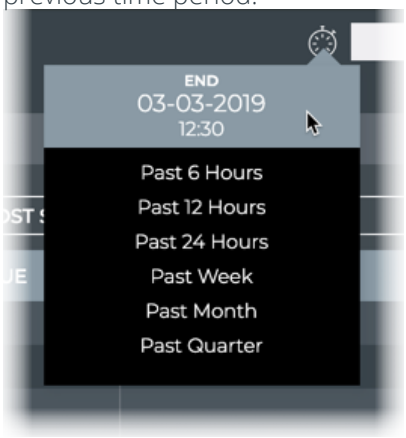
1. Open the large LLDP Service card.
2. Select **SWITCHES WITH MOST SESSIONS** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most LLDP sessions at the top. Scroll down to view those with the fewest sessions.

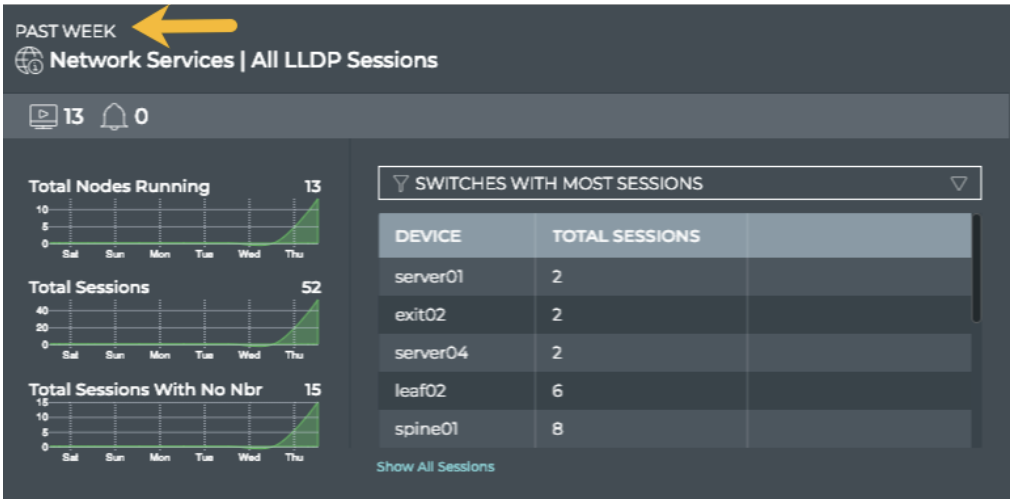


To compare this data with the same data at a previous time:

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.





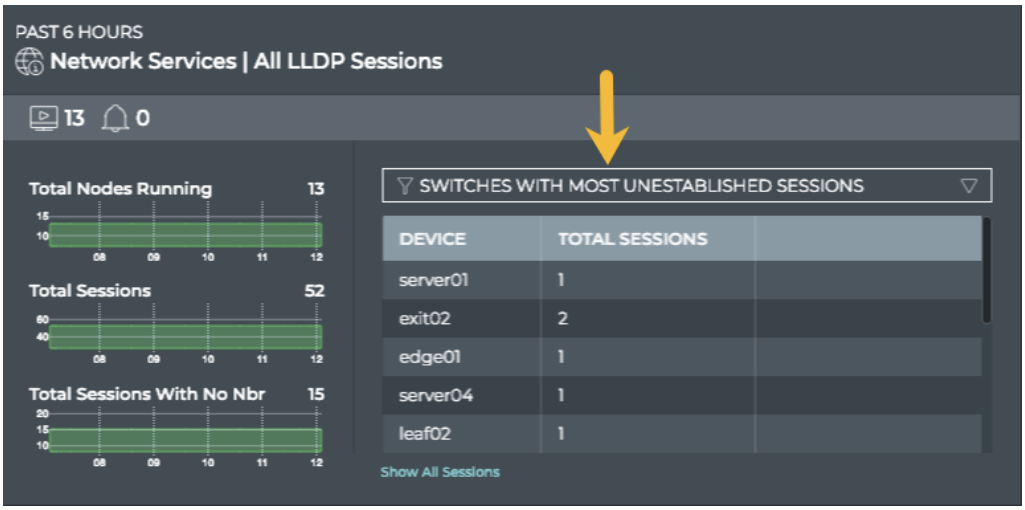
   In this case, notice that the alarms have reduced significantly in the last week. If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running LLDP than previously, looking for changes in the topology, and so forth.

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.

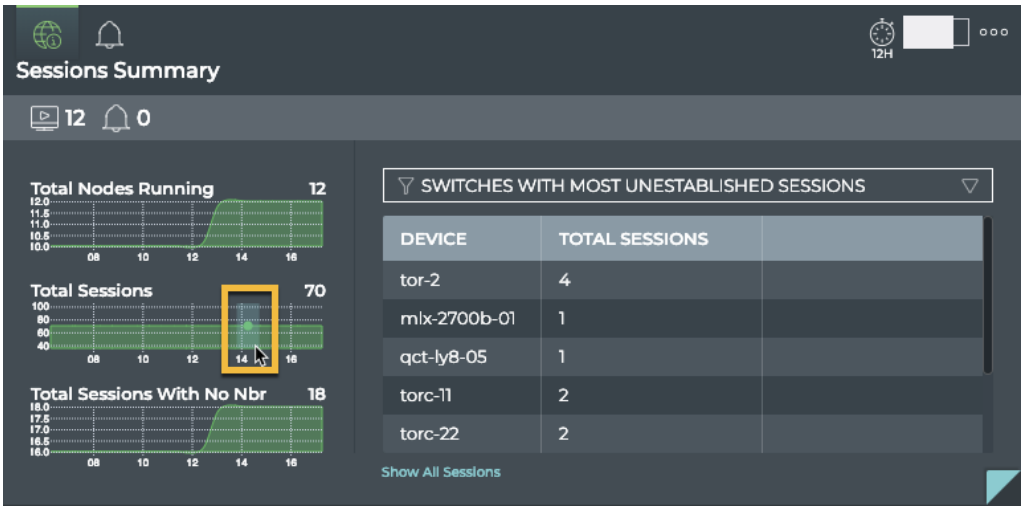
To view switches with the most unestablished LLDP sessions:

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.

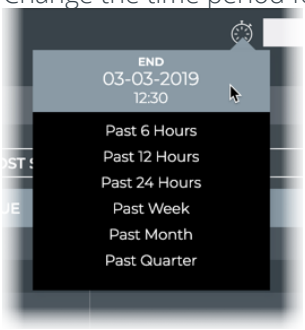


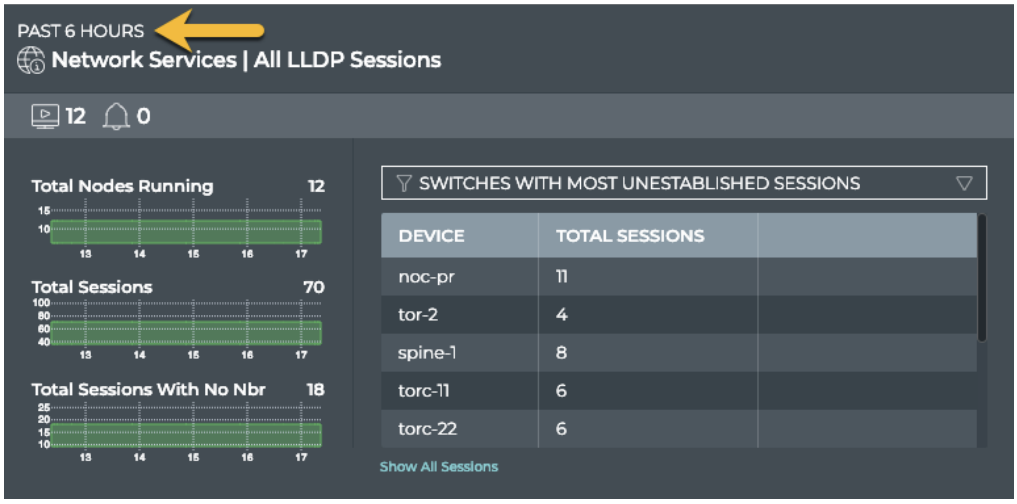
Where to go next depends on what data you see, but a few options include:

- Hover over any of the charts to focus on the number of switches or sessions with the chart characteristic 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 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 (see page 258).

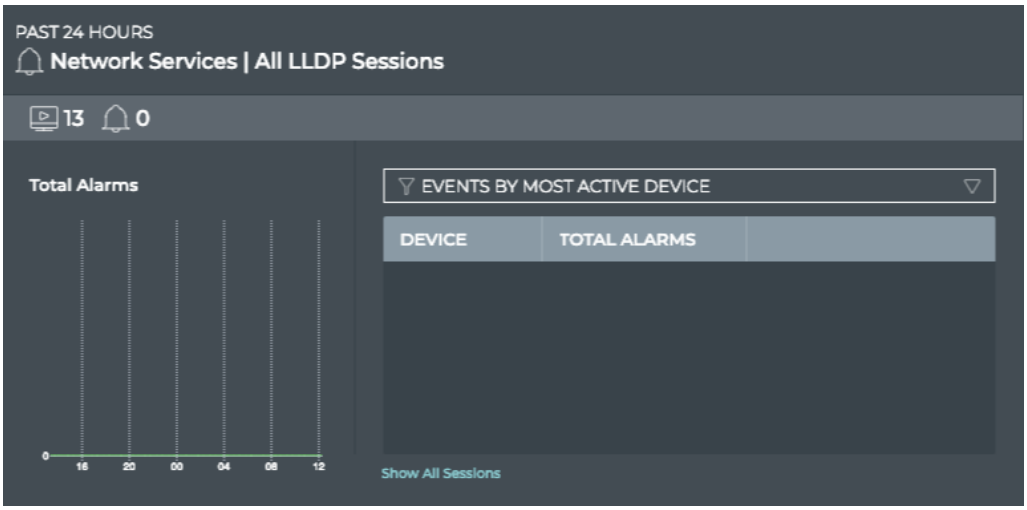
- Click **Show All Sessions** to investigate all LLDP sessions with events in the full screen card.

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 .
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:

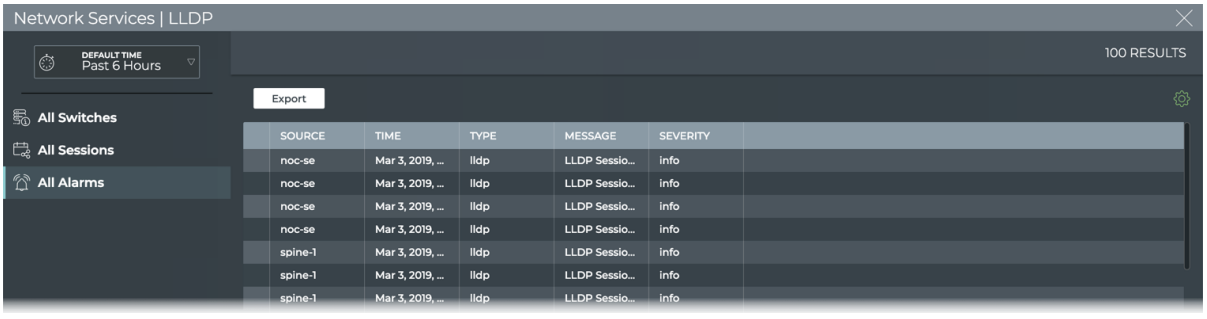
- Hover over the Total Alarms chart to focus on the switches exhibiting alarms during that smaller time slice.
  The table content changes to match the hovered content. Click on the chart to persist the table changes.
- Change the time period for the data to compare with a prior time. If the same switches 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.
2. Click the **All Alarms** tab.



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

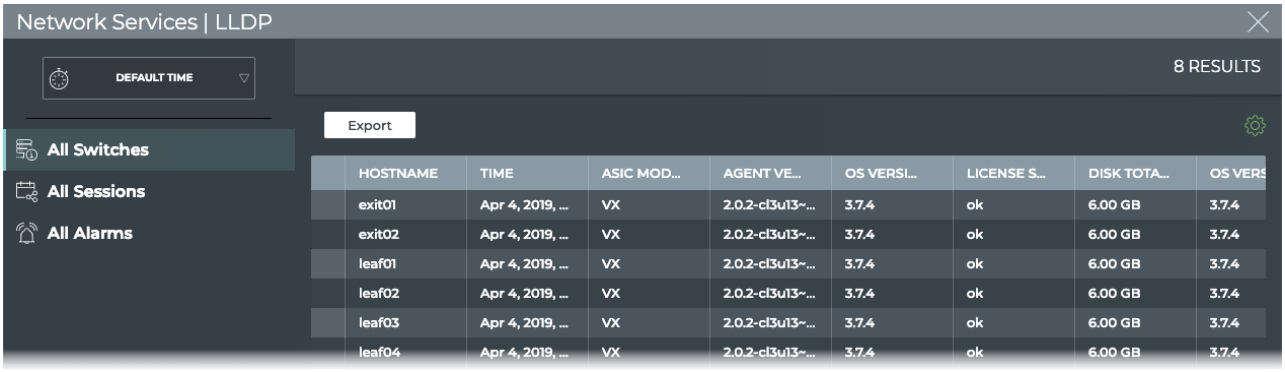
- by **Severity** to determine the most critical events
- by **Time** to find events that may have occurred at a particular time to try to correlate them with other system events

- Export data to a file
- Return to your workbench by clicking in the top right corner

View Detailed Information 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.

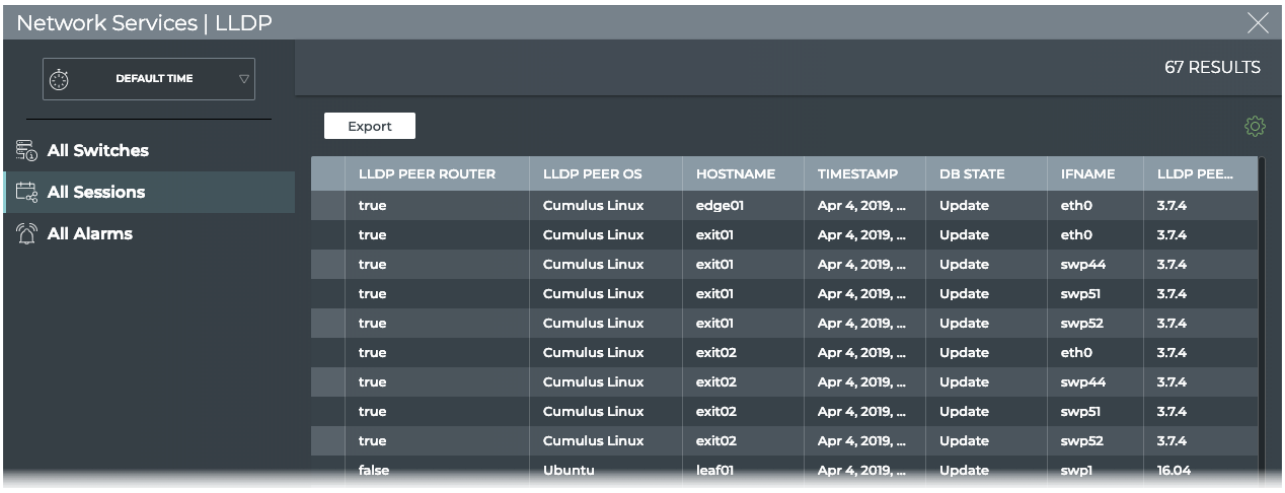


Return to your workbench by clicking in the top right corner.

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.

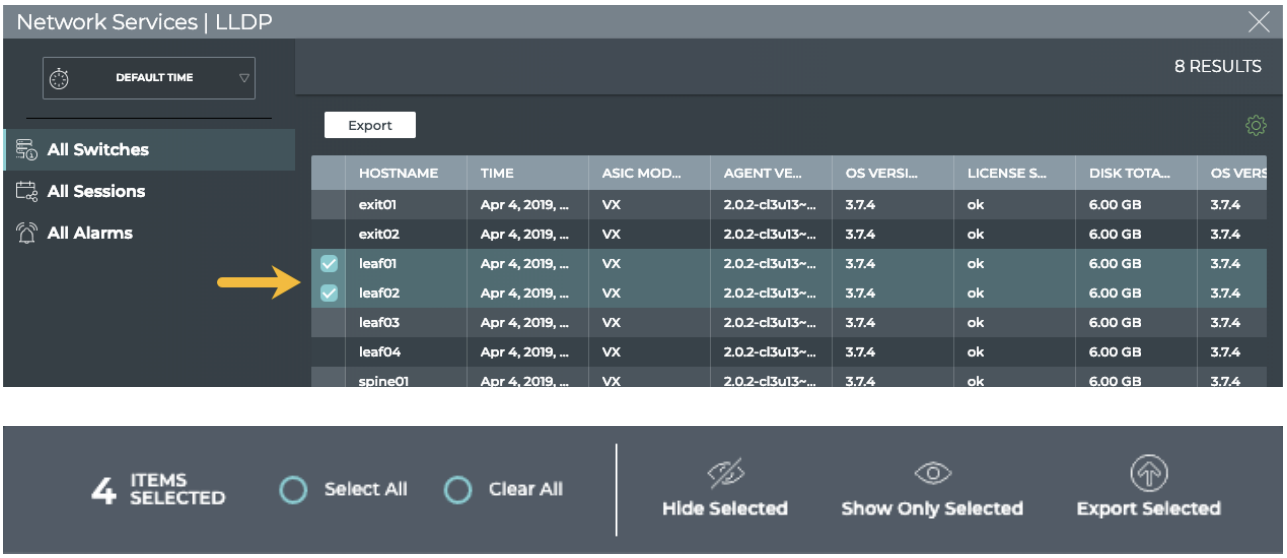


Return to your workbench by clicking in the top right corner.

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).



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 **Export** button.

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

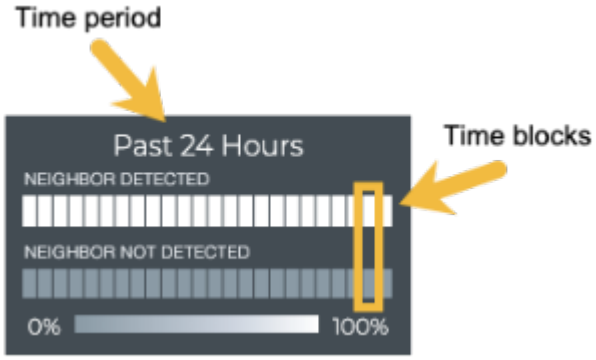
Monitor a Single LLDP Session

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.

To access the single session cards, you must open the full screen LLDP Service (all sessions) card and click on a session. Close the full screen card to view the medium single session card.

Granularity of Data Shown Based on Time Period

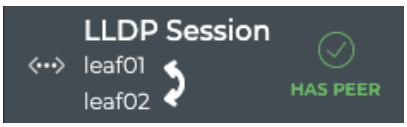
On the medium and large single LLDP session cards, the status of the neighboring peers is represented in heat maps stacked vertically; one for peers that are reachable (neighbor detected), and one for peers that are unreachable (neighbor not detected). Depending on the time period of data on the card, 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.



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

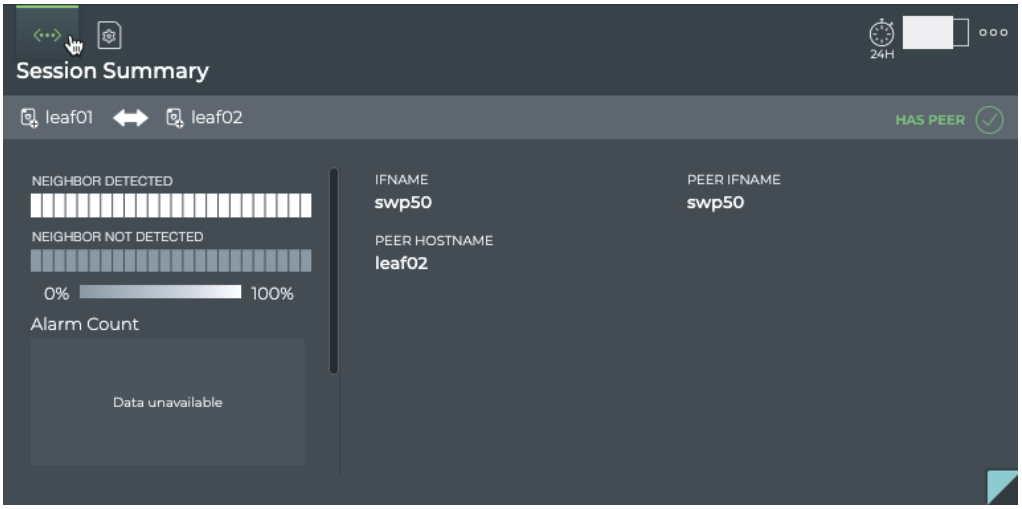
The medium LLDP Session card displays:

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
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

Item	Description
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.

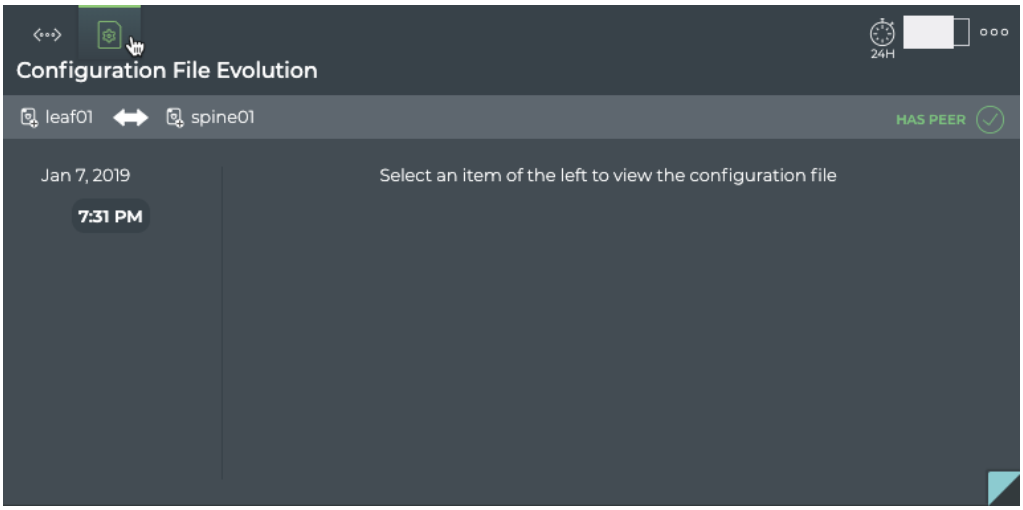
The *Session Summary* tab displays:



	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	**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

	Description
Host Interface Name	Software interface on the host 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

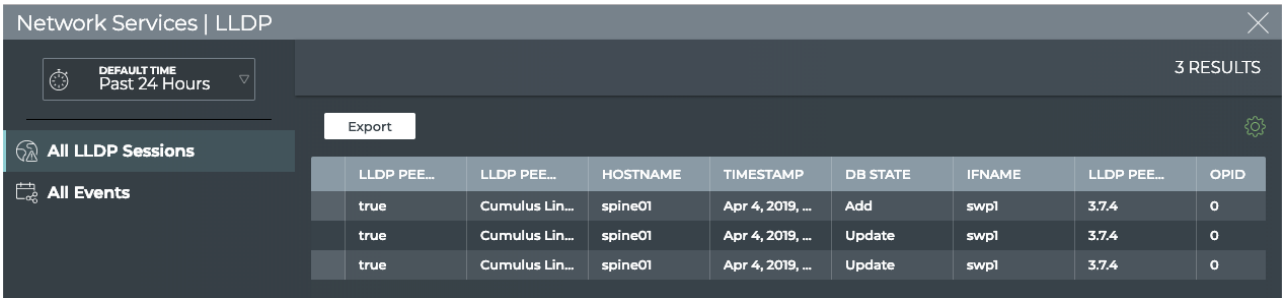
The *Configuration File Evolution* tab displays:



Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
⟷	Indicates data is 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 on to open associated device card.
,	Indication of detected peer, Has Peer or 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	When **File** is selected, the configuration file as it was at the selected time is shown. When **Diff** 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.

Item	Description
	Note: If no configuration file changes have been made, the card shows no results.

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



Item	Description
Title	Network Services | LLDP
✕	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 LLDP Sessions tab	Displays all LLDP sessions on the host device. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session:
	• **DB State**: Session state of the DB.
	• **Ifname**: Name of the host interface where LLDP session is running
	• **LLDP Peer**:
	  • Os: Operating system (OS) used by peer device. Values include Cumulus Linux, RedHat, Ubuntu, and CentOS.
	  • Osv: Version of the OS used by peer device. Example values include 3.7.3, 2.5.x, 16.04, 7.1.
	  • Bridge: Indicates whether the peer device is a bridge (true) or not (false)
	  • Router: Indicates whether the peer device is a router (true) or not (false)
	  • Station: Indicates whether the peer device is a station (true) or not (false)
	• **OPID**: LLDP service identifier
	• **Peer**:
	  • Hostname: User-defined name for the peer device
	  • Ifname: Name of the peer interface where the session is running
	• **Timestamp**: Date and time that the session was started, deleted, updated, or marked dead (device is down)

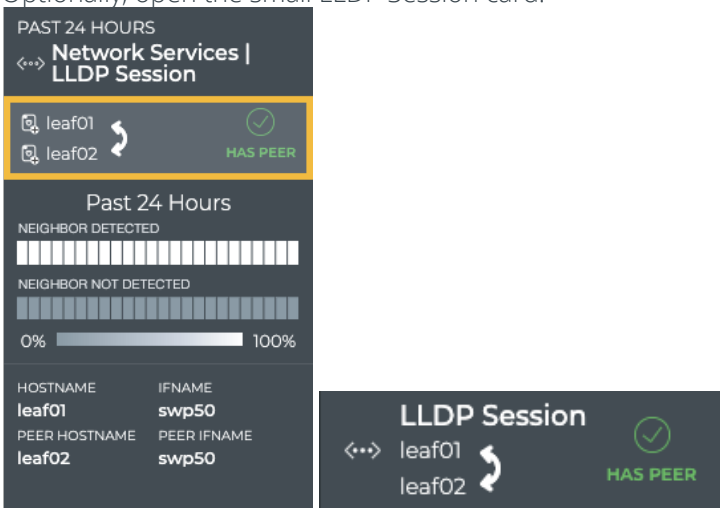
Item	Description
All Events tab	Displays all events network-wide. By default, the event list is sorted by **time**, with the most recent events listed first. The tab provides the following additional data about each event: • **Message**: Text description of an event. Example: LLDP Session with host leaf02 swp6 modified fields leaf06 swp21 • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *lldp* in this card workflow.
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.



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.

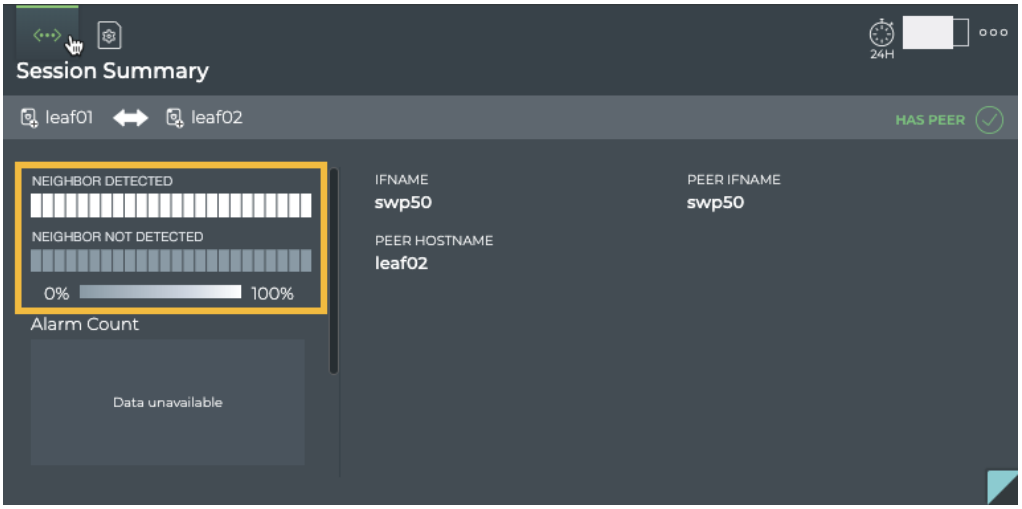
To view the neighbor availability for a given LLDP session on the medium card:

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.

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.

