

Cisco Nexus Dashboard Insights Analysis Hub, Release 6.5.x - For Cisco NDFC or Standalone NX-OS

Table of Contents

New and Changed Information . . . 2
Conformance Report . . . 4
  Conformance Report . . . 4
  Access Conformance Report . . . 5
  View Conformance Report . . . 5
Connectivity Analysis . . . 7
  Connectivity Analysis . . . 7
  Guidelines and Limitations . . . 8
  Create Connectivity Analysis. . . . 10
  View Connectivity Analysis . . . 11
  Manage Connectivity Analysis . . . 17
  Filtering Information . . . 18
Log Collector . . . 20
  Log Collector . . . 20
  Uploading logs to Cisco Intersight Cloud . . . 20
  Log Collector Dashboard . . . 21
  TAC Initiated Log Collector . . . 22
Traffic Analytics . . . 23
  Traffic Analytics . . . 23
  Guidelines and limitations for Traffic Analytics . . . 24
  Configure Traffic Analytics . . . 25
  View Traffic Analytics . . . 26
  Manage Service Endpoint Categories . . . 33
  View Traffic Analytics for Endpoints . . . 34
  Flow Troubleshoot Workflow . . . 34
Sustainability Report . . . 37
  Sustainability Report . . . 37
  View the sustainability report for switches . . . 38
  View the sustainability report for PDUs . . . 41
Delta Analysis . . . 44
  Delta Analysis . . . 44
  Guidelines and Limitations for Delta Analysis . . . 44
  Create Delta Analysis . . . 45
  View Delta Analysis . . . 45
  View Health Delta Analysis . . . 46
  View Policy Delta Analysis . . . 48
Bug Scan . . . 49
  Collecting information on bugs that might affect your network using Bug Scan . . . 49
  View Active and Susceptible Bugs . . . 50
Copyright . . . 53

First Published: 2024-07-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
Support for Traffic Analytics on Classic LAN fabrics	Beginning with NDI release 6.5.2, Traffic Analytics on Classic LAN fabrics is supported, but only over out-of-band (OOB) management ports.	6.5.2	Guidelines and limitations for Traffic Analytics
Bug descriptions included for Bug Scan	The table of bugs in the Bugs area of Bug Scan now includes a description of each bug.	6.5.1	
Sustainability report top 5 devices	The sustainability report now shows the top 5 devices for the highest estimated cost, most energy consumed, and highest estimated greenhouse gas (GHG) emissions.	6.5.1	View the sustainability report for switches
Use of the Cisco Energy Manager instead of Electricity Maps	Nexus Dashboard Insights now obtains the energy cost and greenhouse gas (GHG) emissions data from the Cisco Energy Manager instead of from Electricity Maps. Using the Cisco Energy Manager provides a more robust method for collecting the data by avoiding a possible single point of failure or absence of data for a region.	6.5.1	Sustainability Report

Feature	Description	Release	Where Documented
Operations, Administration, and Maintenance (OAM) support for NDFC in Connectivity Analysis	OAM option in Connectivity Analysis enable you to locate potential drops for active hosts or to track details such as reachability and actual route of the flow in a VXLAN EVPN based fabric topology, without the need of active traffic between the hosts.	6.5.1	Connectivity Analysis
Terminology change	The term " sites" is renamed to " fabrics" .	6.5.1	Entire document

This document is available from your Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit Cisco Nexus Dashboard Insights Documentation.

Conformance Report

Conformance Report

Conformance report enables you to visualize and understand the lifecycle of your hardware and software in the network. This assists you in planning upgrades and hardware refresh. Conformance Report is generated everyday for each fabric for hardware and software conformance and weekly for each fabric for scale conformance. In the report you can view the conformance status of software, hardware, combination of both software and hardware, and scale conformance status for fabrics.

You can use Conformance Report to view current and project the future status of software and hardware inventory in your network against known EoS and EoL notices to ensure conformance. You can also monitor scale conformance status for onboarded fabrics.

Using Conformance Report you can,

- Minimize risk of running End-of-Sale (EoS) or End-of-Life (EoL) switches.
- View current status of software and hardware inventory in your network against known EoS and EoL notices to ensure conformance.
- Project