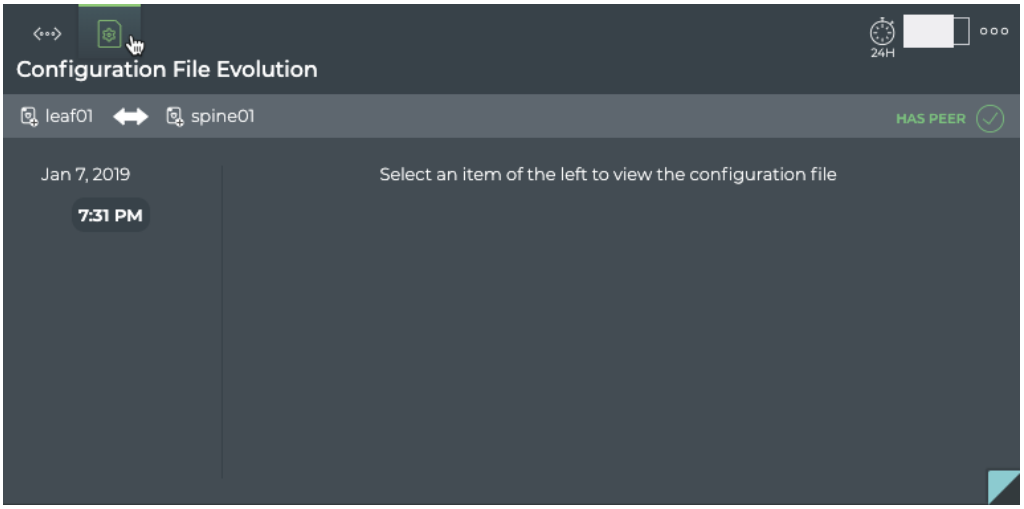
View Changes to the LLDP Service Configuration File

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.

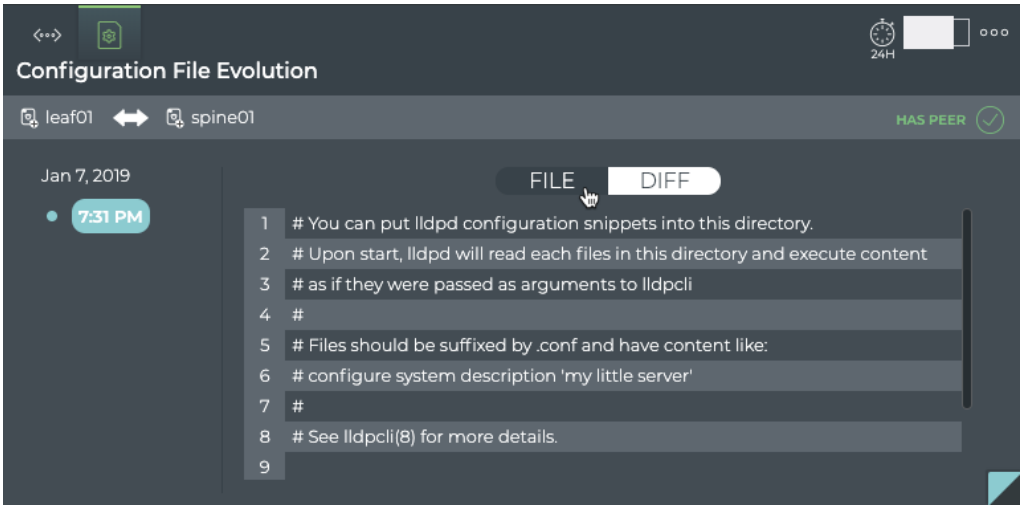
To view the configuration file changes:

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

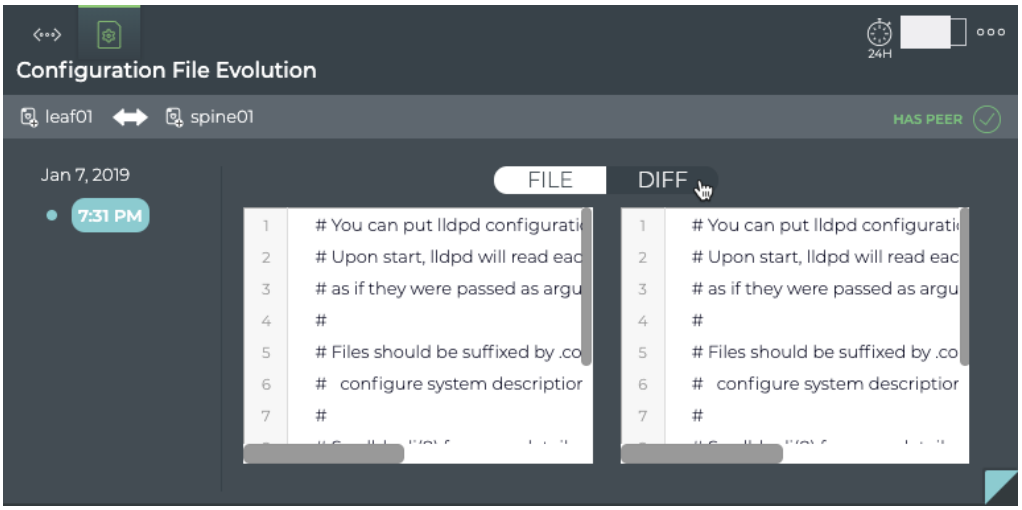
   to open the **LLDP Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.



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.



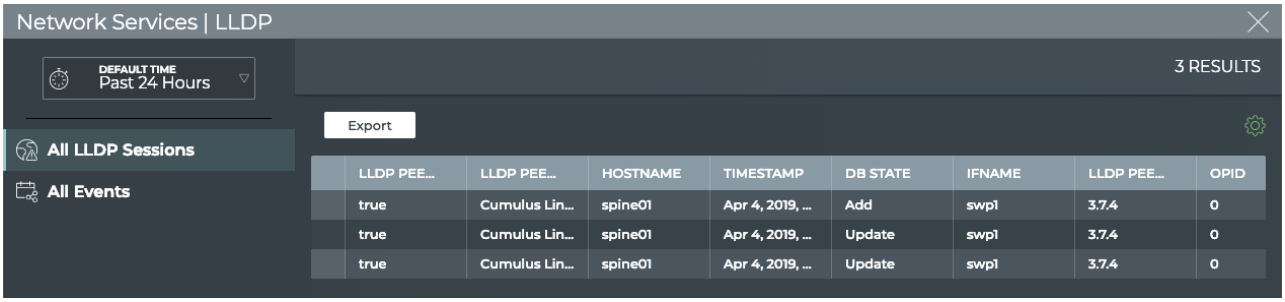
The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted in red and green. In this example, we don't have any changes to the file, so the same file is shown on both sides, and thus no highlighted lines.



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.



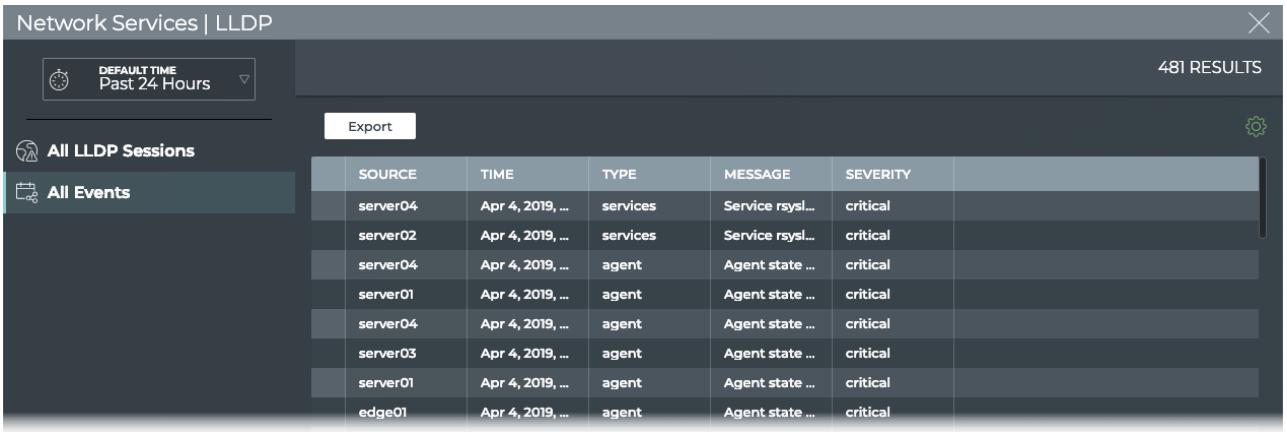
To return to your workbench, click

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.



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.

MLAG or CLAG?

The Cumulus Linux implementation of MLAG is referred to by other vendors as CLAG, MC-LAG or VPC. The Cumulus NetQ UI uses the CLAG terminology.

Contents

This topic describes how to...

Monitor the CLAG Service (All Sessions)

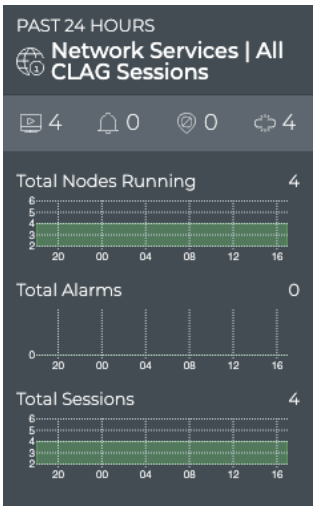
With NetQ, you can monitor the number of nodes running the CLAG service, view sessions running, and view alarms triggered by the CLAG service. For an overview and how to configure CLAG in your data center network, refer to Multi-Chassis Link Aggregation - MLAG.

CLAG Service Card Workflow Summary

The small CLAG Service card displays:

Item	Description
	Indicates data is for all sessions of a Network Service or Protocol
Title	**CLAG**: All CLAG Sessions, or the CLAG Service
	Total number of switches with the CLAG service enabled during the designated time period
	Total number of CLAG-related alarms received during the designated time period
Chart	Distribution of CLAG-related alarms received during the designated time period

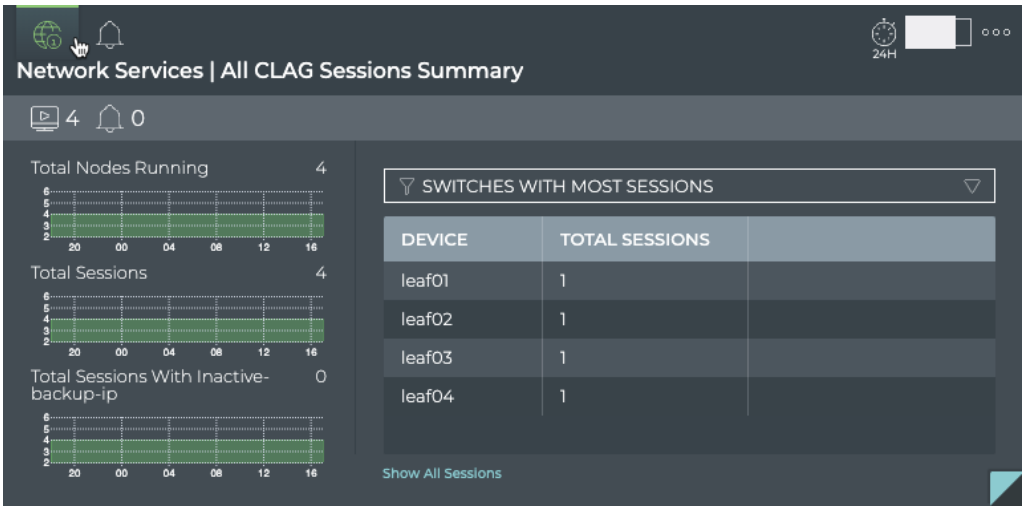
The medium CLAG Service card displays:



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
Title	Network Services | All CLAG Sessions
	Total number of switches with the CLAG service enabled during the designated time period
	Total number of CLAG-related alarms received during the designated time period
	Total number of sessions with an inactive backup IP address
	Total number of bonds with only a single connection
Total Nodes Running chart	Total number and distribution of switches with CLAG service enabled during the designated time period
Total Alarms chart	Total number and distribution of CLAG-related alarms received during the designated time period
Total Sessions chart	Total number and distribution of CLAG sessions network-wide during the designated time period

The large CLAG service card contains two tabs.

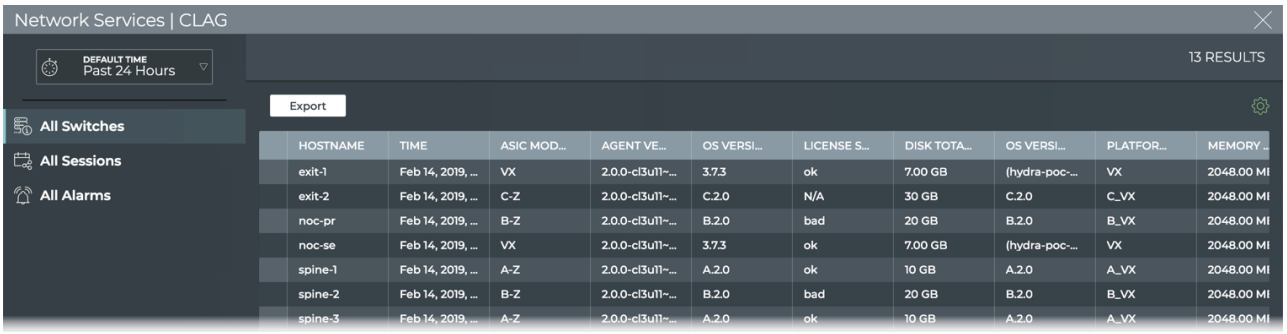
The *All CLAG Sessions Summary* tab which displays:



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	All CLAG Sessions Summary
	Total number of switches with the CLAG service enabled during the designated time period
	Total number of CLAG-related alarms received during the designated time period
Total Nodes Running chart	Total number and distribution of switches with CLAG service enabled during the designated time period
Total Sessions chart	Total number and distribution of CLAG sessions network-wide during the designated time period
Total Sessions with Inactive-backup-ip chart	Total number and distribution of sessions without an active backup IP defined
Table/Filter options	When the **SWITCHES WITH MOST SESSIONS** filter is selected, the table displays switches running CLAG sessions in decreasing order of session count—devices with the largest number of sessions are listed first When the **SWITCHES WITH MOST UNESTABLISHED SESSIONS** filter is selected, the table displays switches running CLAG sessions in decreasing order of unestablished session count—devices with the largest number of unestablished sessions are listed first

Item	Description
Show All Sessions	Link to view all CLAG sessions in the full screen card

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



Item	Description
Title	Network Services | CLAG
✕	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	Displays all switches and hosts running the CLAG service. By default, the device list is sorted by **hostname**. This tab provides the following additional data about each device:
	• **Agent**
	  • State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).
	  • 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.
	• **ASIC**
	  • Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.
	  • Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.
	  • Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.
	  • Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.

Item	Description

	• Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.
	• **CPU**
	  • Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.
	  • Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.
	  • Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.
	  • Nos: Number of cores. Example values include 2, 4, and 8.
	• **Disk Total Size**: Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.
	• **License State**: Indicator of validity. Values include ok and bad.
	• **Memory Size**: Total amount of local RAM. Example values include 8192 MB and 2048 MB.
	• **OS**
	  • Vendor: Operating System manufacturer. Values include Cumulus Networks, RedHat, Ubuntu, and CentOS.
	  • Version: Software version number of the OS. Example values include 3.7.3, 2.5.x, 16.04, 7.1.
	  • Version Id: Identifier of the OS version. For Cumulus, this is the same as the *Version* (3.7.x).
	• **Platform**
	  • Date: Date and time the platform was manufactured. Example values include 7/12/18 and 10/29/2015.
	  • MAC: System MAC address. Example value: 17:01:AB:EE:C3:F5.
	  • Model: Manufacturer's model name. Examples values include AS7712-32X and S4048-ON.
	  • Number: Manufacturer part number. Examples values include FP3ZZ7632014A, 0J09D3.
	  • Revision: Release version of the platform
	  • Series: Manufacturer serial number. Example values include D2060B2F044919GD000060, CN046MRJCES0085E0004.
	  • Vendor: Manufacturer of the platform. Example values include Cumulus Express, Dell, EdgeCore, Lenovo, Mellanox.
	• **Time:** Date and time the data was collected from device.

All Sessions tab	Displays all CLAG sessions network-wide. By default, the session list is sorted by hostname. This tab provides the following additional data about each session: • **Backup Ip**: IP address of the interface to use if the peerlink (or bond) goes down

Item	Description

	• **Backup Ip Active**: Indicates whether the backup IP address has been specified and is active (true) or not (false)
	• **Bonds**
	  • Conflicted: Identifies the set of interfaces in a bond that do not match on each end of the bond
	  • Single: Identifies a set of interfaces connecting to only one of the two switches
	  • Dual: Identifies a set of interfaces connecting to both switches
	  • Proto Down: Interface on the switch brought down by the `clagd` service. Value is blank if no interfaces are down due to `clagd` service.
	• **Clag Sysmac**: Unique MAC address for each bond interface pair. **Note**: Must be a value between 44:38:39:ff:00:00 and 44:38:39:ff:ff:ff.
	• **DB State**: Session state of the DB.
	• **OPID**: CLAG service identifier
	• **Peer**:
	  • If: Name of the peer interface
	  • Role: Role of the peer device. Values include primary and secondary.
	  • State: Indicates if peer device is up (true) or down (false)
	• **Role**: Role of the host device. Values include primary and secondary.
	• **Timestamp**: Date and time the CLAG session was started, deleted, updated, or marked dead (device went down)
	• **Vxlan Anycast**: Anycast IP address used for VXLAN termination

All Alarms tab	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: • **Message**: Text description of a BGP-related event. Example: Clag conflicted bond changed from swp7 swp8 to @swp9 swp10 • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *clag* in this card workflow.
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 CLAG service is available from the CLAG Service card workflow, including the number of nodes running the service, the number of CLAG-related alarms, and a distribution of those alarms.

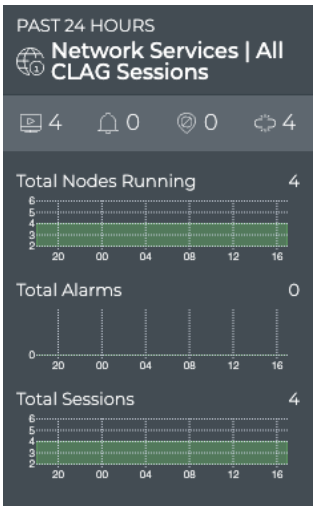
To view the summary, open the small CLAG Service card.

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

View the Distribution of Sessions and Alarms

It is useful to know the number of network nodes running the CLAG 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 CLAG with the alarms present at the same time to determine if there is any correlation between the issues and the ability to establish an CLAG session.

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



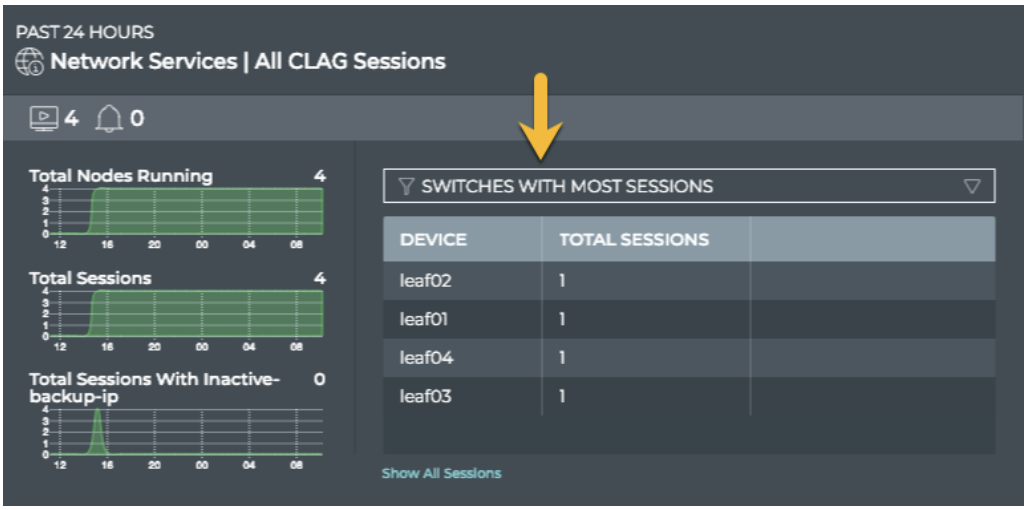
If a visual correlation is apparent, you can dig a little deeper with the large CLAG Service card tabs.

View Devices with the Most CLAG Sessions

You can view the load from CLAG on your switches using the large CLAG Service card. This data enables you to see which switches are handling the most CLAG 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.

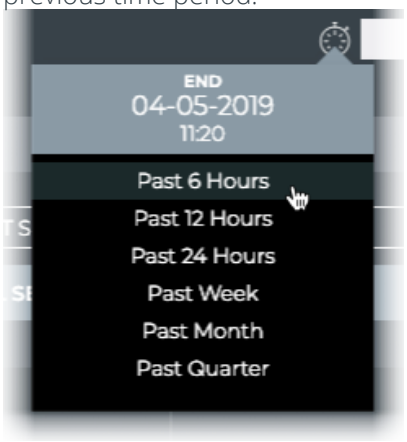
To view switches and hosts with the most CLAG sessions:

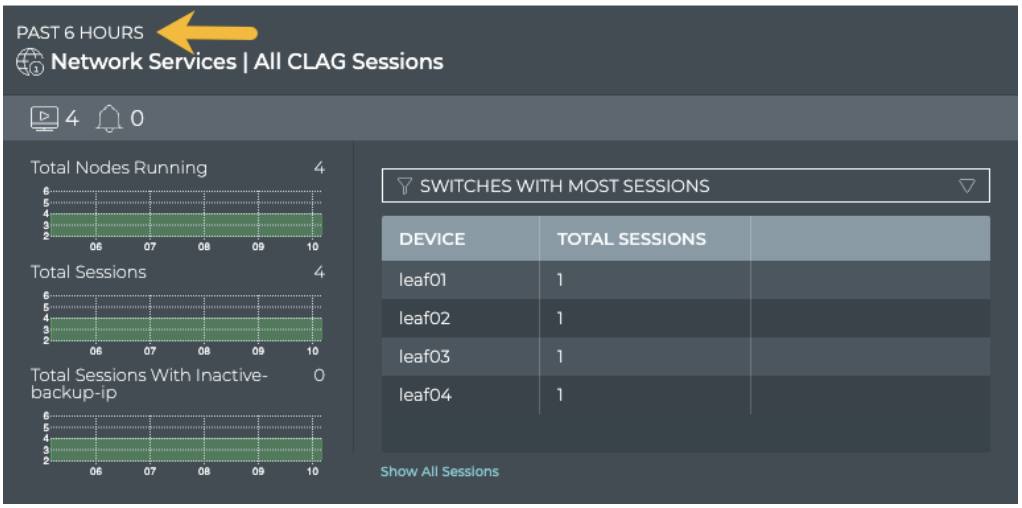
1. Open the large CLAG Service card.
2. Select **SWITCHES WITH MOST SESSIONS** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most CLAG sessions at the top. Scroll down to view those with the fewest sessions.



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

1. Open another large CLAG 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.





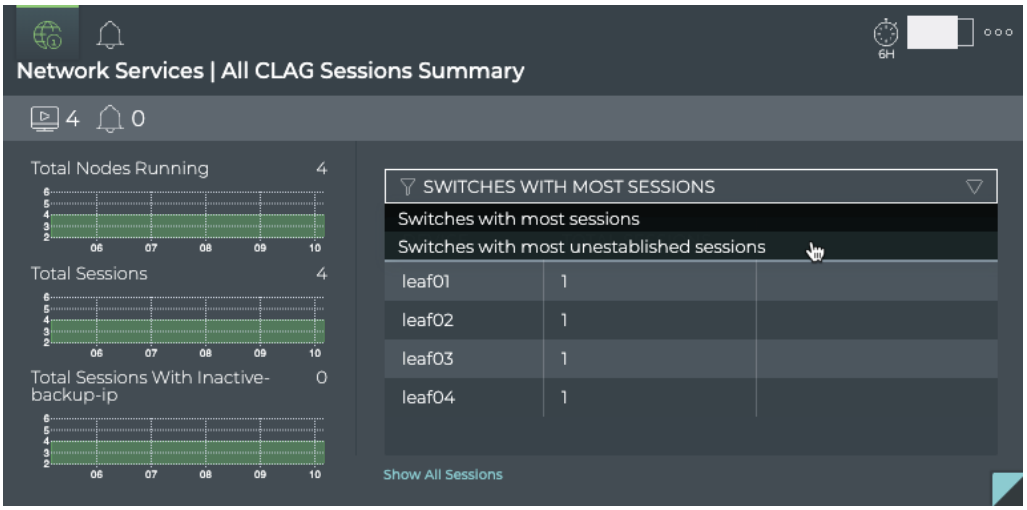
If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running CLAG than previously, looking for changes in the topology, and so forth.

View Devices with the Most Unestablished CLAG Sessions

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

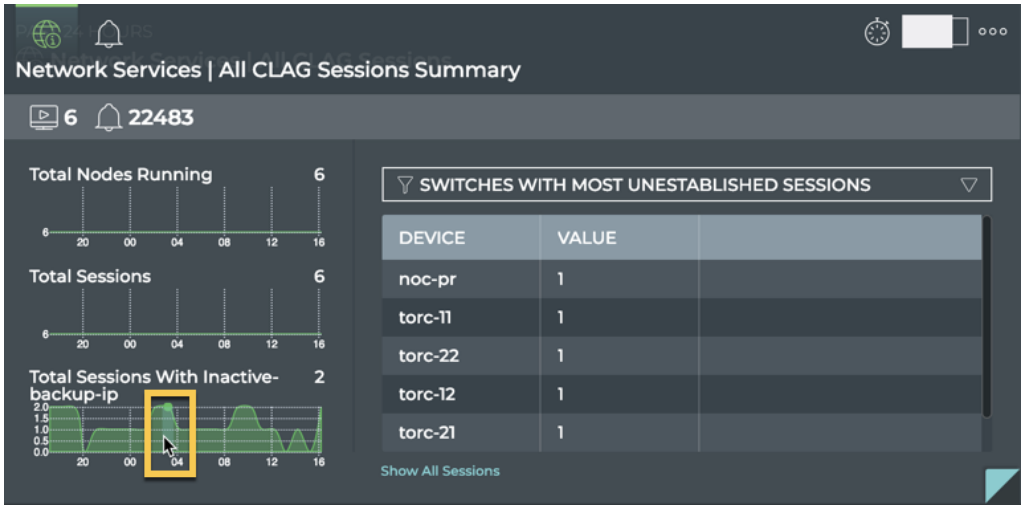
To view switches with the most unestablished CLAG sessions:

1. Open the large CLAG 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.

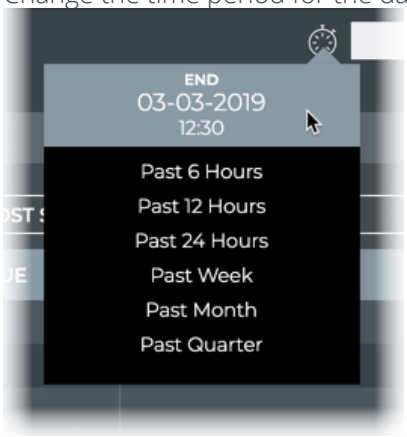


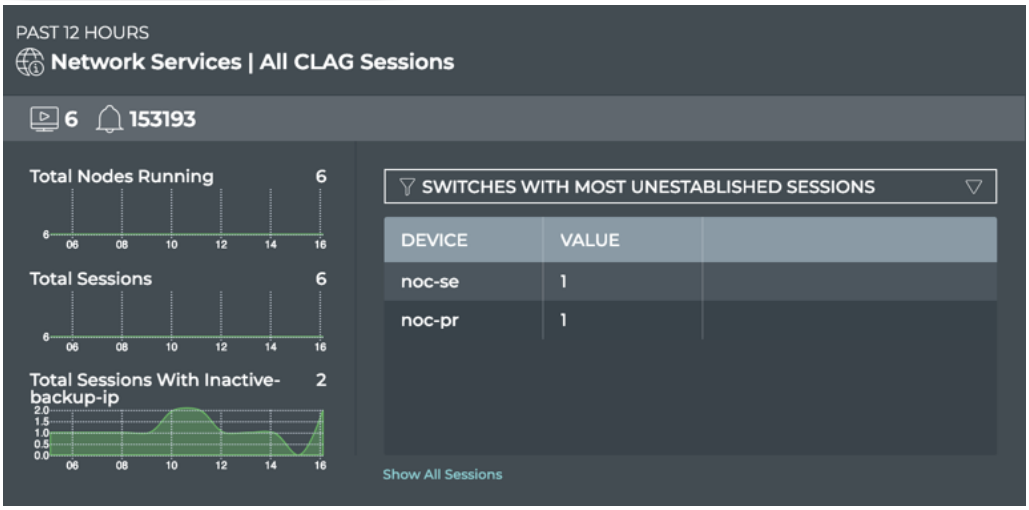
Where to go next depends on what data you see, but a few options include:

- Hover over the any of the charts to focus on the number of switches or sessions with the chart characteristic 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 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 (see page 258).

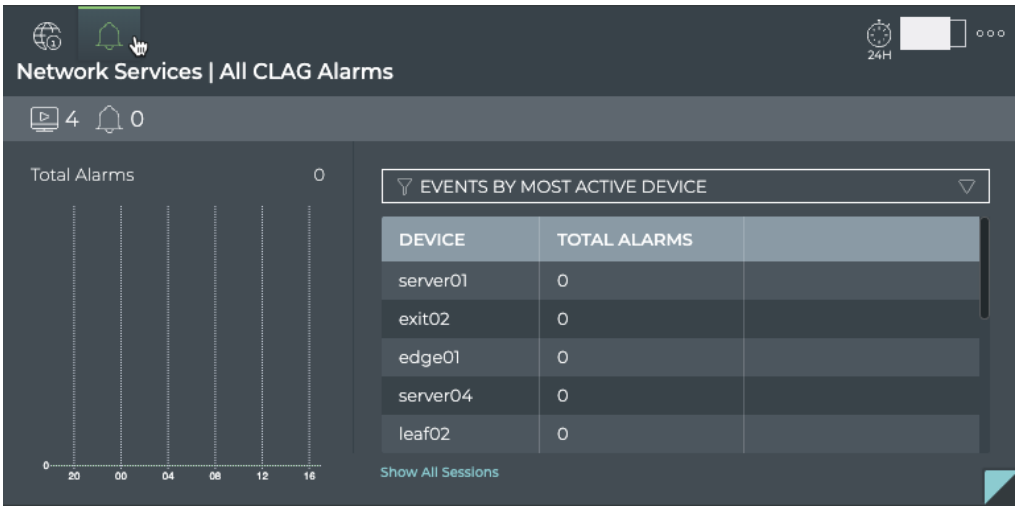
- Click **Show All Sessions** to investigate all CLAG sessions with events in the full screen card.

View Switches with the Most CLAG-related Alarms

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

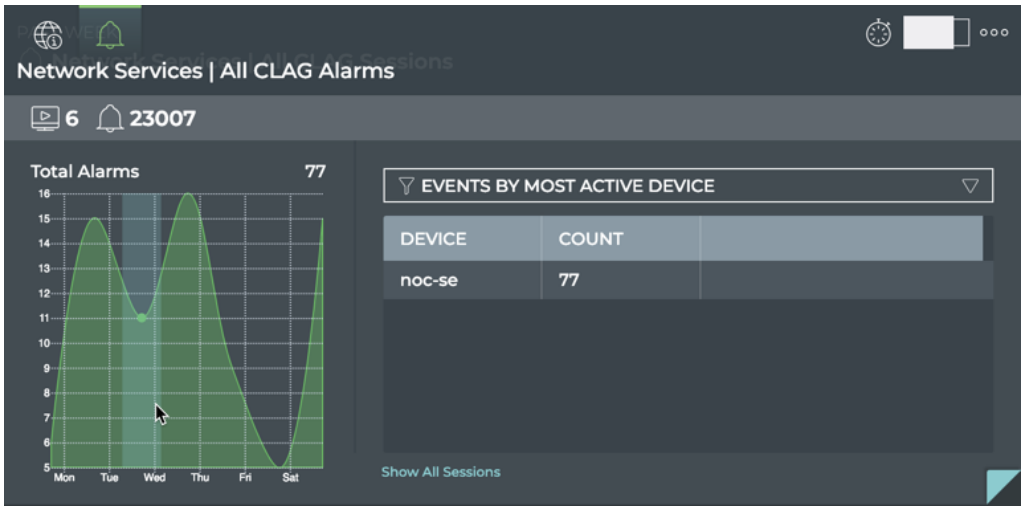
To view switches with most CLAG alarms:

1. Open the large CLAG Service card.
2. Hover over the header and click .
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 CLAG alarms at the top. Scroll down to view those with the fewest alarms.

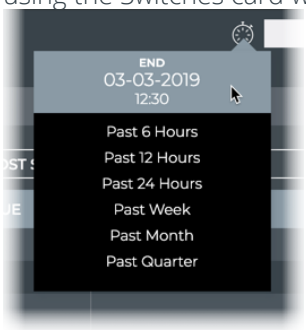


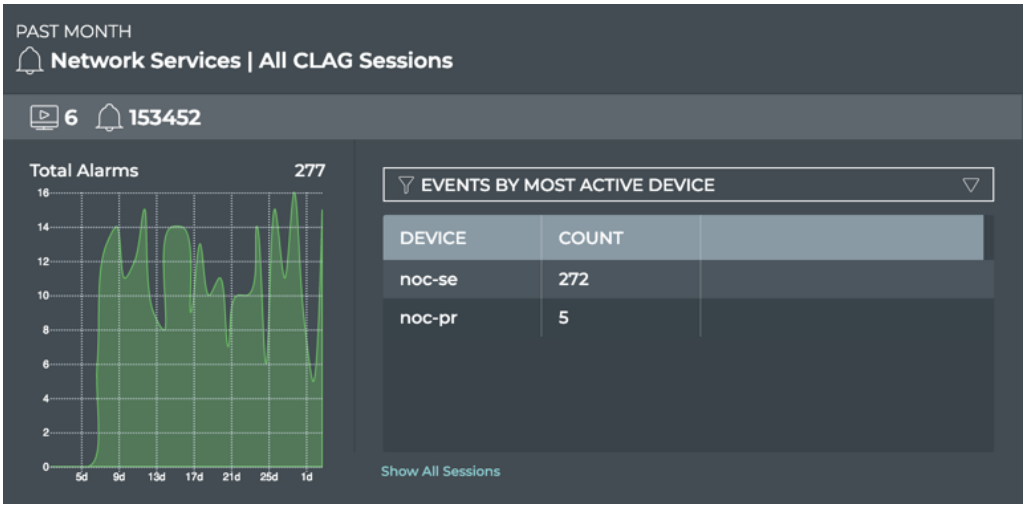
Where to go next depends on what data you see, but a few options include:

- 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.





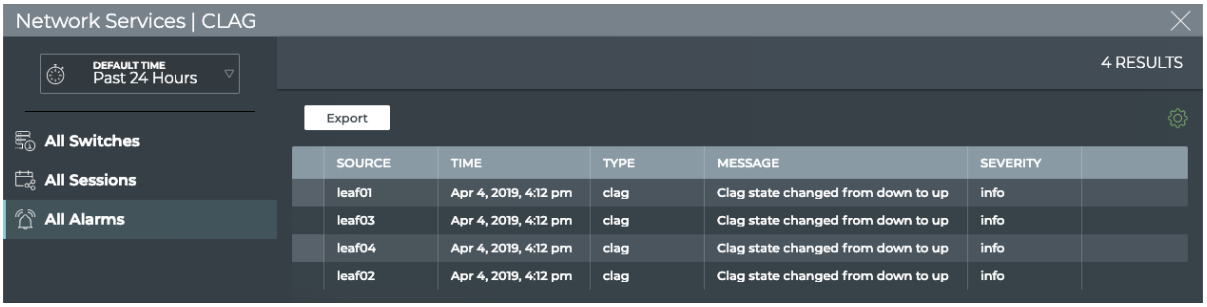
- Click **Show All Sessions** to investigate all CLAG sessions with alarms in the full screen card.

View All CLAG Events

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

To view all CLAG events:

1. Open the full screen CLAG Service card.
2. Click **All Alarms** tab.



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:

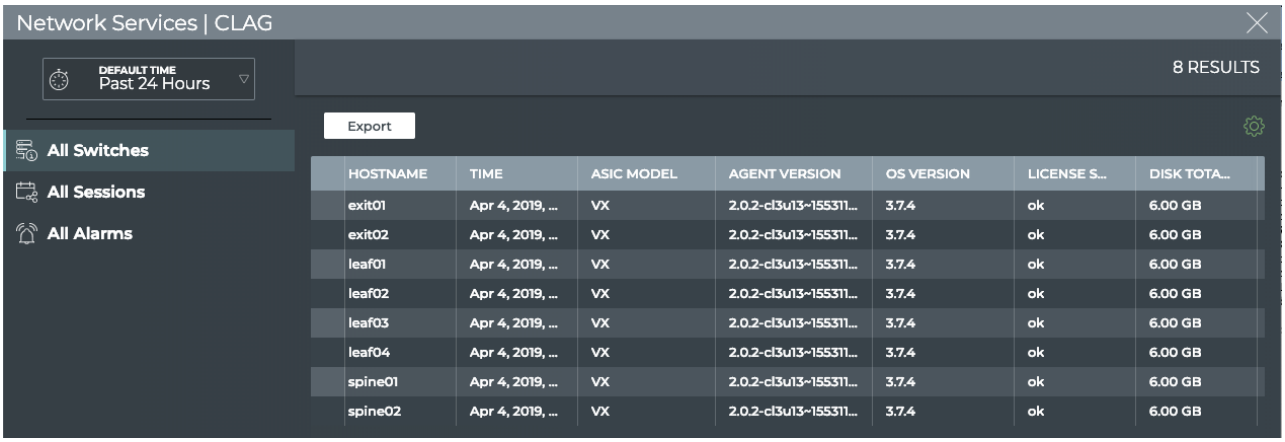
- by **Message** to determine the frequency of particular events
- by **Severity** to determine the most critical events
- by **Time** to find events that may have occurred at a particular time to try to correlate them with other system events

- 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 Detailed Information About All Switches Running CLAG

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

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

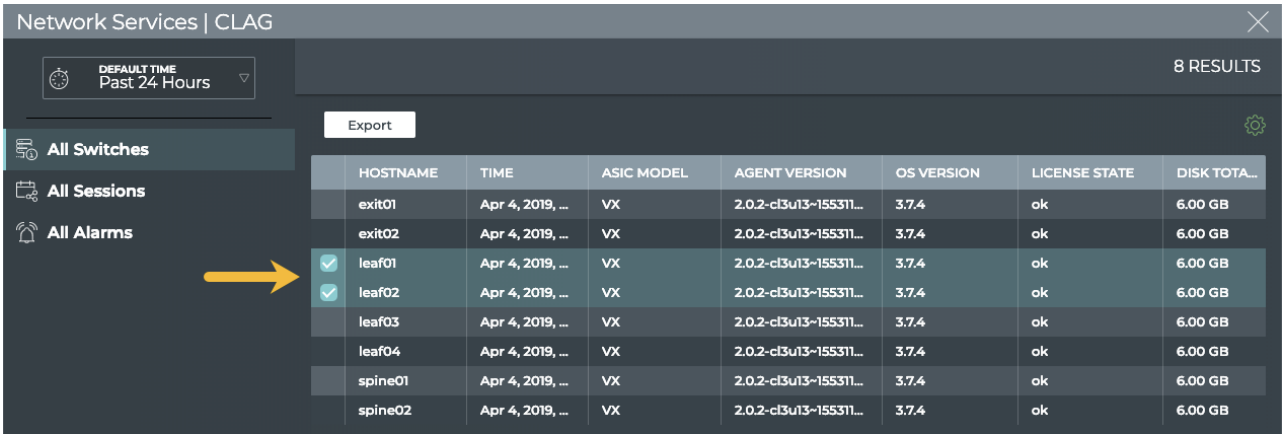


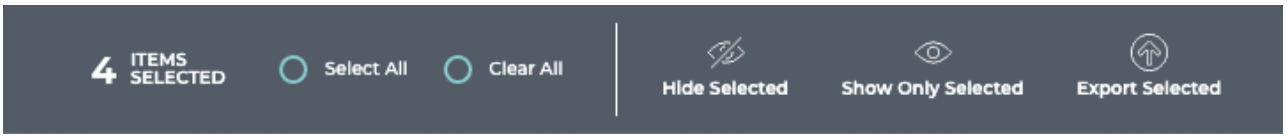
To return to your workbench, click in the top right corner.

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).





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 **Export** button.

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

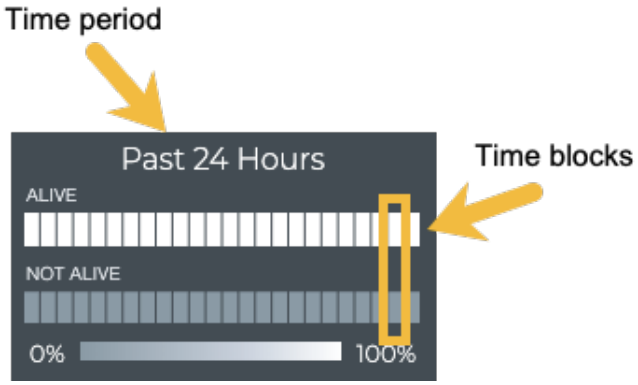
Monitor a Single CLAG Session

With NetQ, you can monitor the number of nodes running the CLAG service, view switches with the most peers alive and not alive, and view alarms triggered by the CLAG service. For an overview and how to configure CLAG in your data center network, refer to Multi-Chassis Link Aggregation - MLAG.

> To access the single session cards, you must open the full screen CLAG Service (all sessions) card and double-click on a session.

Granularity of Data Shown Based on Time Period

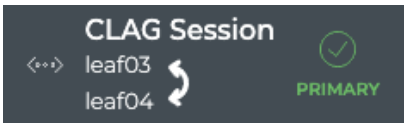
On the medium and large single CLAG session cards, the status of the peers is represented in heat maps stacked vertically; one for peers that are reachable (alive), and one for peers that are unreachable (not alive). Depending on the time period of data on the card, the number of smaller time blocks 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

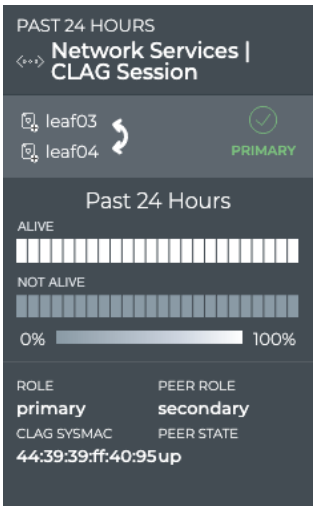
CLAG Session Card Workflow Summary

The small CLAG Session card displays:



Item	Description
⇿	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 ⛨

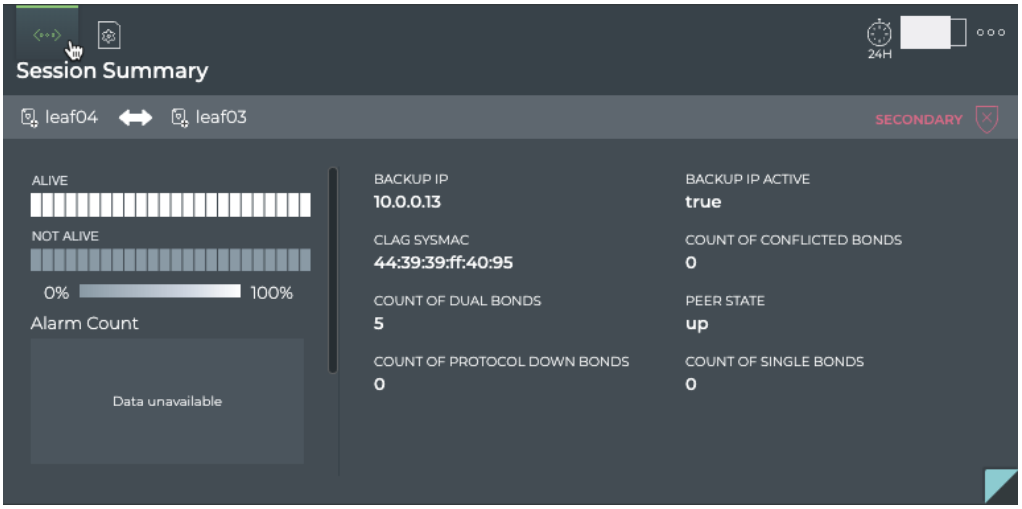
The medium CLAG Session card displays:



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 | CLAG Session
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Arrow points from the host to the peer. Click on to open associated device card.
,	Indication of host role, primary or secondary
Time period	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.
CLAG sysmac	System MAC address of the CLAG 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 CLAG Session card contains two tabs.

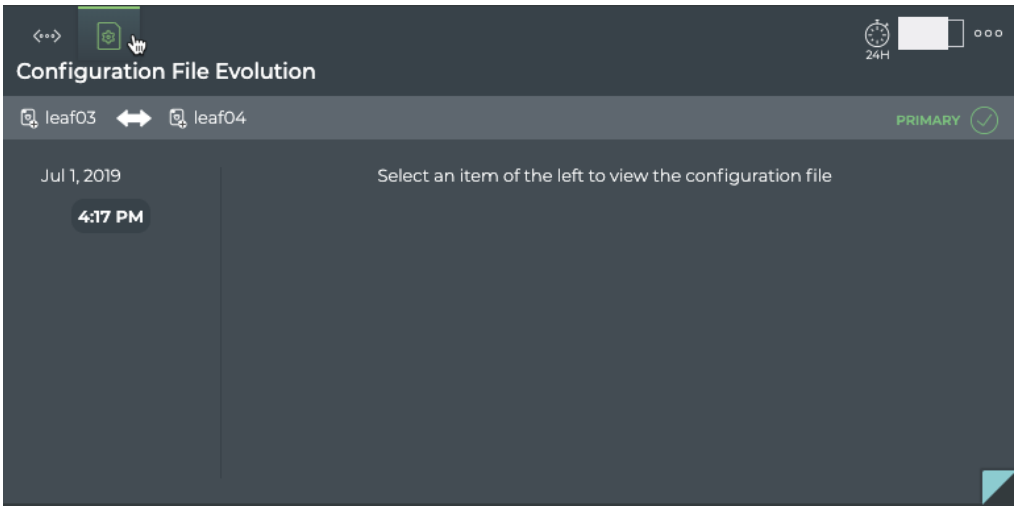
The *Session Summary* tab displays:



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
Title	(Network Services | CLAG 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 on 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 CLAG 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

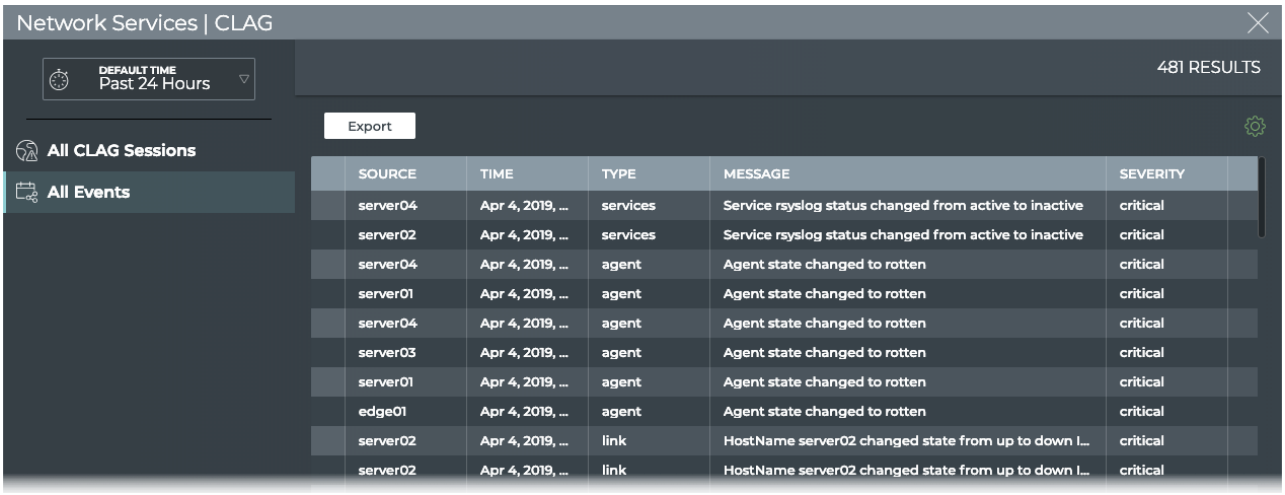
The *Configuration File Evolution* tab displays:



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

Item	Description
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 **File** is selected, the configuration file as it was at the selected time is shown. When **Diff** 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. **Note**: If no configuration file changes have been made, the card shows no results at all.

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



Item	Description
Title	Network Services | CLAG
✕	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 CLAG Sessions tab	Displays all CLAG sessions for the given session. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session: • **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 has been specified and is active (true) or not (false) • **Bonds** • Conflicted: Identifies the set of interfaces in a bond that do not match on each end of the bond

Item	Description
	• Single: Identifies a set of interfaces connecting to only one of the two switches • Dual: Identifies a set of interfaces connecting to both switches • Proto Down: Interface on the switch brought down by the `clagd` service. Value is blank if no interfaces are down due to `clagd` service. • **Clag Sysmac**: Unique MAC address for each bond interface pair. **Note**: Must be a value between 44:38:39:ff:00:00 and 44:38:39:ff:ff:ff. • **DB State**: Session state of the DB. • **OPID**: CLAG service identifier • **Peer**: • If: Name of the peer interface • Role: Role of the peer device. Values include primary and secondary. • State: Indicates if peer device is up (true) or down (false) • **Role**: Role of the host device. Values include primary and secondary. • **Timestamp**: Date and time the CLAG session was started, deleted, updated, or marked dead (device went down) • **Vxlan Anycast**: Anycast IP address used for VXLAN termination
All Events tab	Displays all 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: • **Message**: Text description of an event. Example: Clag conflicted bond changed from swp7 swp8 to @swp9 swp10 • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *clag* in this card workflow.
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

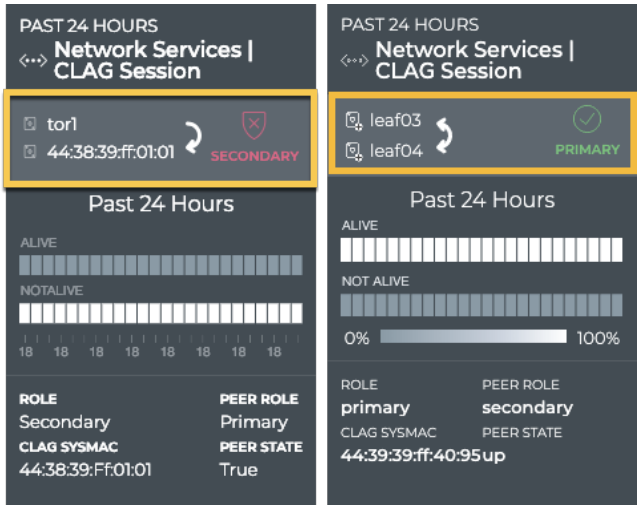
View Session Status Summary

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

To view the summary:

1. Open the full screen CLAG Service card.
2. Select a session from the listing to view.

3. Close the full screen card to view the medium CLAG Session card.



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 CLAG Session Peering State Changes

You can view the peering state for a given CLAG session from the medium and large CLAG Session cards. For a given time period, you can determine the stability of the CLAG 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.

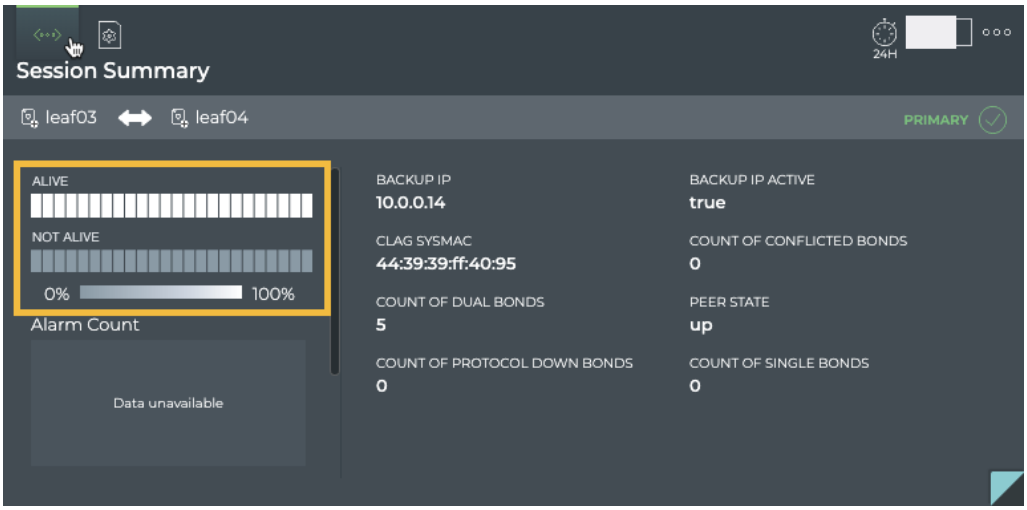
To view the state transitions for a given CLAG session:

1. Open the full screen CLAG Service card.
2. Select a session from the listing to view.
3. Close the full screen card to view the medium CLAG 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 CLAG system MAC address which identify the session in more detail.

To view the peering state transitions for a given CLAG session on the large CLAG 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, CLAG 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.

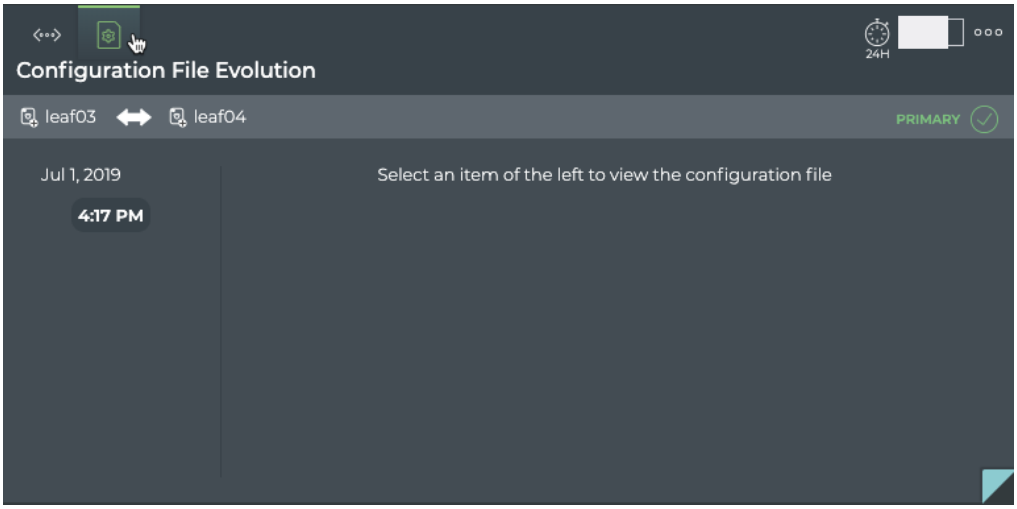
View Changes to the CLAG Service Configuration File

Each time a change is made to the configuration file for the CLAG 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.

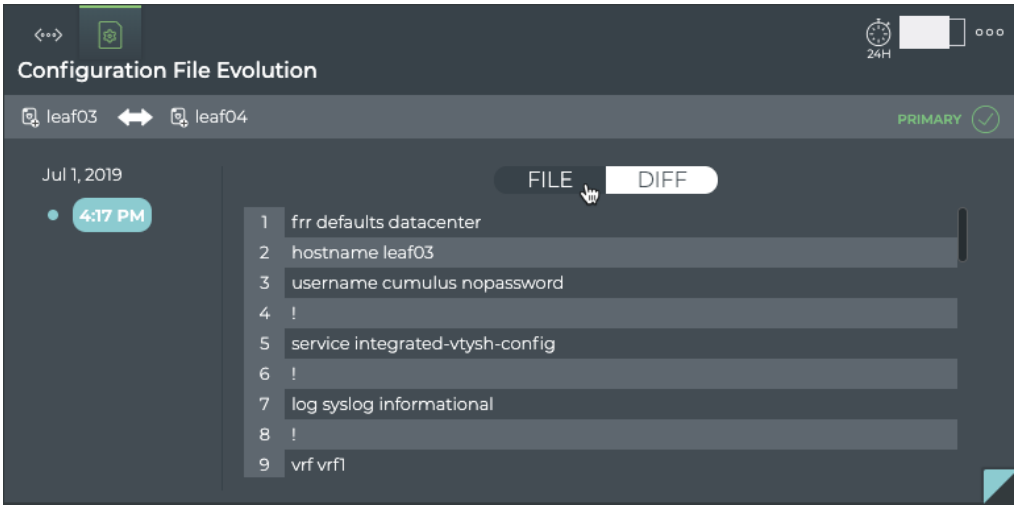
To view the configuration file changes:

1. Open the large CLAG Session card.
2. Hover over the card and click 

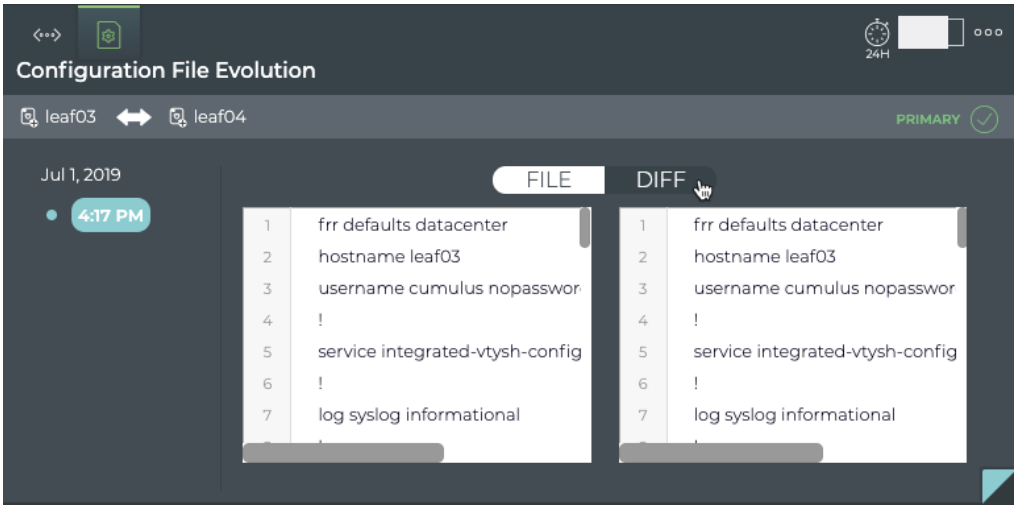
   to open the **Configuration File Evolution** tab.
3. Select the time of interest on the left; when a change may have impacted the performance. Scroll down if needed.



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.



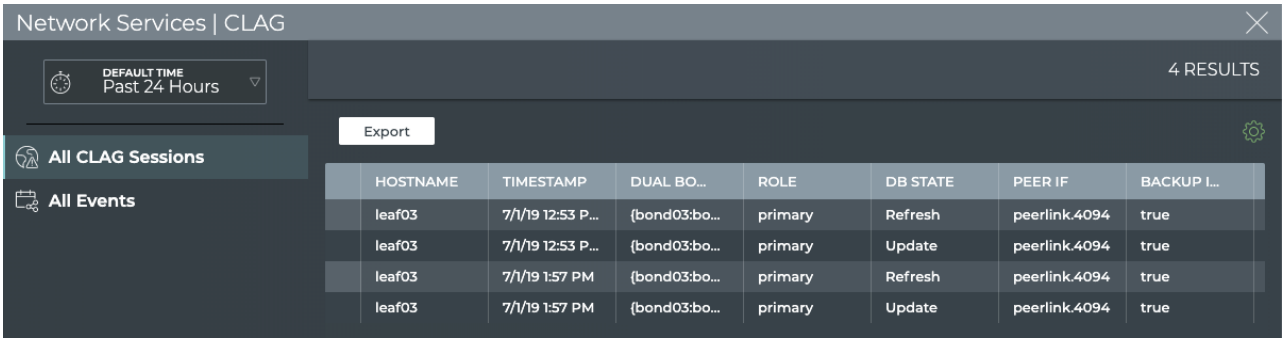
The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted in red and green. In this example, we don't have any changes after this first creation, so the same file is shown on both sides and no highlighting is present.



All CLAG Session Details

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

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



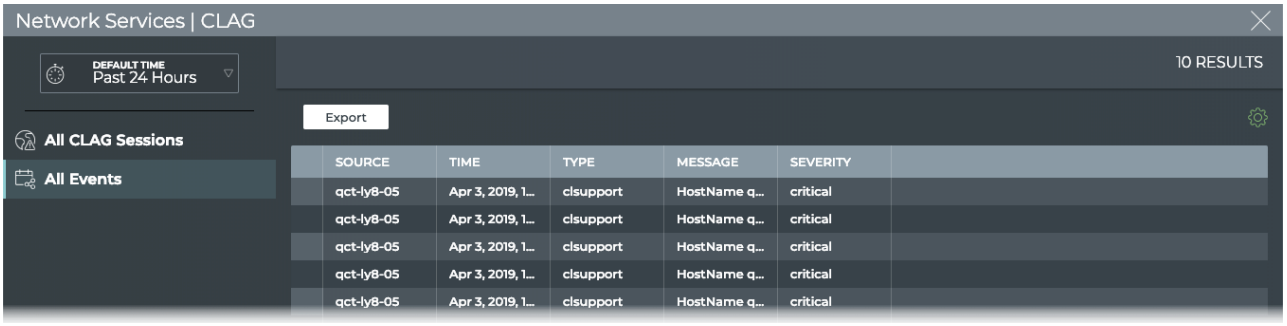
Where to go next depends on what data you see, but a few options include:

- Open the **All Events** tabs to look more closely at the alarm and info events fin 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 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 CLAG Session card, and click the **All Events** tab.



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

- Open the **All CLAG Sessions** tabs to look more closely at the individual sessions.
- 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.

Contents

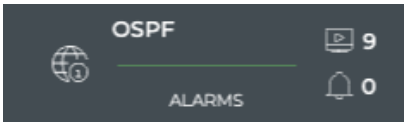
This topic describes how to...

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

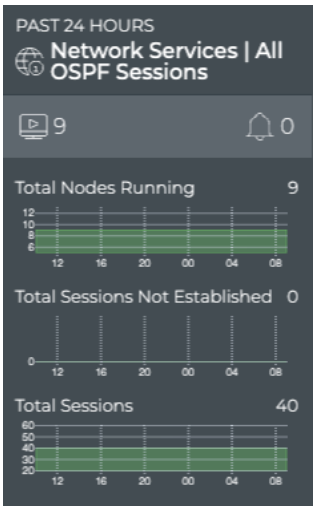
The small OSPF Service card displays:



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

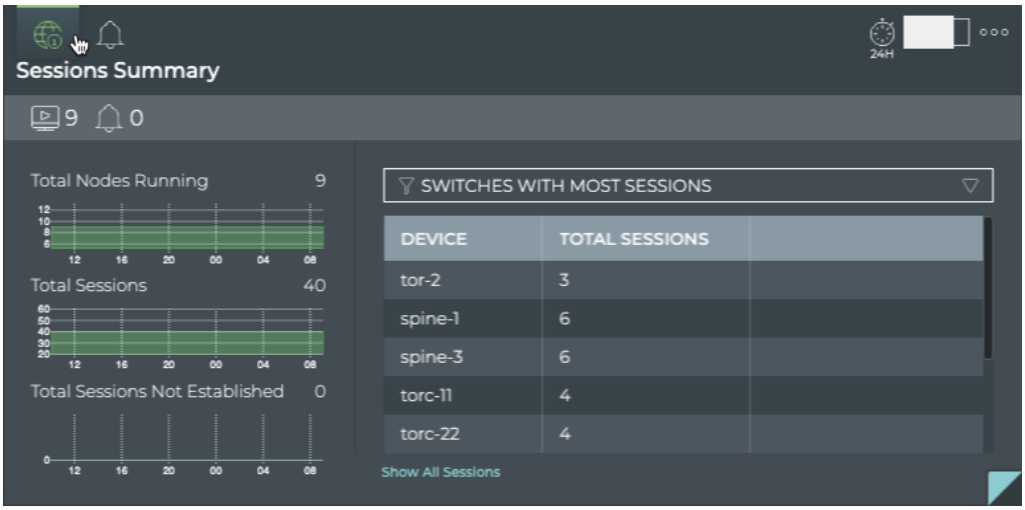
The medium OSPF Service card displays:



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
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	Total number and distribution of switches and hosts with the OSPF service enabled during the designated time period
Total Alarms chart	Total number and distribution of OSPF-related alarms received during the designated time period
Total Sessions chart	Total number and distribution of OSPF sessions during the designated time period

The large OSPF service card contains two tabs.

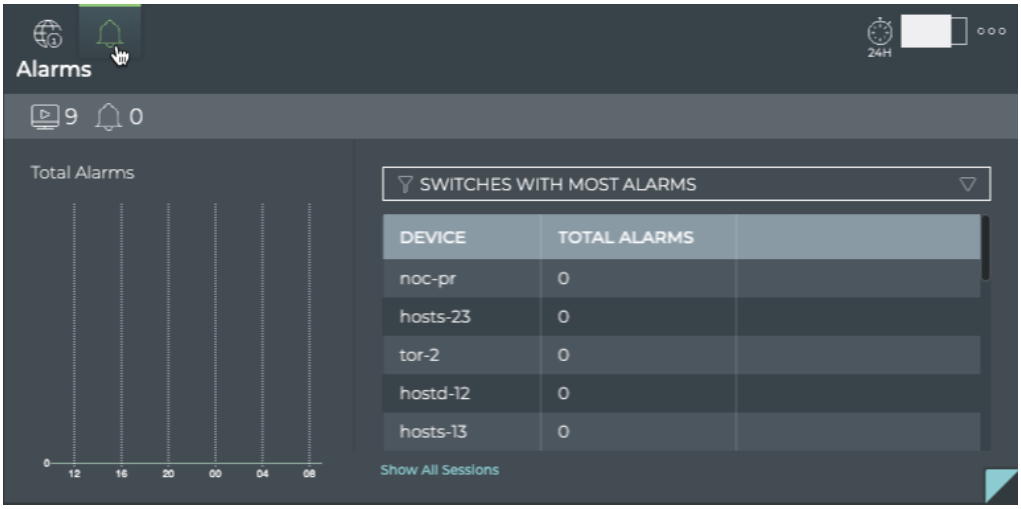
The *Sessions Summary* tab displays:



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)
	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	Total number and distribution of switches and hosts with the OSPF service enabled
Total Sessions chart	Total number and distribution of OSPF sessions during the designated time period
Total Nodes Not Est. chart	Total number and distribution of switches and hosts with unestablished OSPF sessions during the designated time period
Table /Filter options	When the **Switches with Most Sessions** 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

Item	Description
	When the **Switches with Most Unestablished Sessions** 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
Show All Sessions	Link to view data for all OSPF 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
	Indicates data is 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 OSPF service enabled during the designated time period
	Total number of OSPF-related alarms received during the designated time period
Total Alarms chart	Total number and distribution of OSPF-related alarms received during the designated time period
Table /Filter options	When the selected filter option is **Switches with Most Alarms**, 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

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

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

Item	Description
Title	Network Services | OSPF
✕	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	Displays all switches and hosts running the OSPF service. By default, the device list is sorted by **hostname**. This tab provides the following additional data about each device:
	• **Agent**
	  • State: Indicates communication state of the NetQ Agent on a given device. Values include Fresh (heard from recently) and Rotten (not heard from recently).
	  • 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.
	• **ASIC**
	  • Core BW: Maximum sustained/rated bandwidth. Example values include 2.0 T and 720 G.
	  • Model: Chip family. Example values include Tomahawk, Trident, and Spectrum.
	  • Model Id: Identifier of networking ASIC model. Example values include BCM56960 and BCM56854.
	  • Ports: Indicates port configuration of the switch. Example values include 32 x 100G-QSFP28, 48 x 10G-SFP+, and 6 x 40G-QSFP+.

Item	Description

	• Vendor: Manufacturer of the chip. Example values include Broadcom and Mellanox.
	• **CPU**
	  • Arch: Microprocessor architecture type. Values include x86_64 (Intel), ARMv7 (AMD), and PowerPC.
	  • Max Freq: Highest rated frequency for CPU. Example values include 2.40 GHz and 1.74 GHz.
	  • Model: Chip family. Example values include Intel Atom C2538 and Intel Atom C2338.
	  • Nos: Number of cores. Example values include 2, 4, and 8.
	• **Disk Total Size**: Total amount of storage space in physical disks (not total available). Example values: 10 GB, 20 GB, 30 GB.
	• **License State**: Indicator of validity. Values include ok and bad.
	• **Memory Size**: Total amount of local RAM. Example values include 8192 MB and 2048 MB.
	• **OS**
	  • Vendor: Operating System manufacturer. Values include Cumulus Networks, RedHat, Ubuntu, and CentOS.
	  • Version: Software version number of the OS. Example values include 3.7.3, 2.5.x, 16.04, 7.1.
	  • Version Id: Identifier of the OS version. For Cumulus, this is the same as the *Version* (3.7.x).
	• **Platform**
	  • Date: Date and time the platform was manufactured. Example values include 7/12/18 and 10/29/2015.
	  • MAC: System MAC address. Example value: 17:01:AB:EE:C3:F5.
	  • Model: Manufacturer's model name. Examples values include AS7712-32X and S4048-ON.
	  • Number: Manufacturer part number. Examples values include FP3ZZ7632014A, 0J09D3.
	  • Revision: Release version of the platform
	  • Series: Manufacturer serial number. Example values include D2060B2F044919GD000060, CN046MRJCES0085E0004.
	  • Vendor: Manufacturer of the platform. Example values include Cumulus Express, Dell, EdgeCore, Lenovo, Mellanox.
	• **Time:** Date and time the data was collected from device.

All Sessions tab	Displays all OSPF sessions network-wide. By default, the session list is sorted by **hostname**. This tab provides the following additional data about each session: • **Area**: Routing domain for this host device. Example values include 0.0.0.1, 0.0.0.23. • **DB State**: Session state of DB

Item	Description

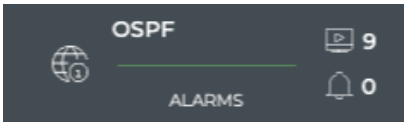
	• **Ifname**: Name of the interface on host device where session resides. Example values include swp5, peerlink-1.
	• **Is IPv6**: Indicates whether the address of the host device is IPv6 (true) or IPv4 (false)
	• **Peer**
	  • Address: IPv4 or IPv6 address of the peer device
	  • Hostname: User-defined name for peer device
	  • ID: Network subnet address of router with access to the peer device
	• **State**: Current state of OSPF. Values include Full, 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.
	• **Timestamp**: Date and time session was started, deleted, updated or marked dead (device is down)

All Alarms tab	Displays all OSPF 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: • **Message**: Text description of a OSPF-related event. Example: swp4 area ID mismatch with peer leaf02 • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of *OSPF* in this card workflow.
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.

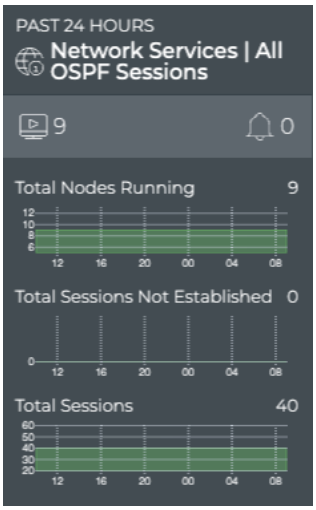


For more detail, select a different size OSPF Service card.

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.



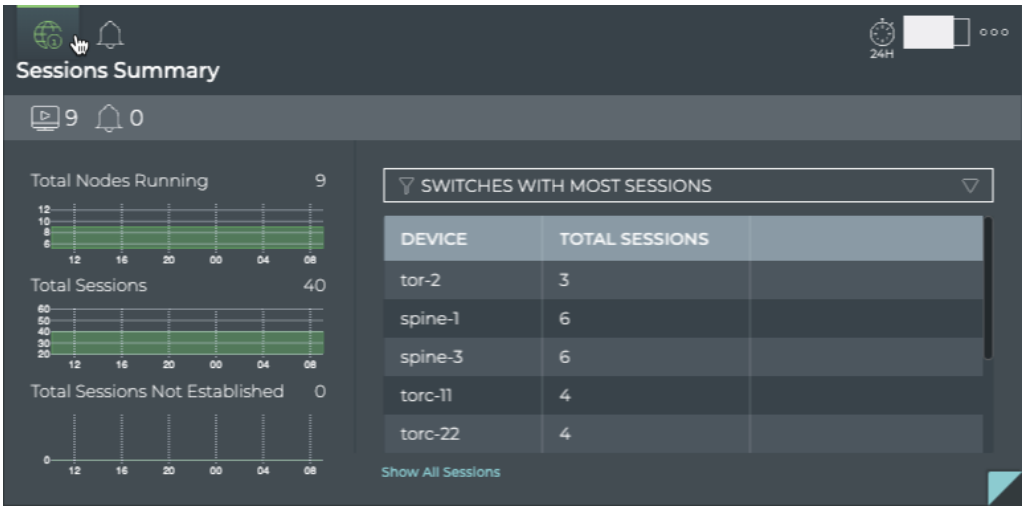
You can dig a little deeper with the large OSPF Service card tabs.

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:

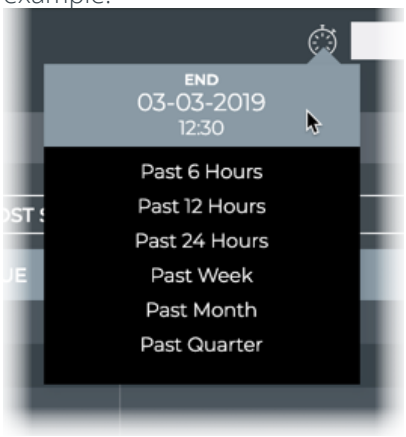
1. Open the large OSPF Service card.
2. Select **SWITCHES WITH MOST SESSIONS** from the filter above the table.
   The table content is sorted by this characteristic, listing nodes running the most OSPF sessions at the top. Scroll down to view those with the fewest sessions.

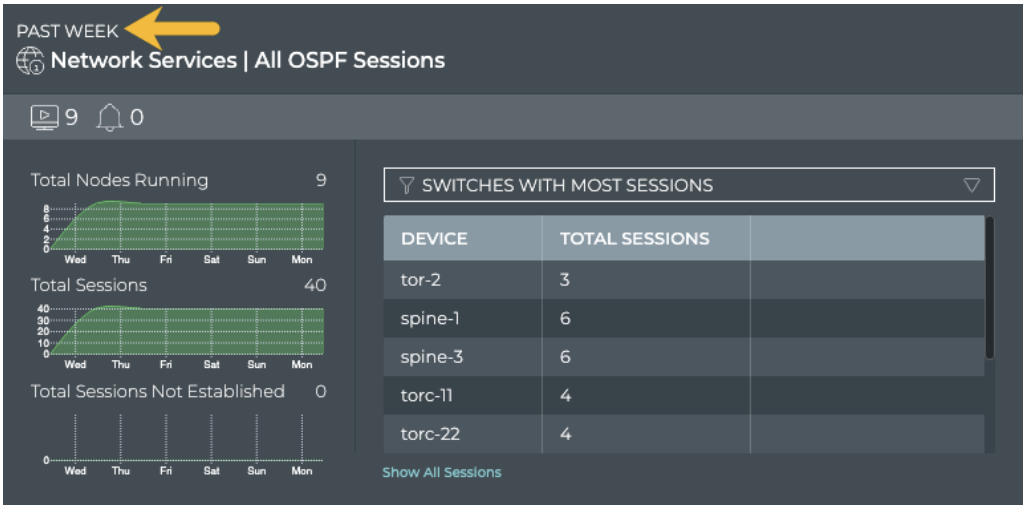


To compare this data with the same data at a previous time:

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.





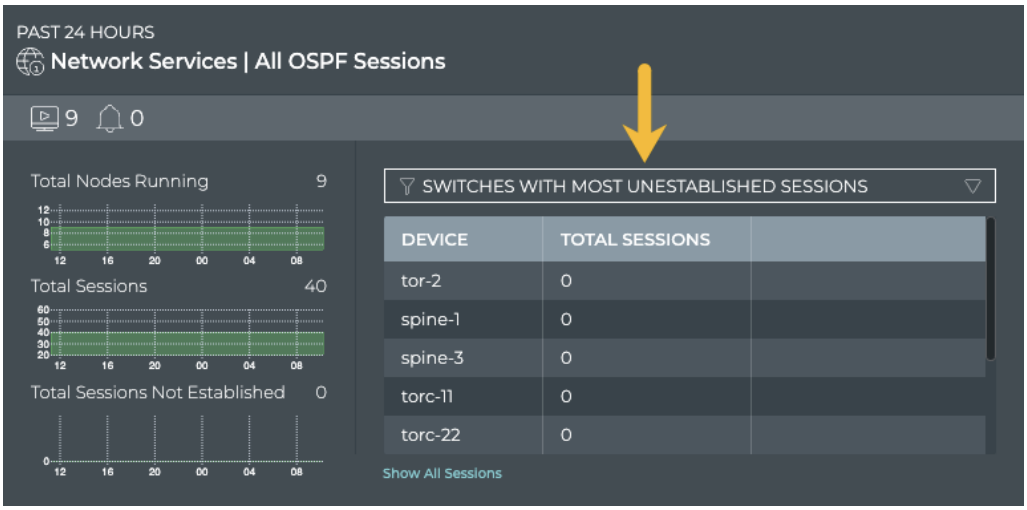
You can now see whether there are significant differences between this time and the original time. If the changes are unexpected, you can investigate further by looking at another time frame, determining if more nodes are now running OSPF than previously, looking for changes in the topology, and so forth.

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.

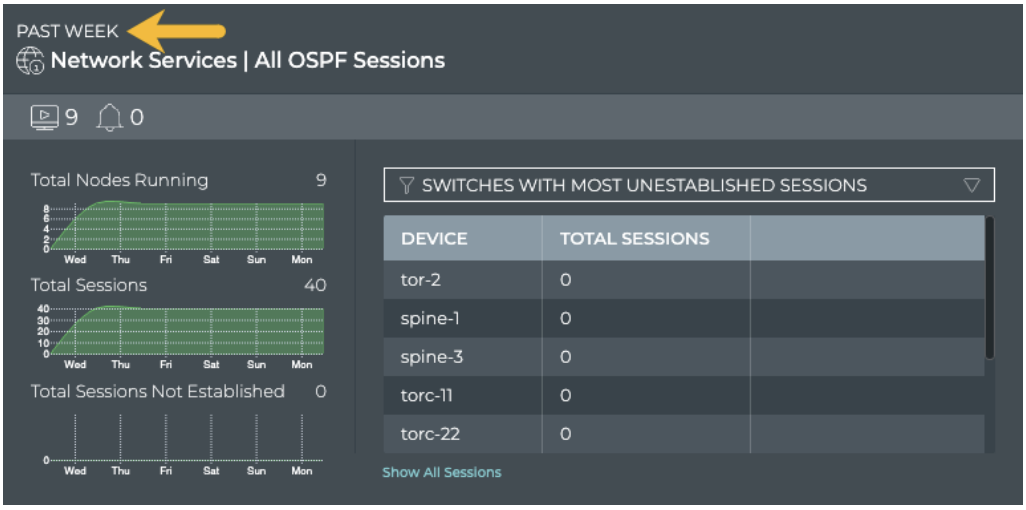
To view switches with the most unestablished OSPF sessions:

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.



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

- Hover over the **Total Nodes Not Est.** chart to focus on the switches and hosts with the most unestablished sessions 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 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 (see page 258).

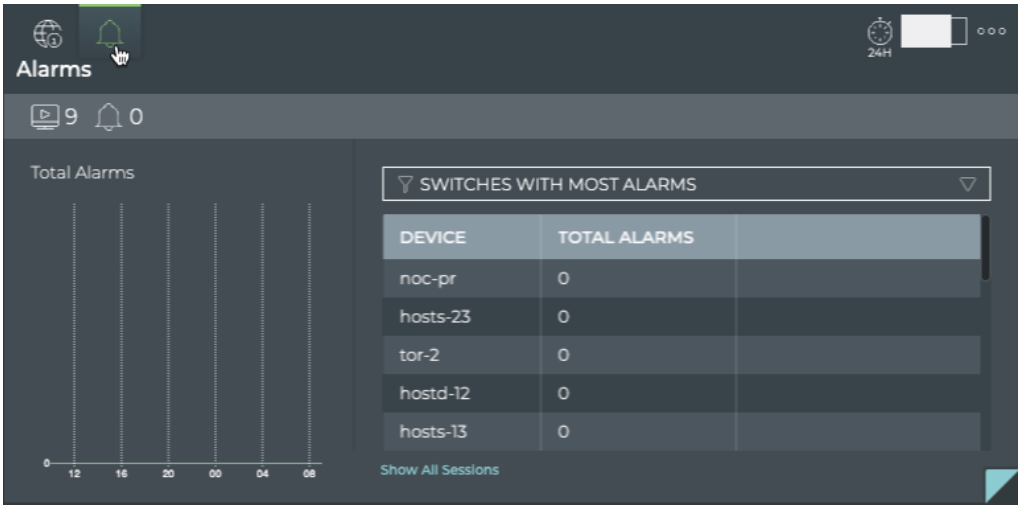
- Click **Show All Sessions** to investigate all OSPF sessions with events in the full screen card.

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:

- 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 OSPF sessions with events in the full screen card.

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.

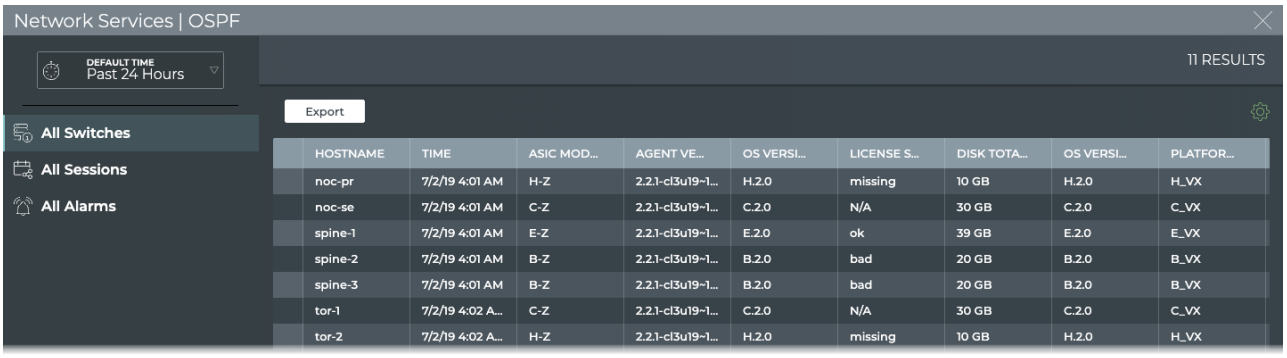
Where to go next depends on what data you see, but a couple of options include:

- 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.

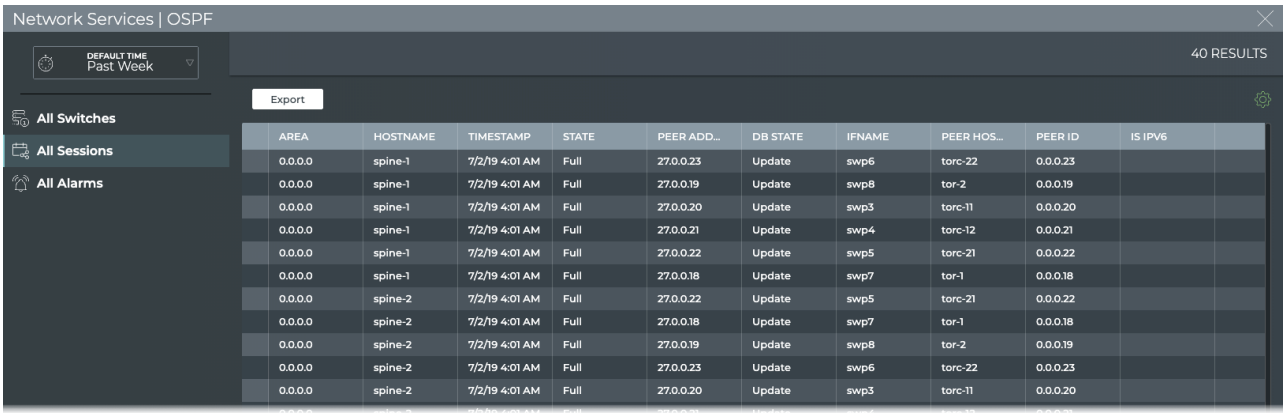


To return to your workbench, click ✕ in the top right corner.

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.

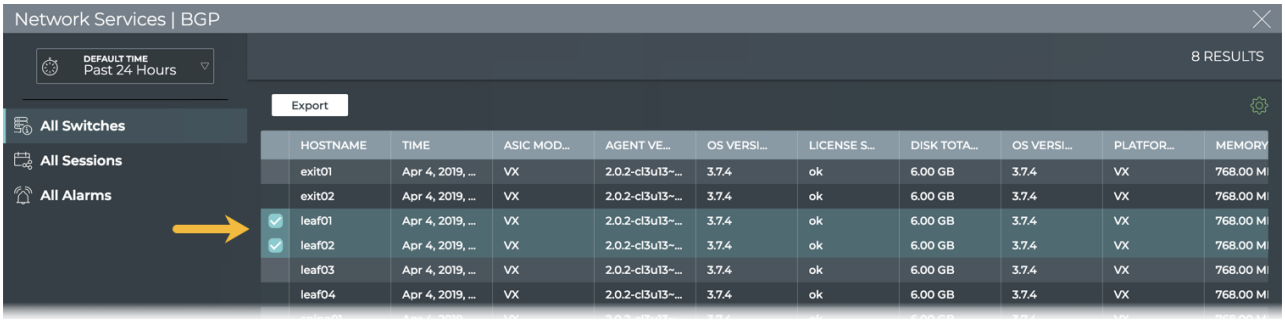


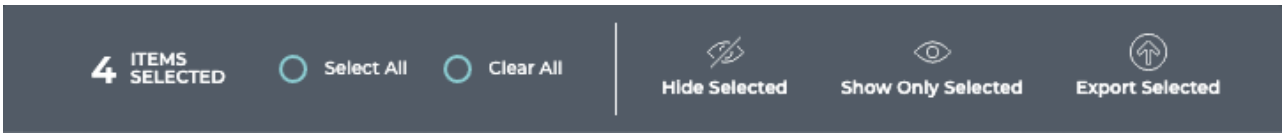
To return to your workbench, click ✕ in the top right corner.

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).





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 **Export** button.

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

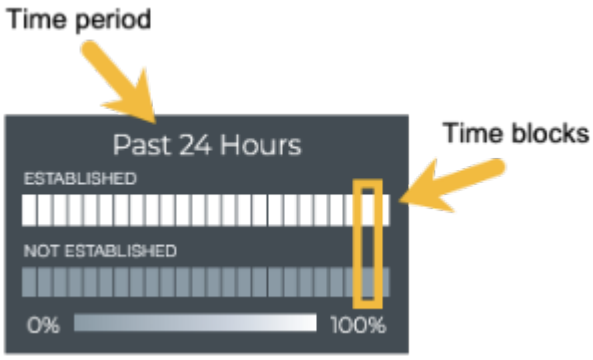
Monitor a Single OSPF Session

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.

To access the single session cards, you must open the full screen OSPF Service (all sessions) card, click the All Sessions tab, and double-click on a session. The full screen card automatically closes so you can view the medium single session card.

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.



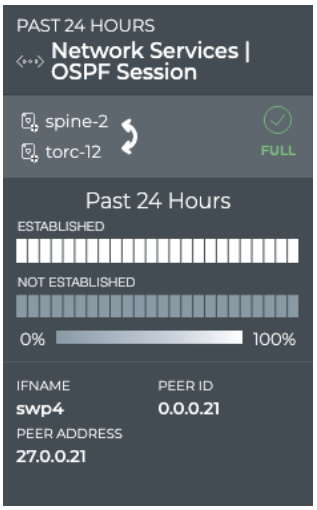
Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

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.
✓ , ✗	Current state of OSPF. ✓ Full or ✗ 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.

The medium OSPF Session card displays:

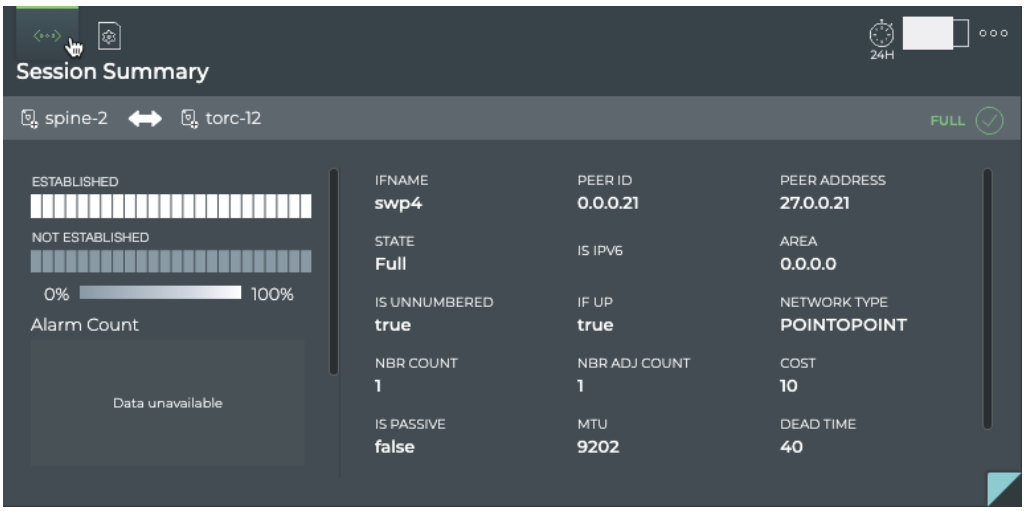


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
⟨•••⟩	Indicates data is for a single session of a Network Service or Protocol
Title	Network Services | OSPF Session
	Hostnames of the two devices in a session. Arrow points in the direction of the session.
✓ , ✗	Current state of OSPF. ✓ Full or ✗ 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.
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 Granularity of Data Shown Based on Time Period (see page) .
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:

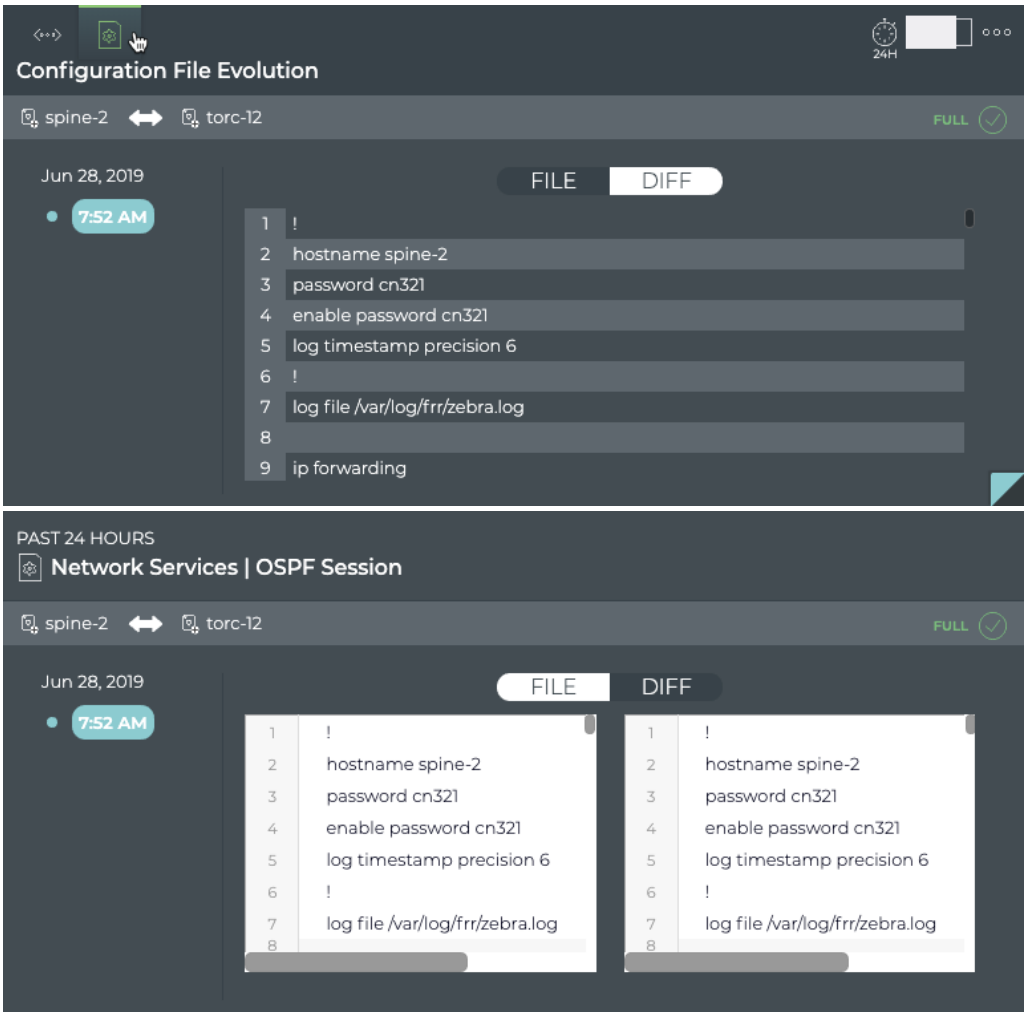


Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
<⋯>	Indicates data is for a single session of a Network Service or Protocol
Title	Session Summary (Network Services | OSPF Session)
Summary bar	Hostnames of the two devices in a session. Arrow points in the direction of the session.
	Current state of OSPF. ✓ Full or ⊗ 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading.

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 Granularity of Data Shown Based on Time Period (see page) .
Alarm Count Chart	Distribution and count of OSPF alarm events over the given time period
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. Full or 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
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	

Item	Description
	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.

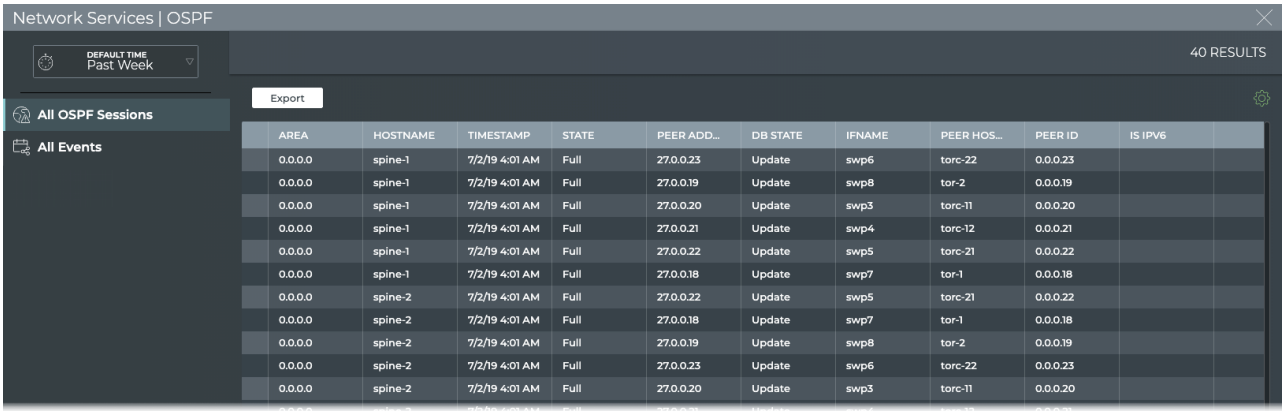
The *Configuration File Evolution* tab displays:



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) **Configuration File Evolution**
	Device identifiers (hostname, IP address, or MAC address) for host and peer in session. Click on to open associated device card.

Item	Description
✓, ✗	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 **File** is selected, the configuration file as it was at the selected time is shown. When **Diff** 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. **Note**: If no configuration file changes have been made, the card shows no results at all.

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



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

All OSPF Sessions tab	Displays all OSPF sessions running on the host device. The session list is sorted by **hostname** by default. This tab provides the following additional data about each session:
	• **Area**: Routing domain for this host device. Example values include 0.0.0.1, 0.0.0.23.
	• **DB State**: Session state of DB
	• **Ifname**: Name of the interface on host device where session resides. Example values include swp5, peerlink-1.
	• **Is IPv6**: Indicates whether the address of the host device is IPv6 (true) or IPv4 (false)
	• **Peer**
	  ◦ Address: IPv4 or IPv6 address of the peer device
	  ◦ Hostname: User-defined name for peer device

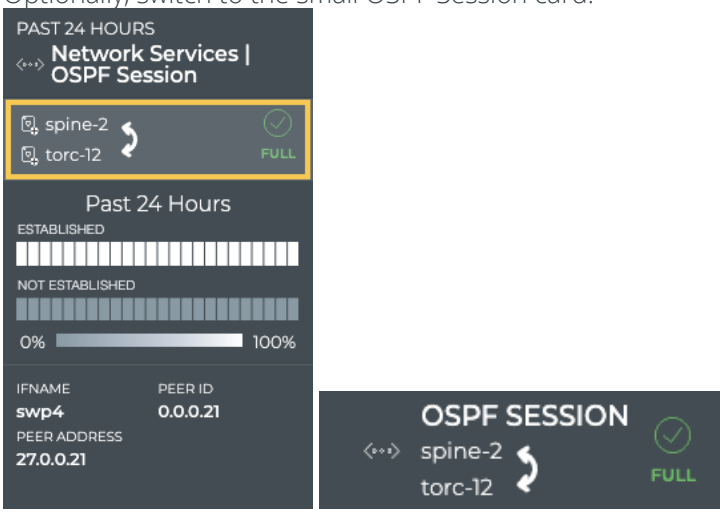
Item	Description
	• ID: Network subnet address of router with access to the peer device • **State**: Current state of OSPF. Values include Full, 2-way, Attempt, Down, Exchange, Exstart, Init, and Loading. • **Timestamp**: Date and time session was started, deleted, updated or marked dead (device is down)
All Events tab	Displays all 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: • **Message**: Text description of a OSPF-related event. Example: OSPF session with peer tor-1 swp7 vrf default state changed from failed to Established • **Source**: Hostname of network device that generated the event • **Severity**: Importance of the event. Values include critical, warning, info, and debug. • **Type**: Network protocol or service generating the event. This always has a value of OSPF in this card workflow.
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 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.

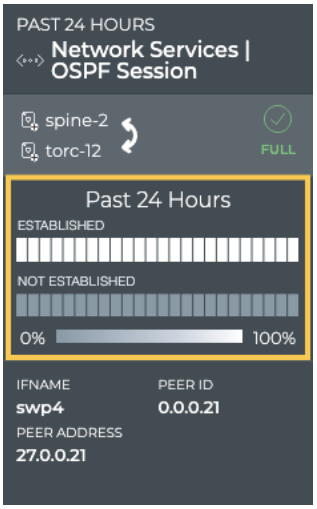


View OSPF Session State Changes

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:

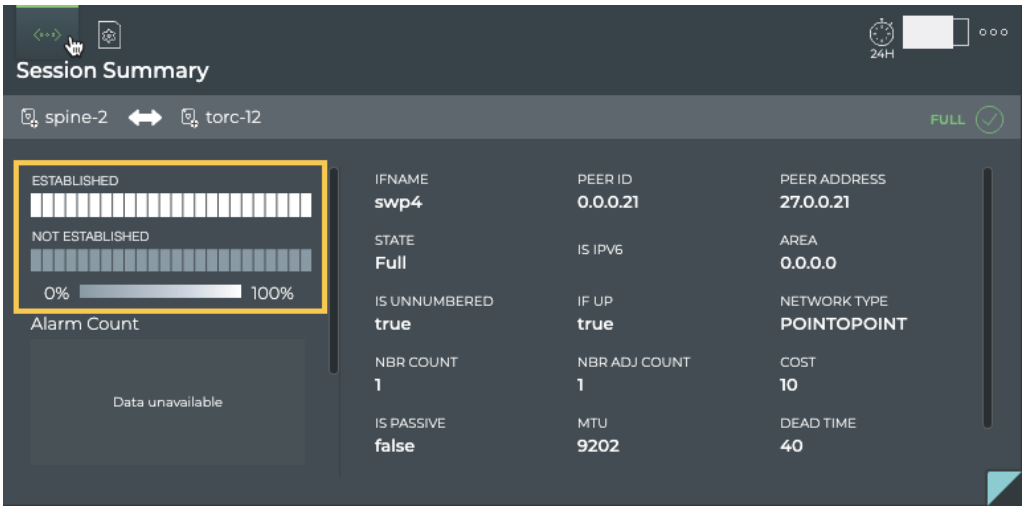
1. Add the Network Services | All OSPF Sessions card.
2. Switch to the full screen card.
3. Open the large OSPF Service card.
4. Click the **All Sessions** tab.
5. Double-click the session of interest. The full screen card closes automatically.



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.

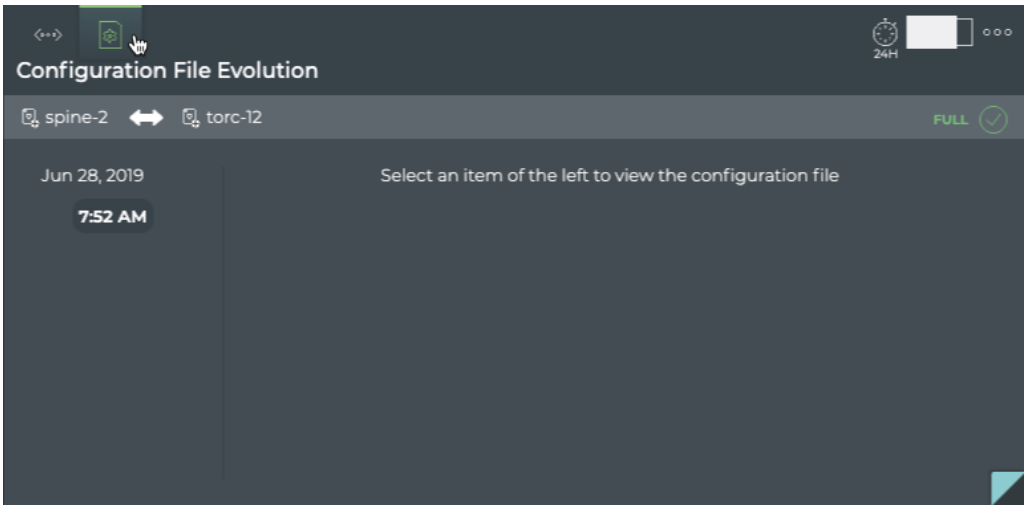
View Changes to the OSPF Service Configuration File

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:

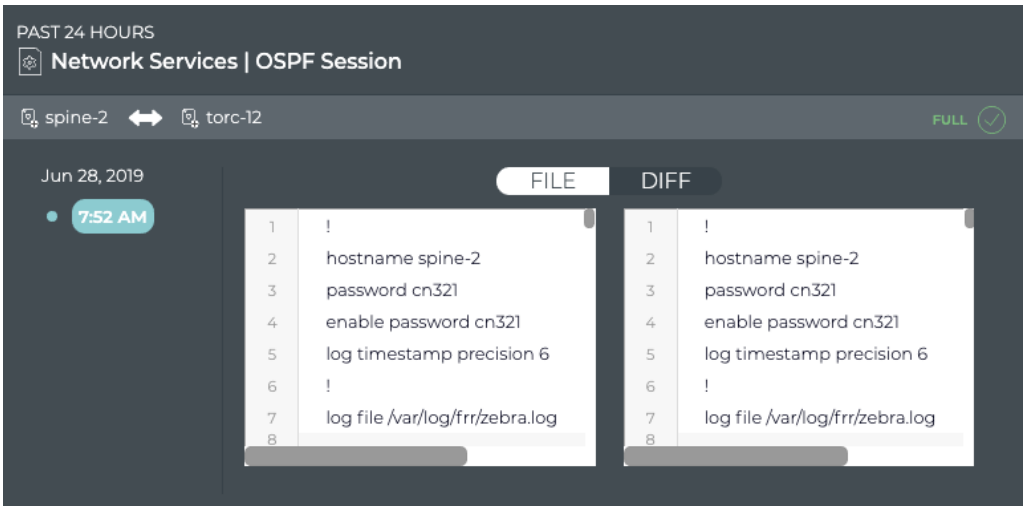
1. Open the large OSPF Session card.
2. Hover over the card and click 

   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.

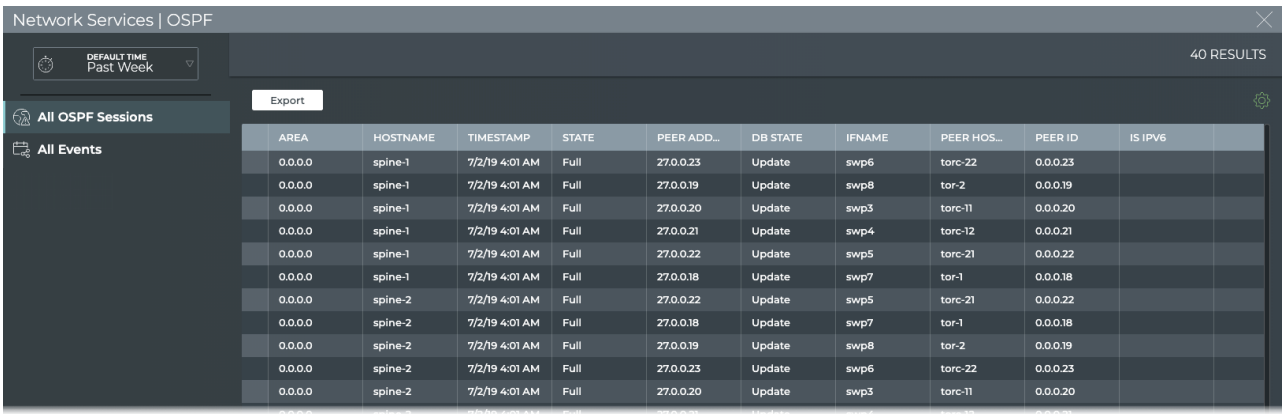
The Diff view displays the changes between this version (on left) and the most recent version (on right) side by side. The changes are highlighted in red and green. In this example, we don't have a change to highlight, so it shows the same file on both sides.



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.

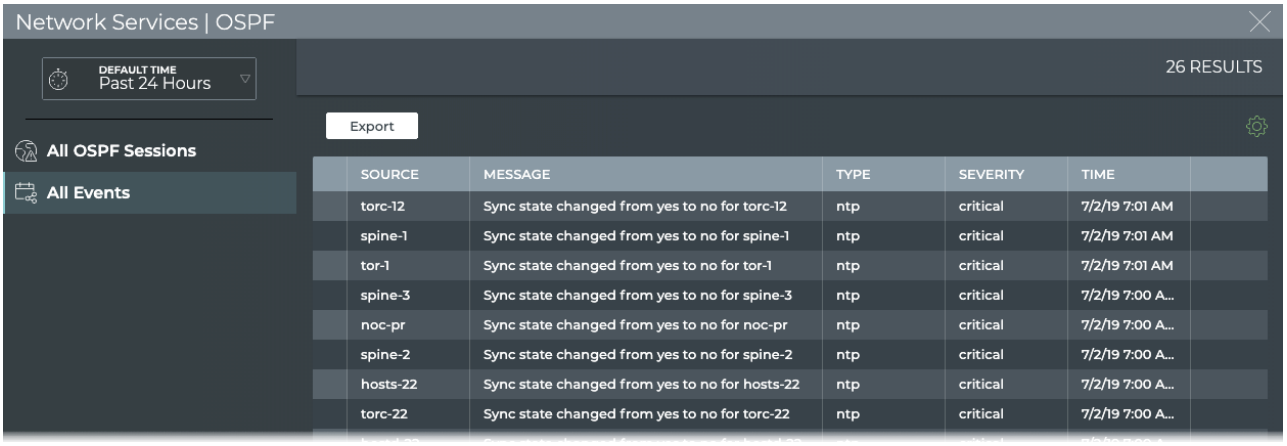


To return to your workbench, click ✕ in the top right corner.

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 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.

Contents

This topic describes how to...

- Scheduled Trace Results Card Workflow Summary (see page 251)
- Granularity of Data Shown Based on Time Period (see page 255)
- View Scheduled Trace Results (see page 256)

Create a Trace Request

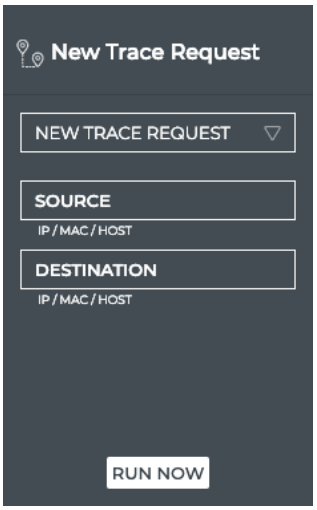
Two types of connectivity checks can be run–an immediate (on-demand) trace and a scheduled trace. The Trace Request card workflow is used to configure and run both of these trace types.

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
Go	Click to start the trace now

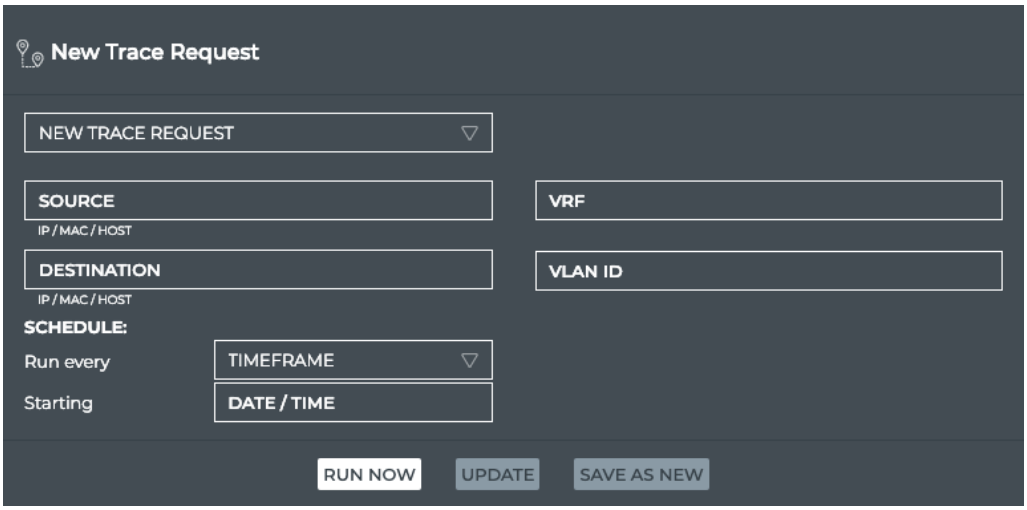
The medium Trace Request card displays:



Item	Description
	Indicates a trace request
Title	New Trace Request

Item	Description
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
Destination	(Required) IP address of device where to end the trace
Run Now	Start the trace now

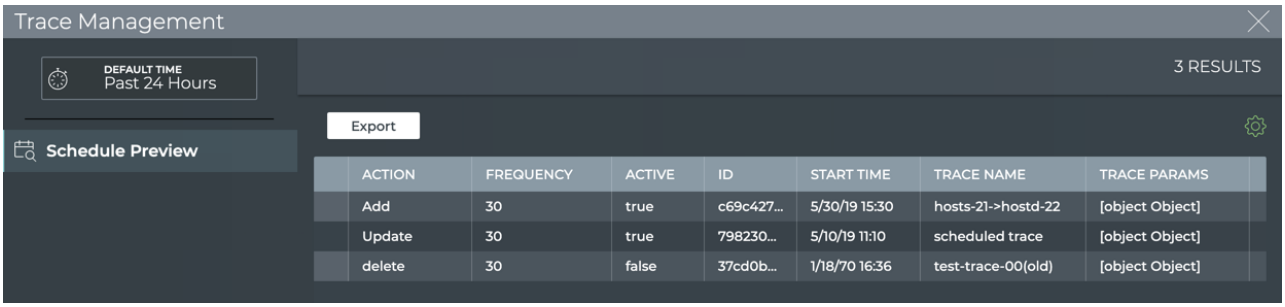
The large Trace Request card displays:



Item	Description
	Indicates a trace request
Title	New Trace Request
Trace selection	Leave *New Trace Request* 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.
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.

Item	Description
Schedule	Sets the frequency with which to run a new trace (**Run every**) and when to start the trace for the first time (**Starting**).
Run Now	Start the trace now
Update	**Update** is available when a scheduled trace request is selected from the dropdown list and you make a change to its configuration. Clicking **Update** saves the changes to the *existing* scheduled trace.
Save As New	**Save As New** is available in two instances: • When you enter a source, destination, and schedule for a new trace. Clicking **Save As New** in this instance saves the new scheduled trace. • When changes are made to a selected scheduled trace request. Clicking **Save As New** in this instance saves the modified scheduled trace *without* changing the original trace on which it was based.

The full screen Trace Request card displays:



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	Displays all scheduled trace requests for the given user. By default, the listing is sorted by **Start Time**, with the most recently started traces listed at the top. The tab provides the following additional data about each event: • **Action**: Indicates latest action taken on the trace job. Values include Add, Deleted, Update. • **Frequency**: How often the trace is scheduled to run

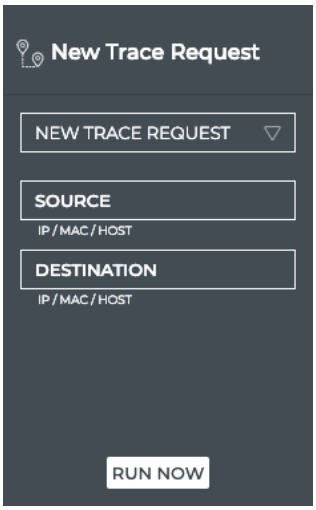
Item	Description
	• **Active**: Indicates if trace is actively running (true), or stopped from running (false) • **ID**: Internal system identifier for the trace job • **Trace Name**: User-defined name for a trace • **Trace Params**: Indicates source and destination, optional VLAN or VRF specified, and whether to alert on failure
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 a Layer 3 On-demand Trace Request

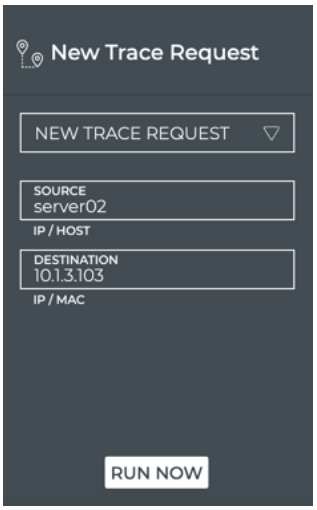
It is helpful to verify the connectivity between two devices when you suspect an issue is preventing proper communication between them. It you cannot find a path through a layer 3 path, you might also try checking connectivity through a layer 2 path.

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*.

> 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.

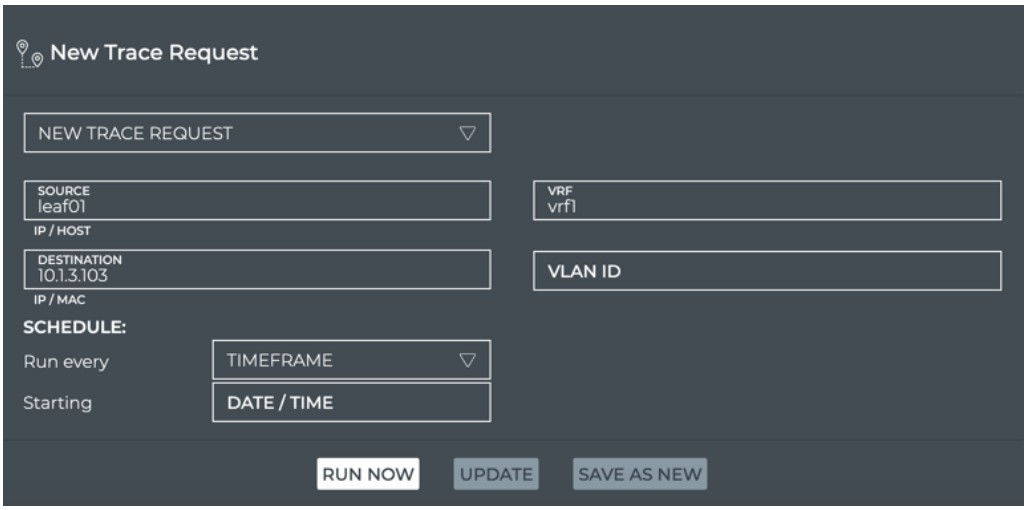
4. Click **Run Now**. A corresponding Trace Results card is opened on your workbench. Refer to View Layer 3 Trace Results (see page) for details.

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.



In this example, we are starting our trace at *leaf01* and ending it at *10.1.3.103* using VRF *vrf1*.

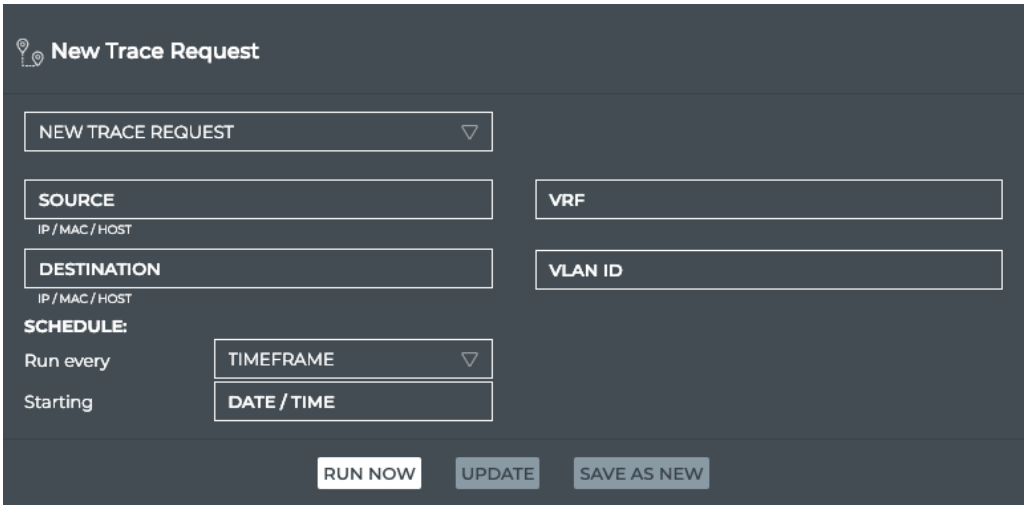
5. Click **Run Now**. A corresponding Trace Results card is opened on your workbench. Refer to View Layer 3 Trace Results (see page) for details.

Create a Layer 2 Trace

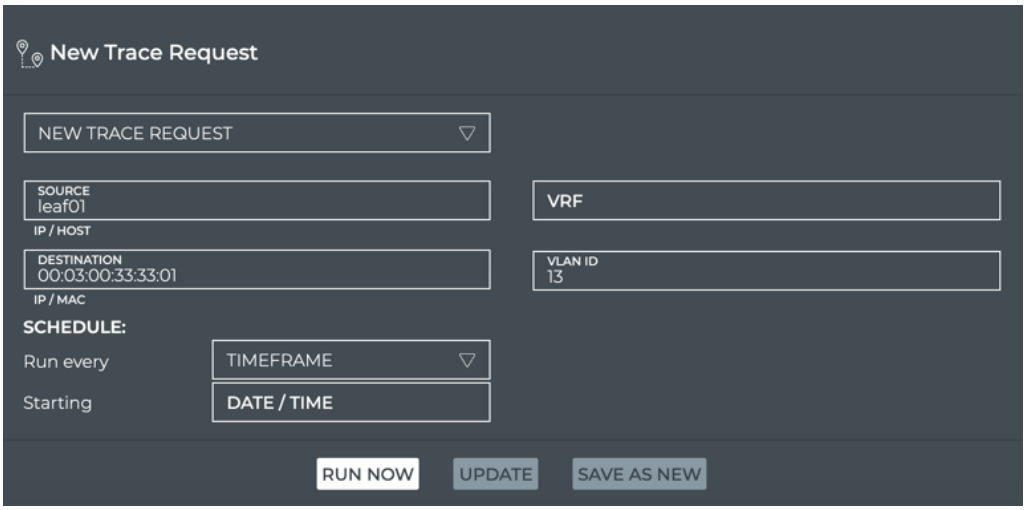
It is helpful to verify the connectivity between two devices when you suspect an issue is preventing proper communication between them. It you cannot find a path through a layer 2 path, you might also try checking connectivity through a layer 3 path.

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.



In this example, we are starting our trace at *leaf01* and ending it at *00:03:00:33:33:01* using VLAN *13*.

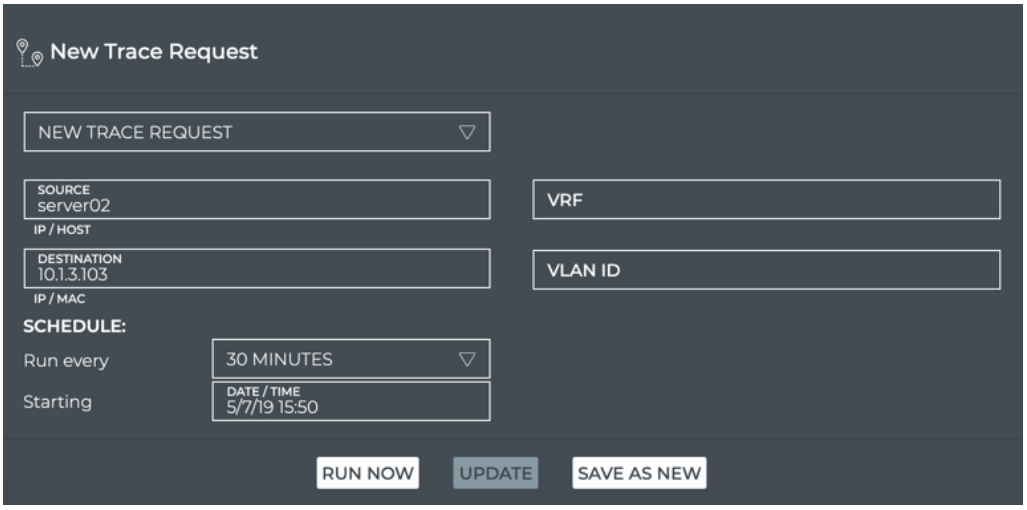
5. Click **Run Now**. A corresponding Trace Results card is opened on your workbench. Refer to View Layer 2 Trace Results (see page) for details.

Create a Trace to Run on a Regular Basis (Scheduled Trace)

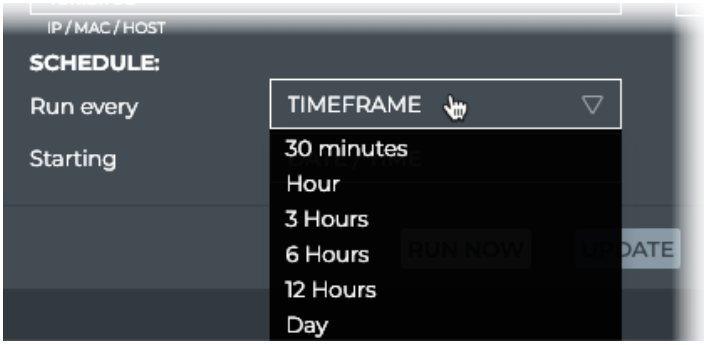
There may be paths through your network that you consider critical to your everyday or particularly important operations. In that case, it might be useful to create one or more traces to periodically confirm that at least one path is available between the relevant two devices. Scheduling a trace request can be performed from the large Trace Request card.

To schedule a trace:

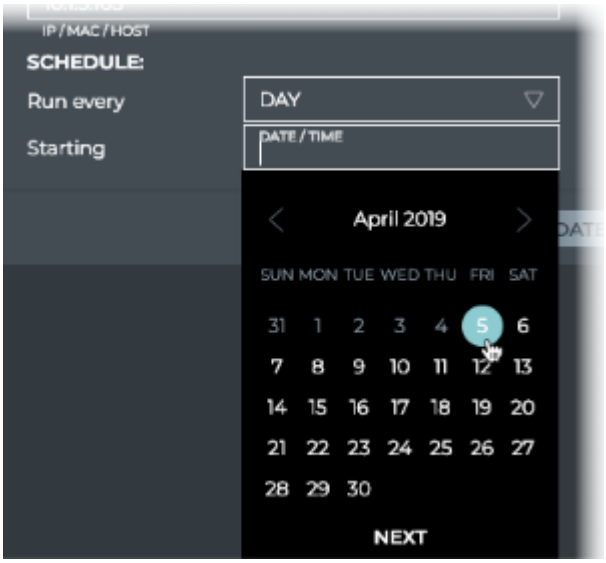
1. Open the large Trace Request card.
2. In the **Source** field, enter the hostname or IP address of the device where you want to start the trace.
3. In the **Destination** field, enter the MAC address (layer 2) or IP address (layer 3) of the device where you want to end the trace.
4. Optionally, enter a VLAN ID (layer 2) or VRF interface (layer 3).



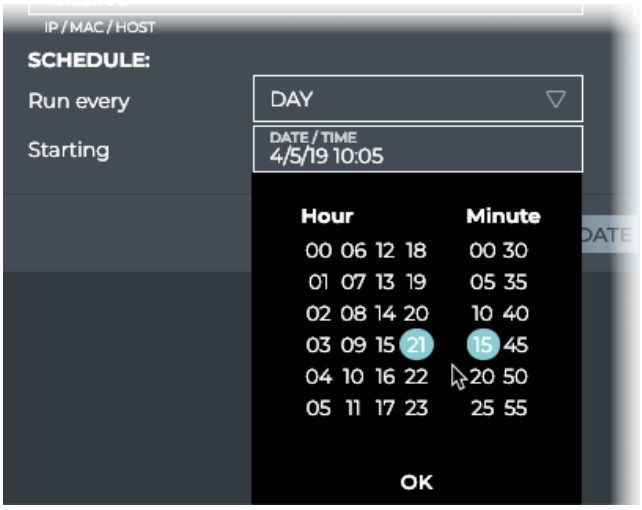
5. Click **Timeframe** under **Schedule** to specify how often you want to run the trace.



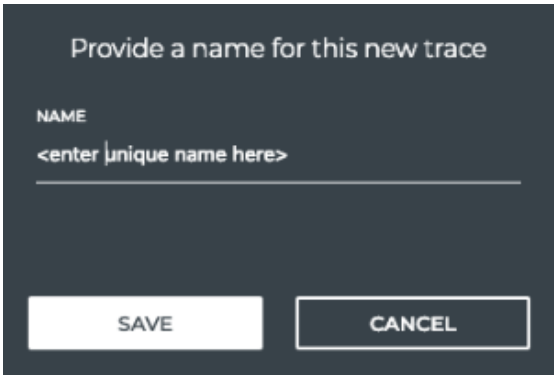
6. Click **Date/Time** to specify the day you want the trace to run for the first time.



7. Click **Next**.
8. Click the time you want the trace to run for the first time.



9. Click **OK**.
10. 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.

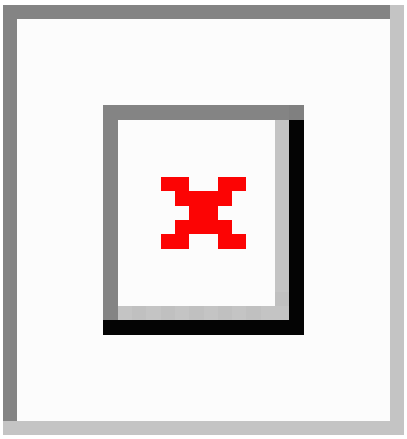
2. Select the scheduled trace from the **Select Trace** or **New Trace Request** list. **Note**: In the medium and large cards, the trace details are filled in on selection of the scheduled trace.
3. Click **Go** or **Run Now**. A corresponding Trace Results card is opened on your workbench.

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.

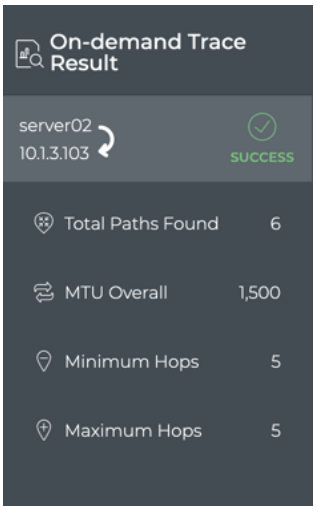
On-demand Trace Results Card Workflow Summary

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.

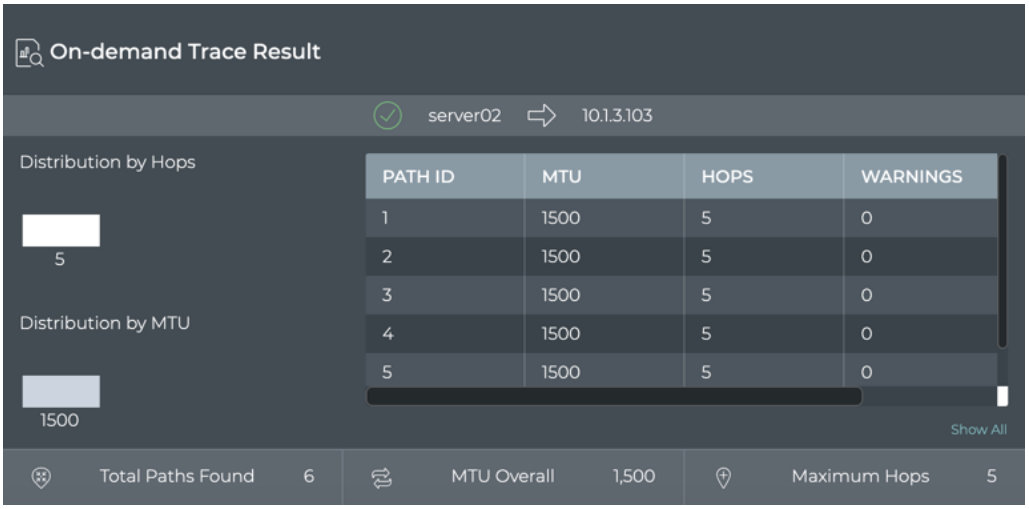
The medium On-demand Trace Results card displays:



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.

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.
Total Paths Found	Number of paths found between the two devices
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

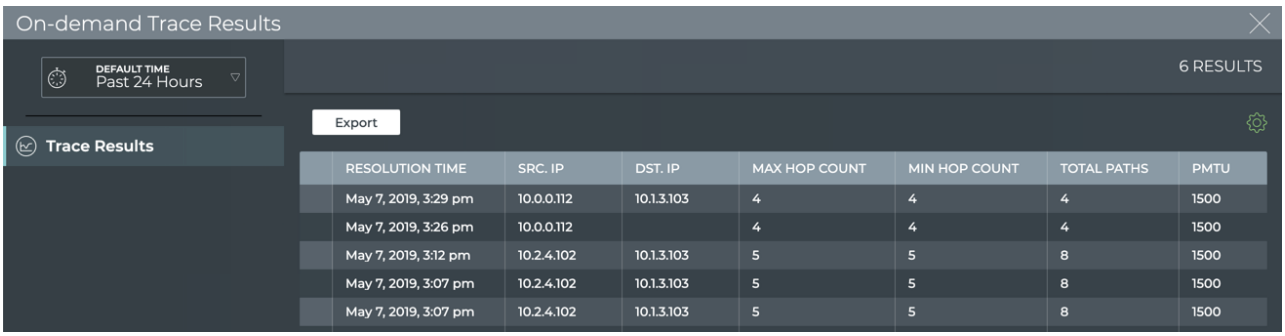
The large On-demand Trace Results card displays:



Item	Description
	Indicates an on-demand trace result
Title	On-demand Trace Result
✓, ✗	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.

Item	Description
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	Provides detailed path information, sorted by the route identifier, including: • **Route ID**: Identifier of each path • **MTU**: Average speed of the interfaces used • **Hops**: Number of hops to get from the source to the destination device • **Warnings**: Number of warnings encountered during the trace on a given path • **Errors**: Number of errors encountered during the trace on a given path
Total Paths Found	Number of paths found between the two devices
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 full screen On-demand Trace Results card displays:

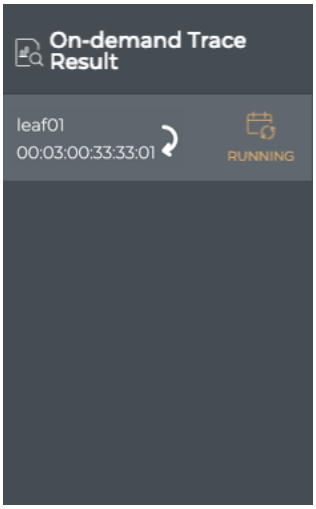


Item	Description
Title	On-demand Trace Results
Trace Results tab	Provides detailed path information, sorted by the **Resolution Time** (date and time results completed), including: • **SCR.IP**: Source IP address • **DST.IP**: Destination IP address

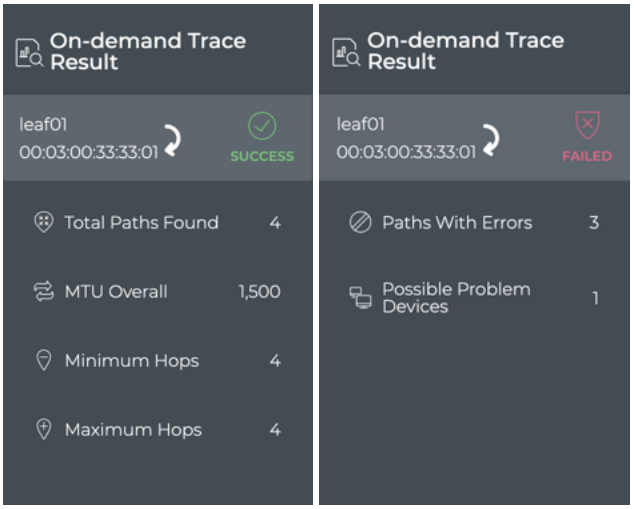
Item	Description
	• **Max Hop Count**: Largest number of hops along a path between the devices • **Min Hop Count**: Smallest number of hops along a path between the devices • **Total Paths**: Number of paths found between the two devices • **PMTU**: Average size of the maximum transmission unit for all interfaces along the paths • **Errors**: Message provided for analysis when a trace fails
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

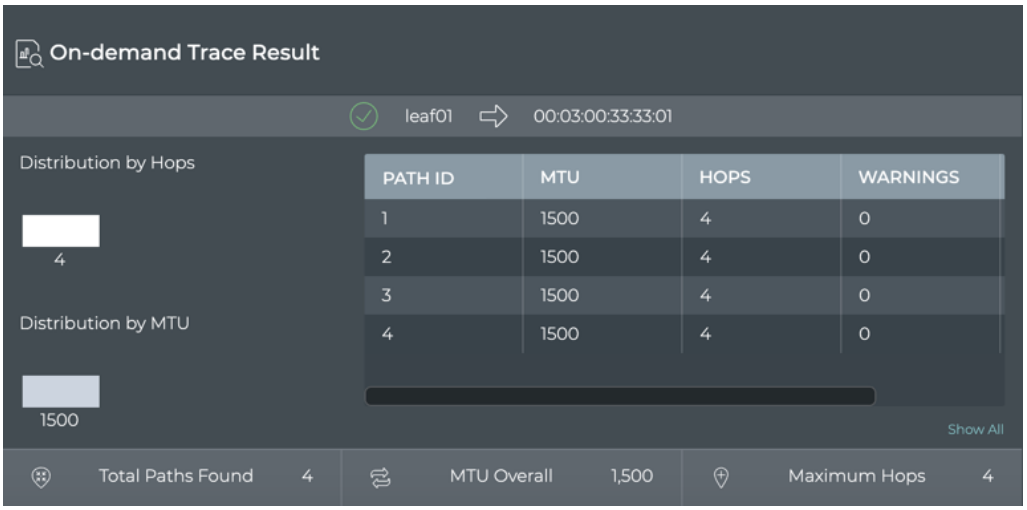
When you start the trace, the corresponding results card is opened on your workbench. While it is working on the trace, a notice is shown on the card indicating it is running.

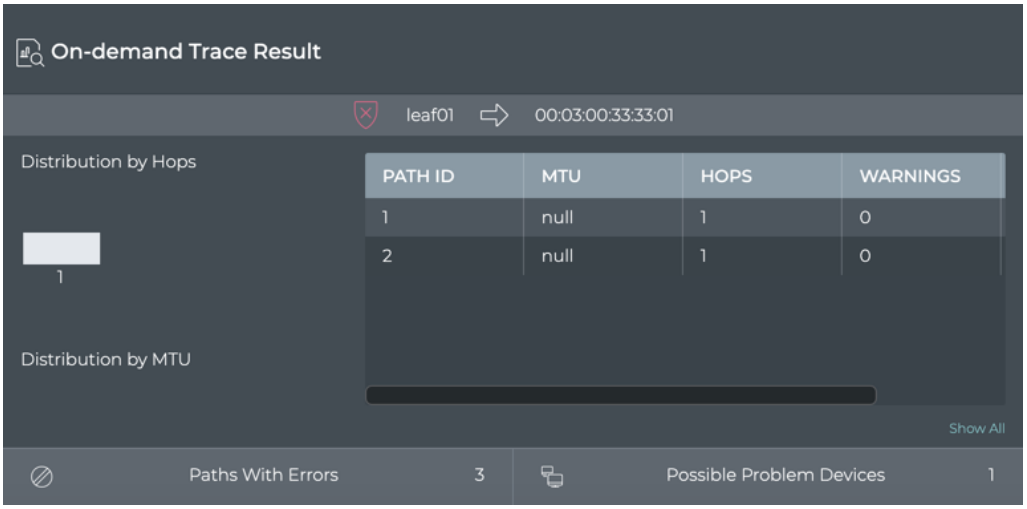


Once the job is completed, the results are displayed.



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.

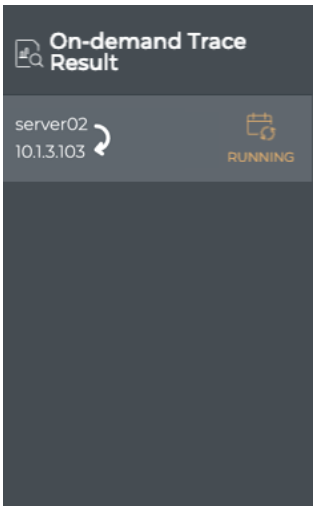




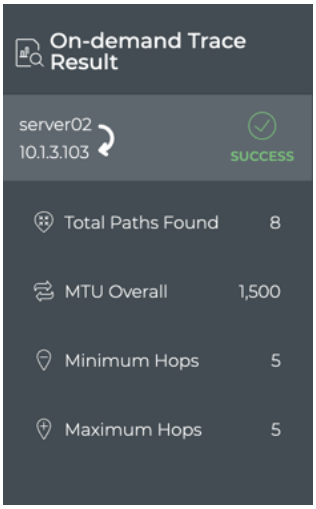
In our example, we can verify that every path option had four hops since the distribution chart only shows one hop count and the table indicates each path had a value of four hops. Similarly, you can view the MTU data. If there had been any warnings, the count would have been visible in the table.

View Layer 3 Trace Results

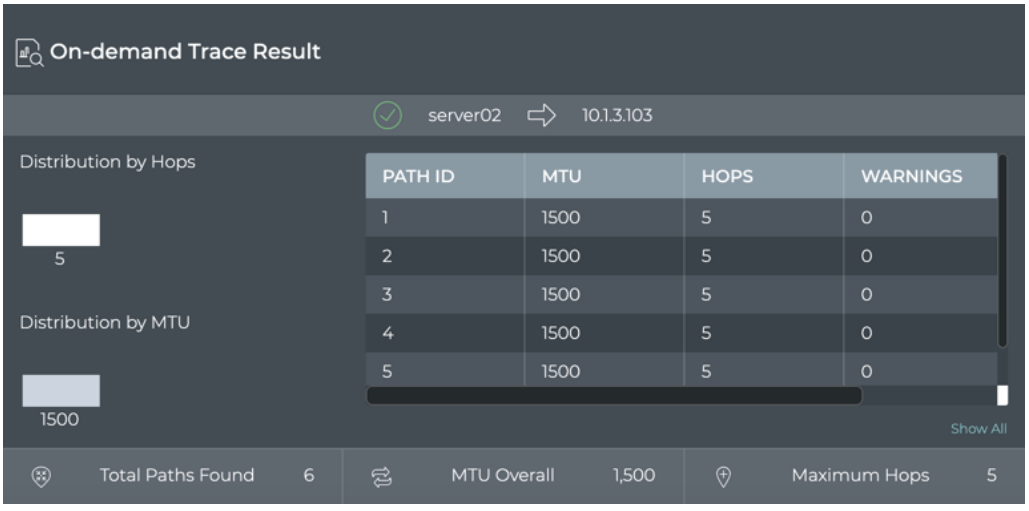
When you start the trace, the corresponding results card is opened on your workbench. While it is working on the trace, a notice is shown on the card indicating it is running.



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. Eight 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.

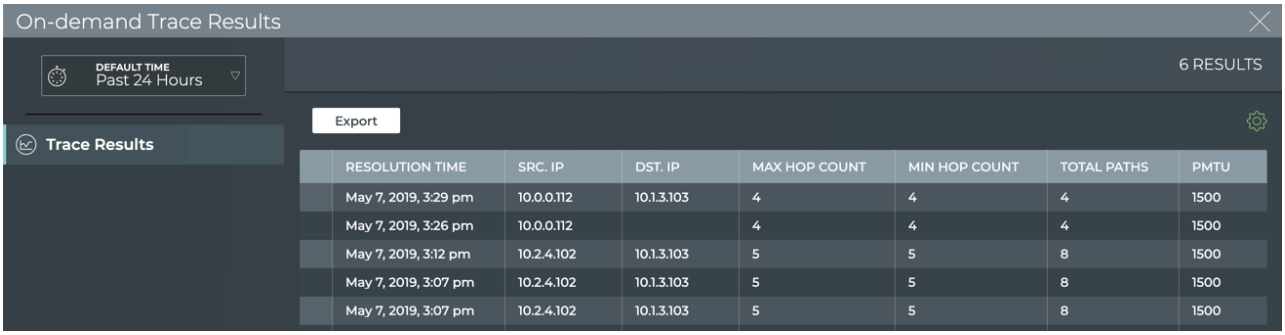


In our example, we can verify that every path option had five hops since the distribution chart only shows one hop count and the table indicates each path had a value of five hops. Similarly, you can view the MTU data. If there had been any warnings, the count would have been visible in the table.

View All On-demand Trace Results

If you have run multiple on-demand traces, you may find it easier to view the results all together in a single view. The full screen Trace Results card provides this information.

To view all on-demand trace results, open the full screen On-demand Trace Results card.



Ordered by most recent trace, you can now view all recent traces together.

View Scheduled Trace Results

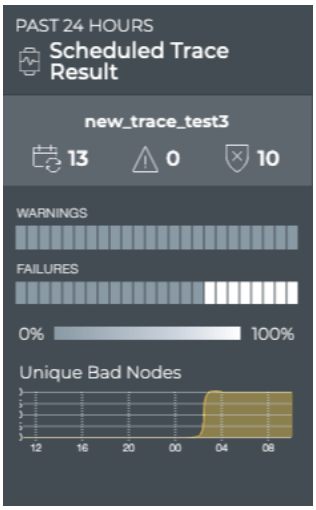
You can view the results of scheduled traces at any time. Results are displayed on the Scheduled Trace Results cards.

Scheduled Trace Results Card Workflow Summary

The small Scheduled Trace Results card displays:

Item	Description
	Indicates a scheduled trace result
	Source and destination of the trace, identified by their address or hostname. Source is listed on left with arrow pointing to destination.
Results	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. • Number of trace runs completed in the designated time period • Number of runs with warnings • Number of runs with errors

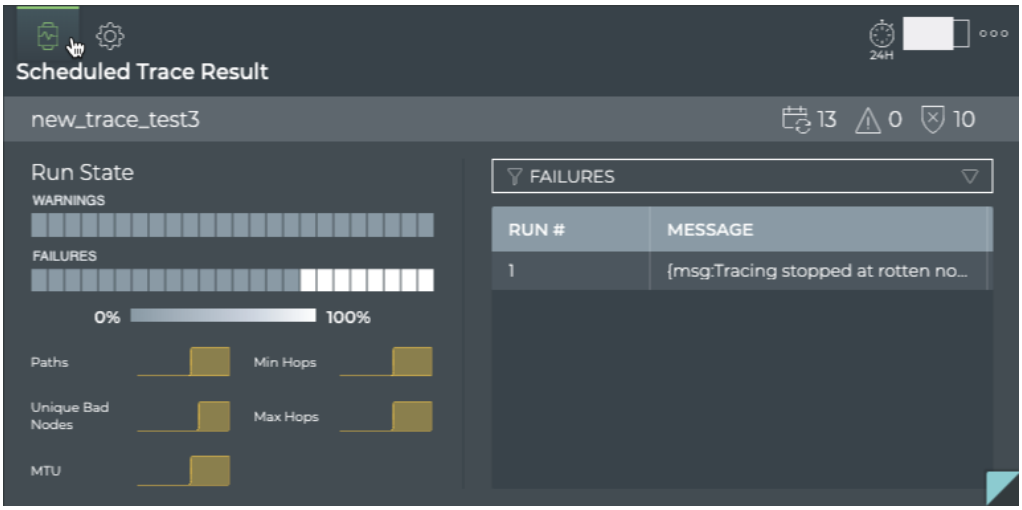
The medium Scheduled Trace Results card displays:



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	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. • Number of trace runs completed in the designated time period • Number of runs with warnings • Number of runs with errors
Charts	**Heat map:** A time segmented view of the results. For each time segment, the color represents the percentage of warning and failed results. Refer to Granularity of Data Shown Based on Time Period (see page) for details on how to interpret the results. **Unique Bad Nodes**: Distribution of unique nodes that generated the indicated warnings and /or failures

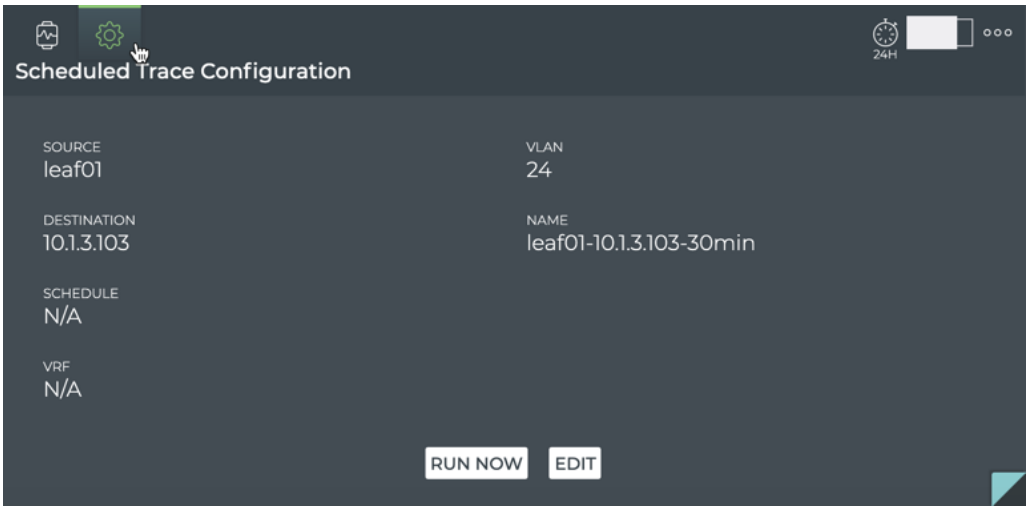
The large Scheduled Trace Results card contains two tabs:

The *Results* tab displays:



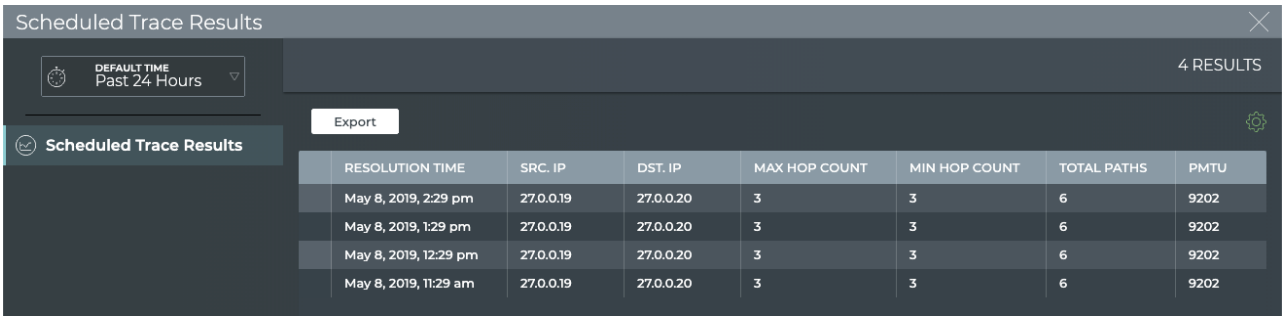
Item	Description
Time period	Range of time in which the displayed data was collected; applies to all card sizes
	Indicates a scheduled trace result
Title	Scheduled Trace Result
Summary	Name of scheduled validation and summary of trace results: a successful result implies all paths were successful without any warnings or failures; a failure result implies there was at least one path with warnings or errors. • Number of trace runs completed in the designated time period • Number of runs with warnings • Number of runs with errors
Charts	**Heat map:** A time segmented view of the results. For each time segment, the color represents the percentage of warning and failed results. Refer to Granularity of Data Shown Based on Time Period (see page) for details on how to interpret the results. **Small charts**: 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.
Table /Filter options	When the **Failures** filter option is selected, the table displays the failure messages received for each run. When the **Paths** filter option is selected, the table displays all of the paths tried during each run. When the **Warning** filter option is selected, the table displays the warning messages received for each run.

The *Configuration* 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 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
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:

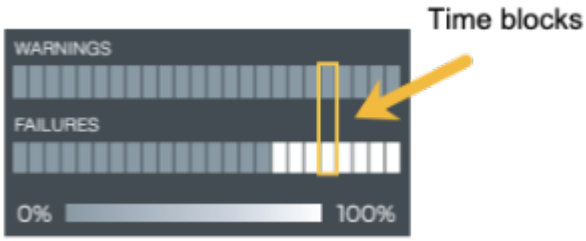


Item	Description
Title	Scheduled Trace Results
✕	Closes full screen card and returns to workbench
Time period	Range of time in which the displayed data was collected; applies to all card sizes; select an alternate time period by clicking ▽
Results	Number of results found for the selected tab
Scheduled Trace Results tab	Displays the basic information about the trace, including: • **Resolution Time**: Time that trace was run • **SRC.IP**: IP address of the source device • **DST.IP**: Address of the destination device • **Max Hop Count**: Maximum number of hops across all paths between the devices • **Min Hop Count**: Minimum number of hops across all paths between the devices • **Total Paths**: Number of available paths found between the devices • **PMTU**: Average of the maximum transmission units for all paths • **Errors**: Message provided for analysis if trace fails Click on a result to open a detailed view of the results.
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.



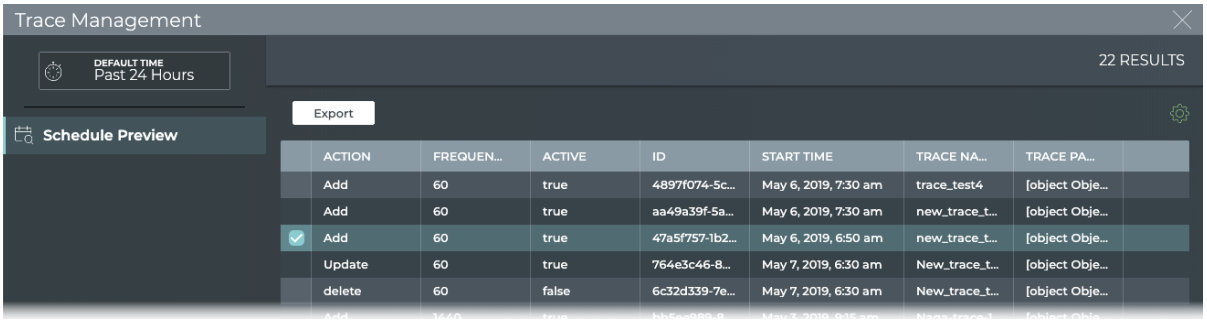
Time Period	Number of Runs	Number Time Blocks	Amount of Time in Each Block
6 hours	18	6	1 hour
12 hours	36	12	1 hour
24 hours	72	24	1 hour
1 week	504	7	1 day
1 month	2,086	30	1 day
1 quarter	7,000	13	1 week

View Scheduled Trace Results

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

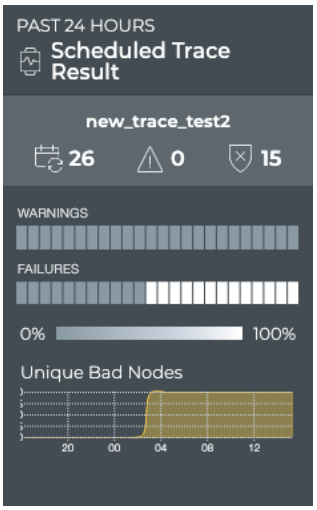
To view the results:

1. Open the full screen Trace Request card to view all scheduled traces that have been run.

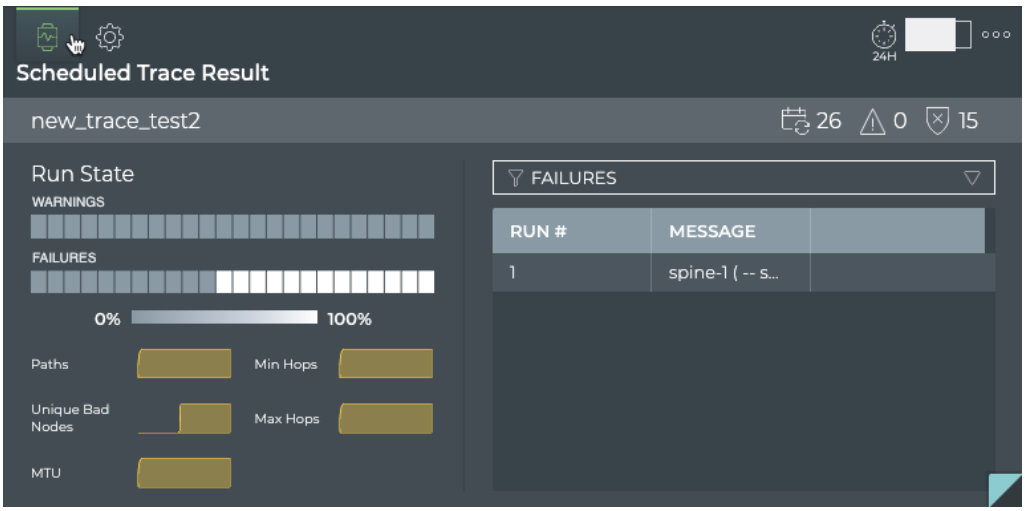


2. Select the scheduled trace you want to view results for by clicking in the first column of the result and clicking the check box.

3. On the Edit Menu that appears at the bottom of the window, click (Open Cards). This opens the medium Scheduled Validation Results card(s) for the selected items.

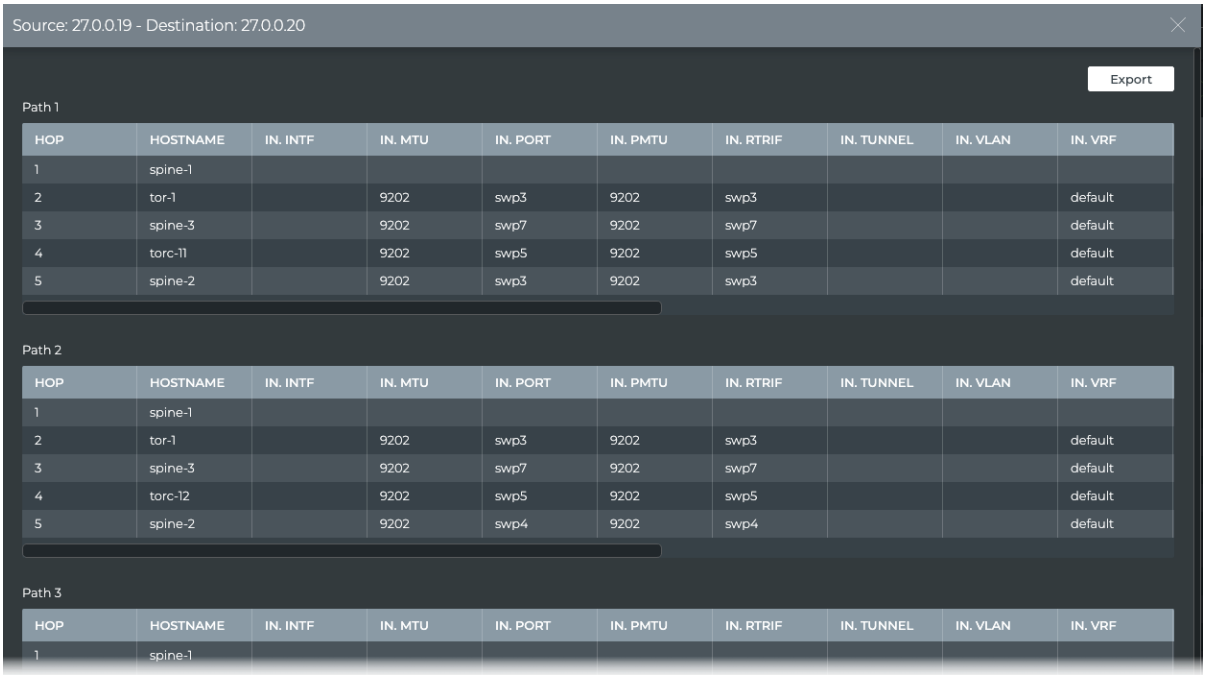


4. Note the distribution of results. Are there many failures? Are they concentrated together in time? Has the trace begun passing again?
5. Hover over the heat maps to view the status numbers and what percentage of the total results that represents for a given region.
6. Switch to the large Scheduled 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 (see page) 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:



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, spine-1 in this case. It exits this device at switch port 7 with an MTU of 9202 and over the default VRF too get to tor-1. The trace goes in to swp 3 with an MTU of 9202 over its default VRF interface. It exits tor-1 through switch port 5 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 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 the Network (see page 46).

Contents

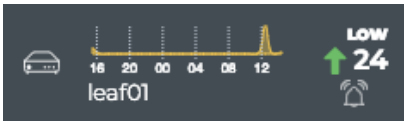
This topic describes...

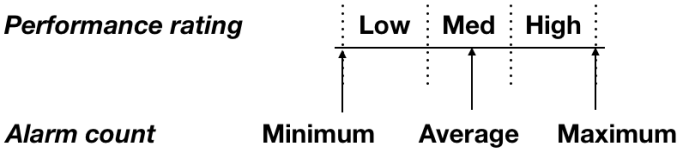
Monitor Switch Performance

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.

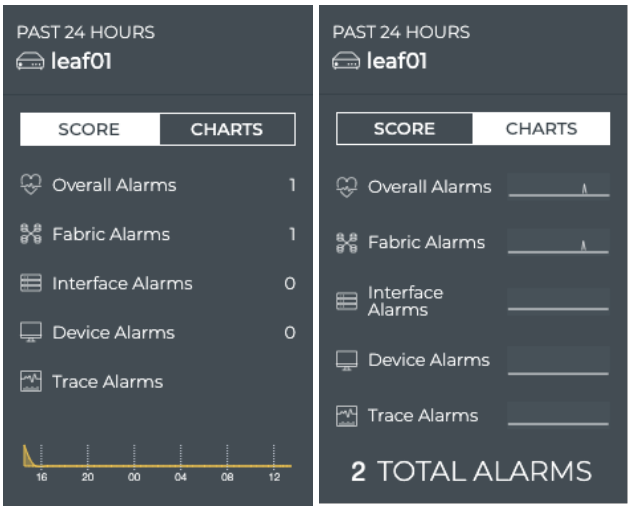
Switch Card Workflow Summary

The small Switch card displays:



Item	Description
	Indicates data is for a single switch
title	Hostname of switch
Chart	Distribution of switch alarms during the designated time period
Trend	Trend of alarm count, represented by an arrow: • **Pointing upward and green**: alarm count is higher than the last two time periods, an increasing trend • **Pointing downward and bright pink**: alarm count is lower than the last two time periods, a decreasing trend • **No arrow**: alarm count is unchanged over the last two time periods, trend is steady
Count	Current count of alarms on the switch
Rating	Overall performance of the switch. Determined by the count of alarms relative to the average count of alarms during the designated time period: • **Low**: Count of alarms is below the average count; a nominal count • **Med**: Count of alarms is in range of the average count; some room for improvement • **High**: Count of alarms is above the average count; user intervention recommended 

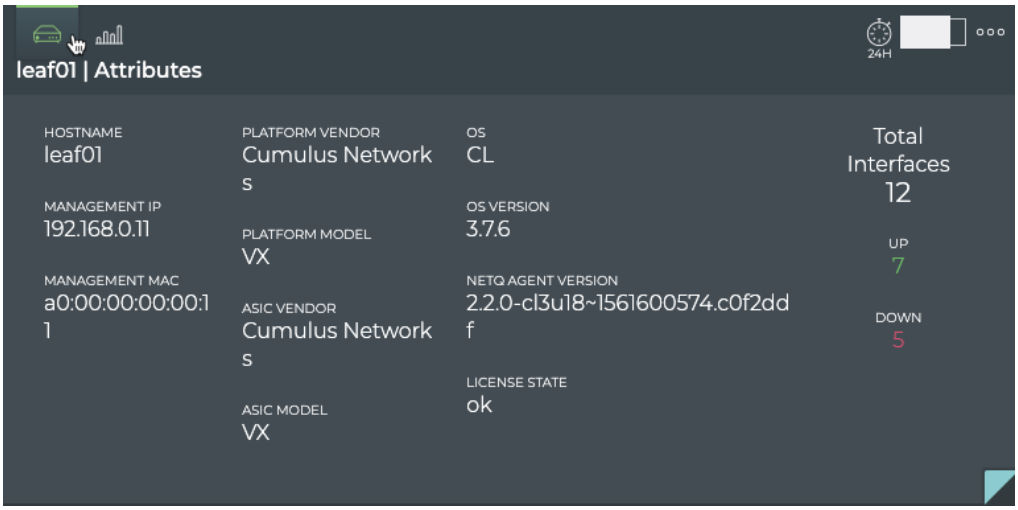
The medium Switch card displays:



Item	Description
	Indicates data is for a single switch
title	Hostname of switch
Score	When selected, displays distribution and count of alarms generated by this switch during the designated time period
Charts	When selected, displays distribution of overall health score for network services, interfaces, system and trace, as well as total alarm count, during the designated time period

The large Switch card contains two tabs:

The *Attributes* tab displays:



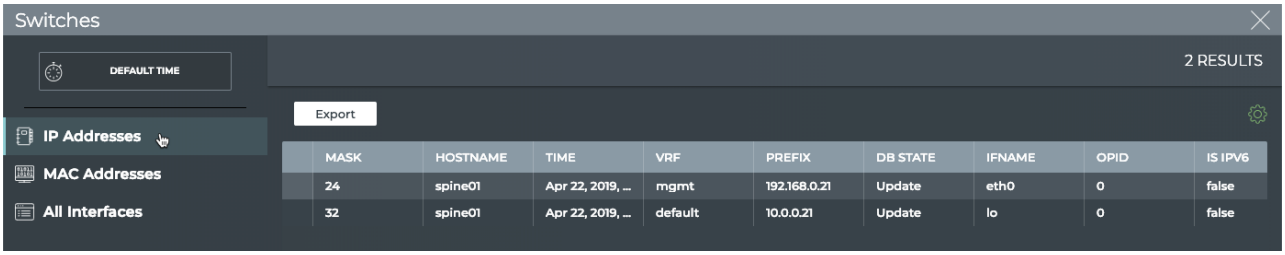
Item	Description
	Indicates data is for a single switch

Item	Description
	
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
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.
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 (*ok*) or invalid/missing (*bad*)
Total Interfaces	Total number of interfaces on this switch, and the number of those that are up and down.

The *Utilization* tab displays:

Item	Description
	Indicates utilization data is for a single switch
Title	<Hostname> | Utilization
Performance	Displays distribution of CPU usage, memory usage, and switch up time during the designated time period
Network	Displays distribution of the size of various network tables (IP, MAC, ACL, Routing, etc.) during the designated time period
Filter	Click to open filter field. Begin typing to view only charts that match the filter.

The full screen Switch card provides tabs for all IP addresses, all MAC addresses, and all interfaces.



Item	Description
Title	Switches
	Closes full screen card and returns to workbench
Default Time	Displayed data is current as of this moment

Item	Description
Results	Number of results found for the selected tab
IP Addresses	Displays all known IP addresses for the switch. This tab provides the following additional data about each address: • **DB State**: Session state of the DB; for internal use only • **Hostname**: User-defined name of the switch • **IfName**: Name of the interface • **Is IPv6**: Indicates whether the address is an IPv6 address (true) or an IPv4 address (false) • **Mask**: Mask for the address • **OpId**: Process identifier; for internal use only • **Prefix**: Prefix for the address • **Time**: Date and time the table was generated • **VRF**: Name of the virtual route forwarding (VRF) interface if deployed
MAC Addresses	Displays all known MAC addresses for the switch. This tab provides the following additional data about each address: • **DB State**: Session state of the DB; for internal use only • **Egress Port**: Importance of the event–critical, warning, info, or debug • **Hostname**: User-defined name of the switch • **Last Changed**: Data and time that the address was last updated or deleted • **OpId**: Process identifier; for internal use only • **Origin**: Indicates whether this switch owns this address (true) or if another switch owns this address (false) • **Remote**: Indicates whether this address is reachable via a VXLAN on another switch (true) or is reachable locally on the switch (false) • **Time**: Date and time the table was generated • **VLAN Id**: Identifier of an associated VLAN if deployed
All Interfaces	Displays all known interfaces on the switch. This tab provides the following additional data about each interface: • **Details**: Information about the interface, such as MTU, table number, members, protocols running, VLANs • **Hostname**: Hostname of the given event • **IfName**: Name of the interface • **Last Changed**: Data and time that the interface was last enabled, updated, deleted, or changed state to down • **OpId**: Process identifier; for internal use only • **State**: Indicates if the interface is *up* or *down*

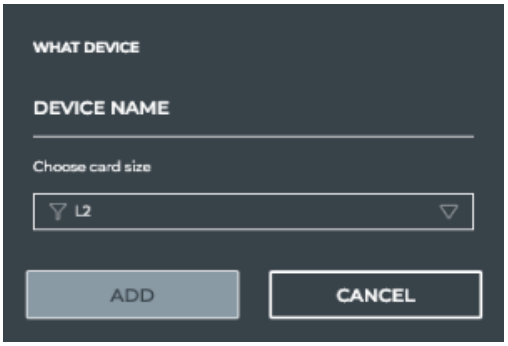
Item	Description
	• **Time**: Date and time the table was generated • **Type**: Kind of interface; for example, VRF, switch port, loopback, ethernet • **VRF**: Name of the associated virtual route forwarding (VRF) interface if deployed
Export	Enables export of all or selected items in a CSV or JSON formatted 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:

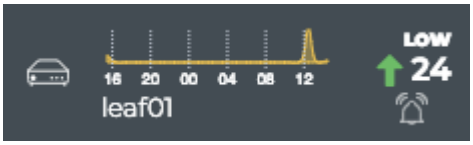
1. Click , and select Devices|Switch. A dialog box opens.



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.



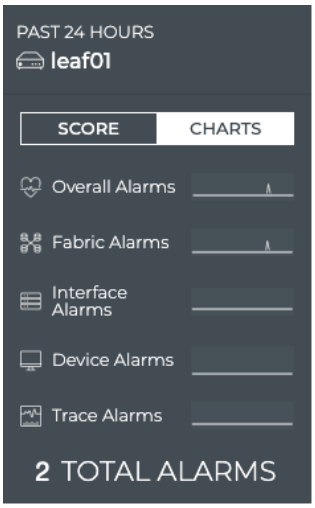
In this example, we see that the leaf01 switch has had very few alarms overall, but the number is trending upward, with a total count of 24 alarms currently.

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:

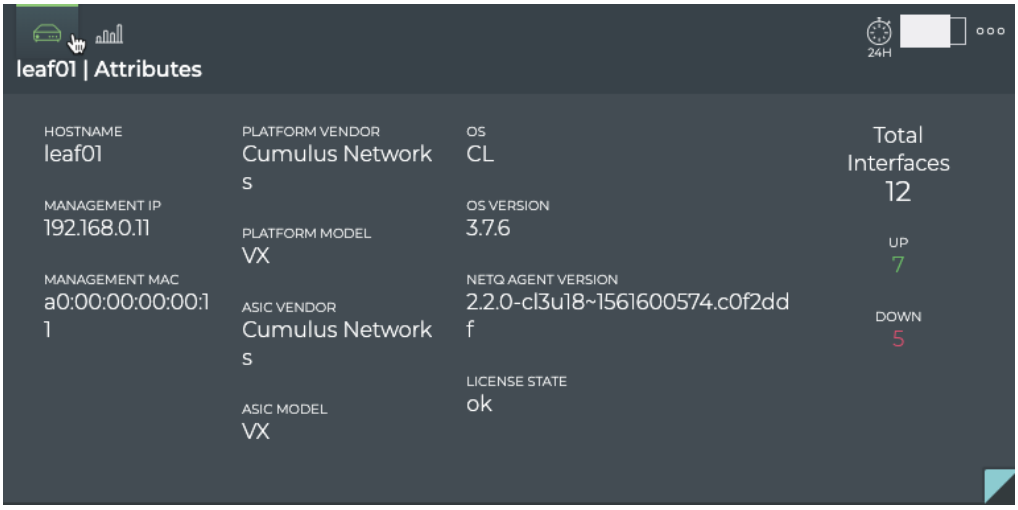
- network services, such as BGP, EVPN, CLAG, NTP, and so forth
- scheduled traces
- interface performance
- platform performance



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 **Score** 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.



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, one displaying hardware-related performance through a series of charts, and one displaying the performance of the network tables, also through a series of charts.

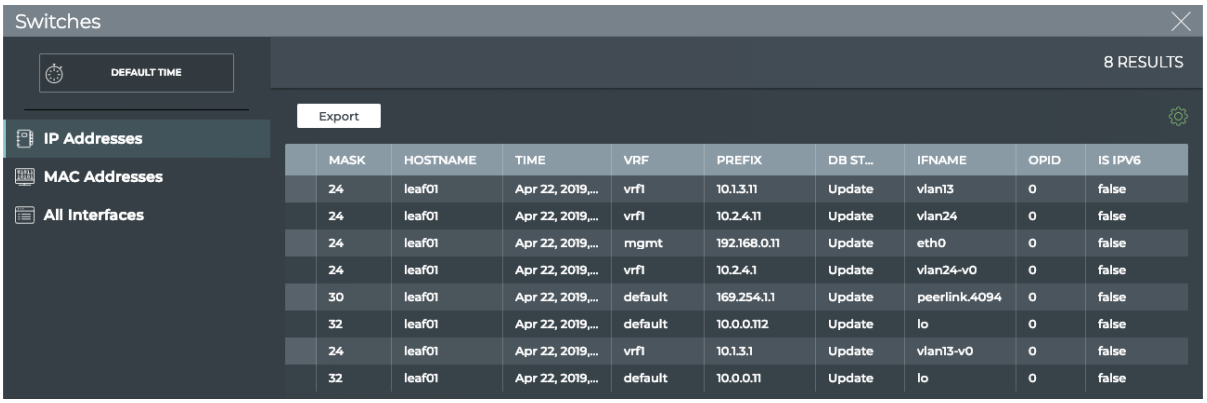
4. Look at the hardware performance charts. Are there any that are reaching critical usage levels? Scroll down to view all available charts.
5. Open a new large Switch card for the same switch and change the time period. Is the performance about the same? Better? Worse? The results can guide your decisions about upgrade options or just times of day when the system is more heavily used.
6. Optionally, filter for a particular chart, by clicking **Filter** above the charts. Begin typing the name of the chart you want to focus on; the charts that match the filter remain, while the others are hidden from view. Delete the filter to see all charts again.
7. Look at the network table performance. Are there any tables that are reaching their maximum size? Does it stay at that level or spike at peak times? Scroll down to view all available charts.
8. Compare this data with that in the second card you opened in step 5. Is the performance about the same? Better? Worse? The results can guide you toward any next steps if needed.
9. Optionally, filter for a particular chart, by clicking **Filter** above the charts. Begin typing the name of the chart you want to focus on; the charts that match the filter remain, while the others are hidden from view. Delete the filter to see all charts again.

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:

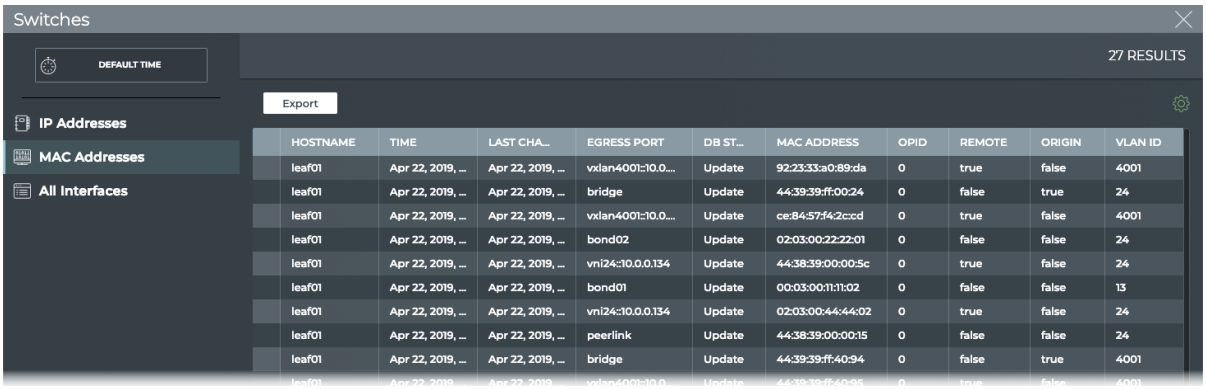
1. Open the full screen Switch card. The **IP addresses** tab is shown by default.



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.



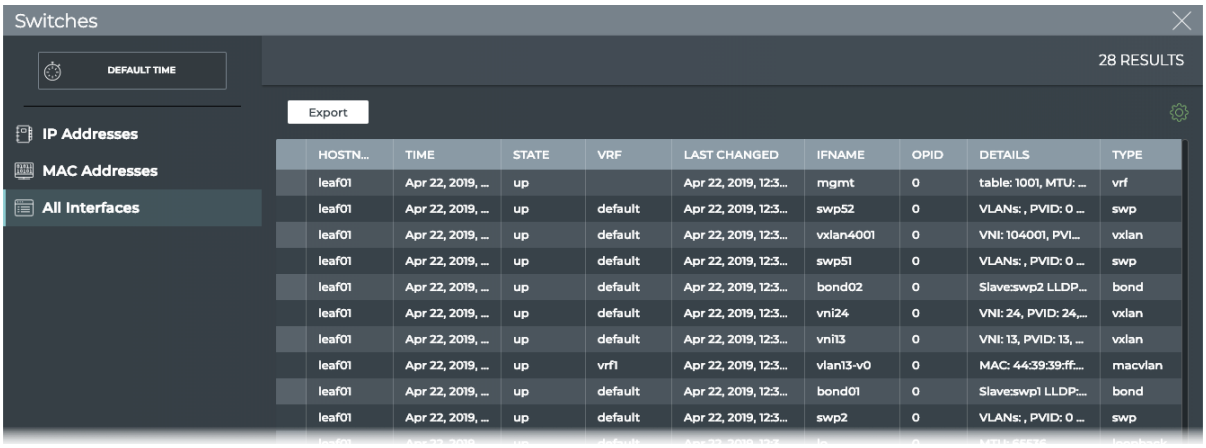
2. Review the addresses for any anomalies, to see the associated egress port, associated VLANs, and so forth.
3. To return to the workbench, click ✕ in the top right corner.

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.



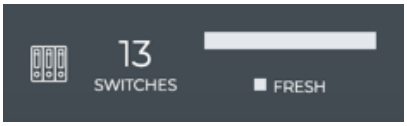
2. Look for interfaces that are down, shown in the **State** column.
3. Look for recent changes to the interfaces, shown in the **Last Changed** column.
4. View details about each interface, shown in the **Details** column.
5. Verify they are of the correct kind for their intended function, shown in 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.

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

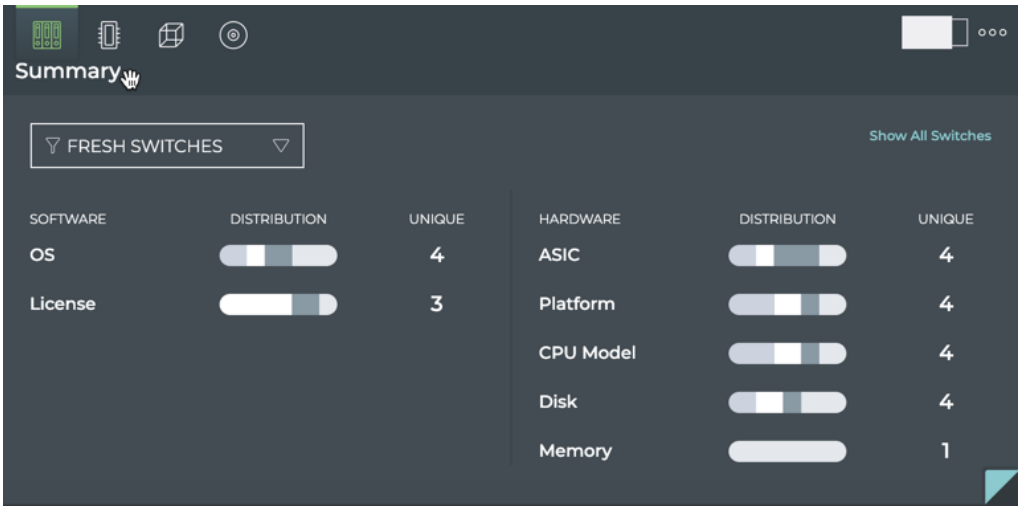
The medium Switch Inventory card displays:

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	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. **Note**: 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.

Item	Description
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.

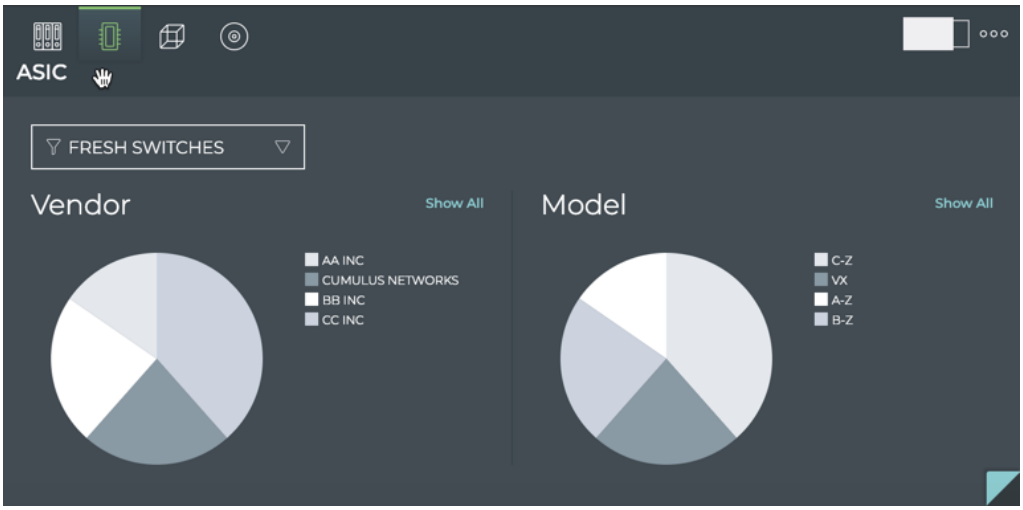
The large Switch Inventory card contains four tabs.

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	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. **Note**: 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.
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 *ASIC* tab displays:

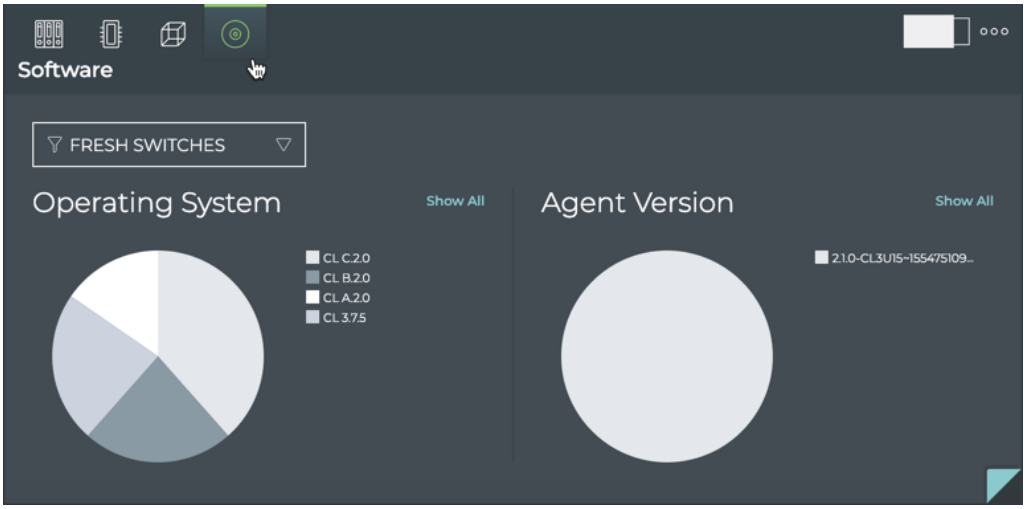


Item	Description
	Indicates data is for ASIC information
Filter	View fresh switches (those you have heard from recently) or rotten switches (those you have not heard from recently) on this card
Vendor chart	Distribution of ASIC vendors. Hover over chart segment to view the number of switches with each 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:

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

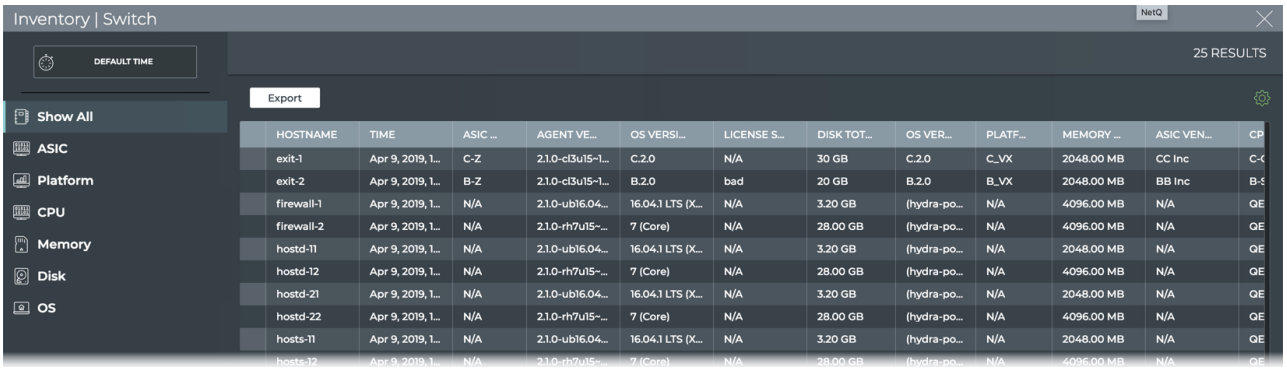
The *Software* tab displays:



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.

Item	Description
Agent Version chart	Distribution of NetQ Agent versions. Hover over chart segment to view the number of switches with each version. **Note**: 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

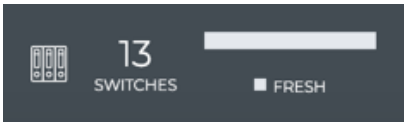
The full screen Switch Inventory card provides tabs for all components, ASIC, platform, CPU, memory, disk, and OS components.



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.

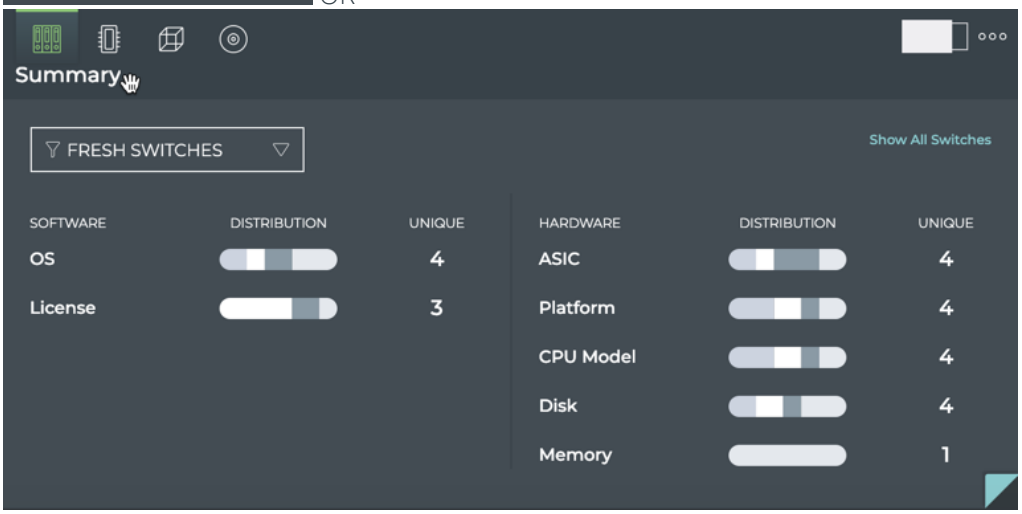
View the Distribution of Any Component Deployed

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

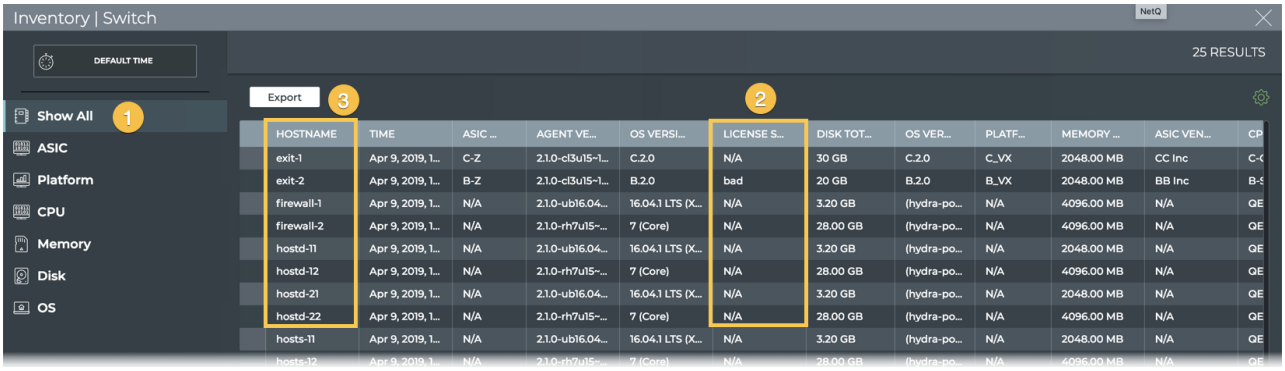
It is important to know when you have switches that have invalid or missing Cumulus Linux licenses, as not all of the features are operational without a valid license. Simply open the medium or large Switch Inventory card, and hover over the License chart to see the count.

To view which vendors and platforms have bad or missing licenses, open the large Switch Inventory card, and click to open the **Platform Details** 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 Details** 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.

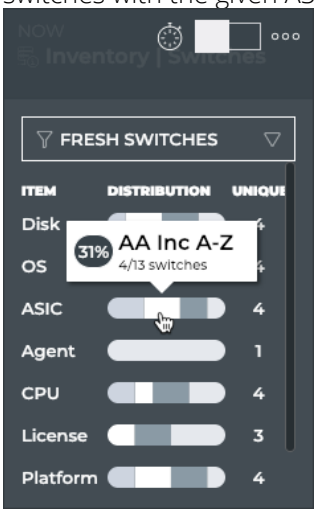


View the Most Commonly Deployed ASIC

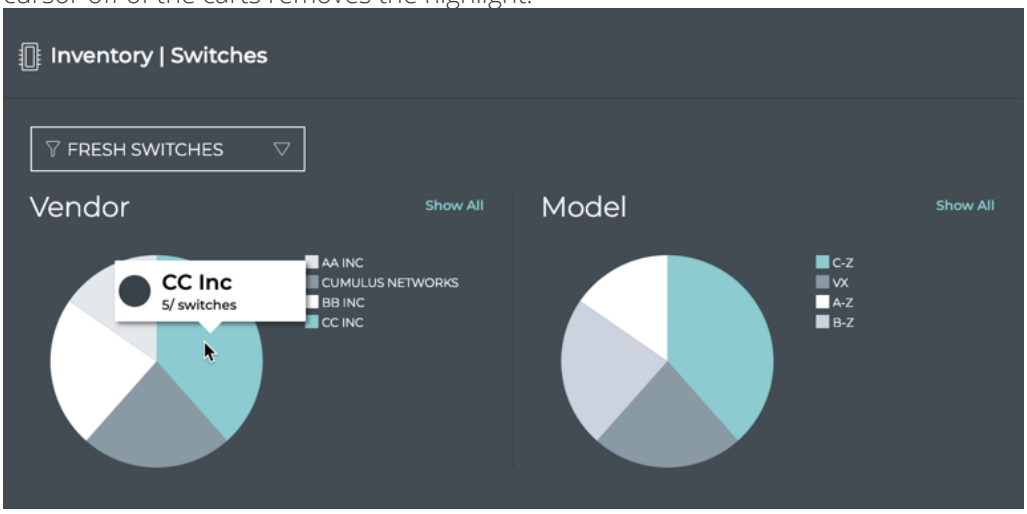
It can be useful to know the quantity and ratio of many components deployed in your network to determine the scope of upgrade tasks, balance vendor reliance, or for detailed troubleshooting. You can view the most commonly deployed components in generally the same way. Some components have additional details contained in large card tabs.

To view the most commonly deployed ASIC, for example:

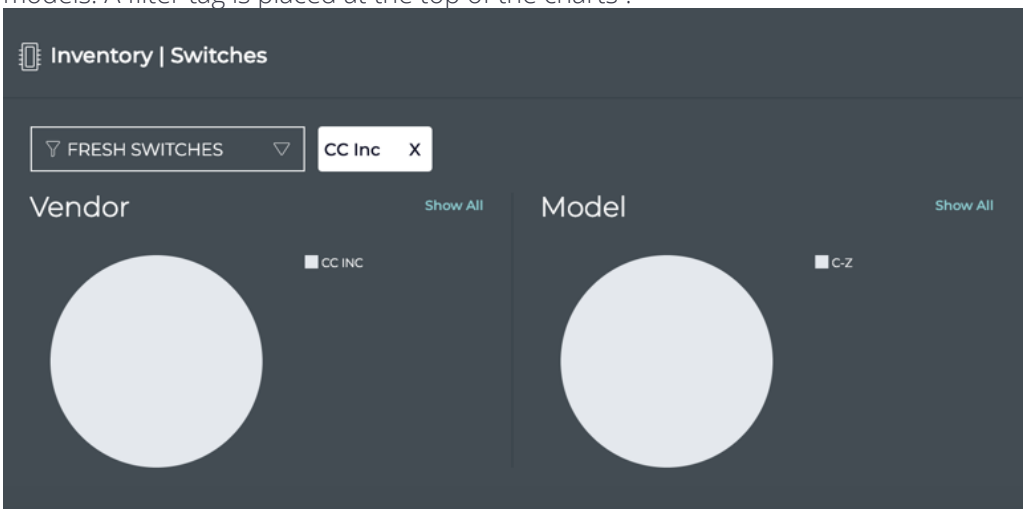
1. Open the medium or large Switch Inventory card.
2. Hover over the *largest* segment in the ASIC chart. The tooltip that appears shows you the number of switches with the given ASIC and the percentage of your entire switch population with this ASIC.



   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, s witch to the large card.
4. Hover over the card, and click to open the **ASIC Details** 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 **Platform** 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 .

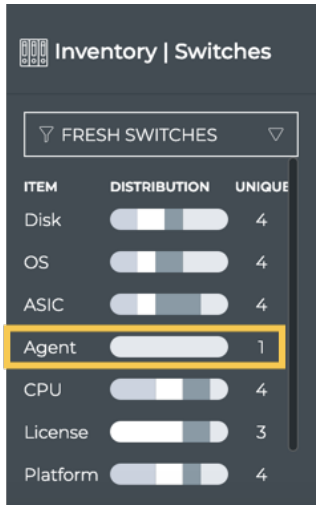


7. To return to the complete view of vendors and platforms, click ✕ on the filter tag.

View the Number of Switches with a Particular NetQ Agent

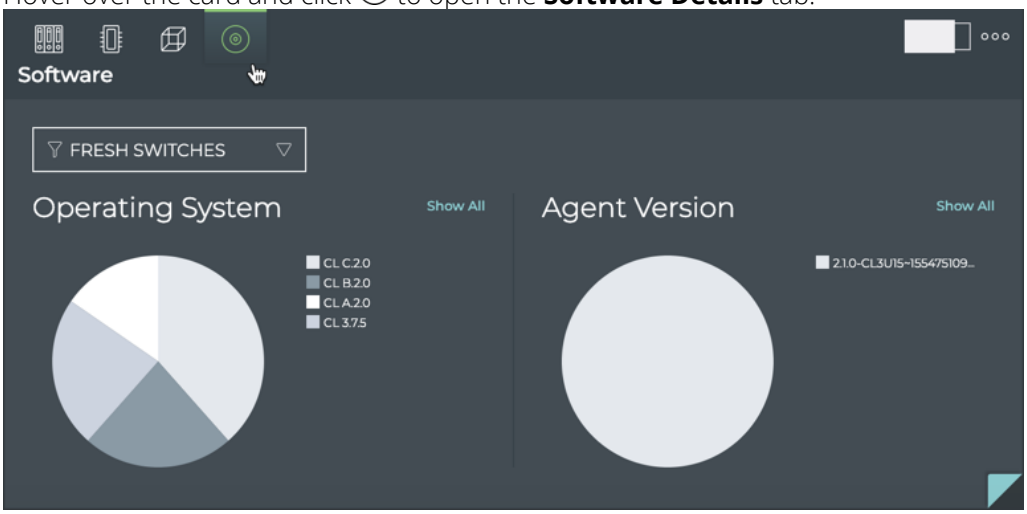
It is recommended that when you upgrade NetQ that you also upgrade the NetQ Agents. You can determine if you have covered all of your agents using the medium or large Switch Inventory card. To view the NetQ Agent distribution by version:

1. Open the medium Switch Inventory card.
2. View the number in the Unique column next to Agent.

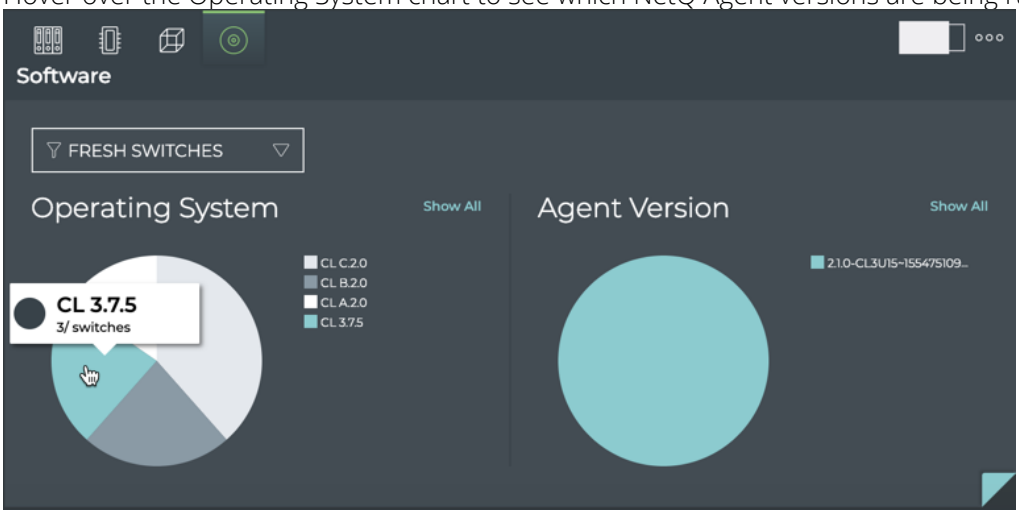


3. If the number is greater than one, you have multiple NetQ Agent versions deployed.
4. If you have multiple versions, hover over the Agent chart to view the count of switches using each version.
5. For more detail, switch to the large Switch Inventory card.

6. Hover over the card and click to open the **Software Details** tab.



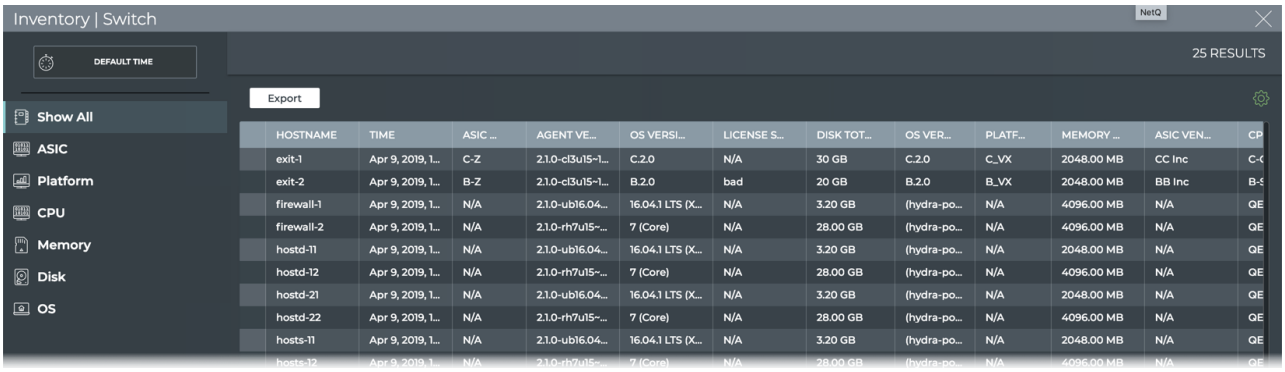
7. Hover over the chart on the right to view the number of switches using the various versions of the NetQ Agent.
8. Hover over the Operating System chart to see which NetQ Agent versions are being run on each OS.



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.

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**.


Inventory | Switch
NetQ
DEFAULT TIME
25 RESULTS
Export
Show All
ASIC
Platform
CPU
Memory
Disk
OS
HOSTNAME TIME ASIC ... AGENT VE... OS VERSI... LICENSE S... DISK TOT... OS VER... PLATF... MEMORY ... ASIC VEN... CP
exit-1 Apr 9, 2019, 1... C-Z 2.1.0-cl3u15~1... C.2.0 N/A 30 GB C.2.0 C_VX 2048.00 MB CC Inc C-
exit-2 Apr 9, 2019, 1... B-Z 2.1.0-cl3u15~1... B.2.0 bad 20 GB B.2.0 B_VX 2048.00 MB BB Inc B-
firewall-1 Apr 9, 2019, 1... N/A 2.1.0-ub16.04... 16.04.1 LTS (X... N/A 3.20 GB (hydra-po... N/A 4096.00 MB N/A QE
firewall-2 Apr 9, 2019, 1... N/A 2.1.0-rh7u15~... 7 (Core) N/A 28.00 GB (hydra-po... N/A 4096.00 MB N/A QE
hostd-11 Apr 9, 2019, 1... N/A 2.1.0-ub16.04... 16.04.1 LTS (X... N/A 3.20 GB (hydra-po... N/A 2048.00 MB N/A QE
hostd-12 Apr 9, 2019, 1... N/A 2.1.0-rh7u15~... 7 (Core) N/A 28.00 GB (hydra-po... N/A 4096.00 MB N/A QE
hostd-21 Apr 9, 2019, 1... N/A 2.1.0-ub16.04... 16.04.1 LTS (X... N/A 3.20 GB (hydra-po... N/A 2048.00 MB N/A QE
hostd-22 Apr 9, 2019, 1... N/A 2.1.0-rh7u15~... 7 (Core) N/A 28.00 GB (hydra-po... N/A 4096.00 MB N/A QE
hosts-11 Apr 9, 2019, 1... N/A 2.1.0-ub16.04... 16.04.1 LTS (X... N/A 3.20 GB (hydra-po... N/A 2048.00 MB N/A QE
hosts-12 Apr 9, 2019, 1... N/A 2.1.0-rh7u15~... 7 (Core) N/A 28.00 GB (hydra-po... N/A 4096.00 MB N/A QE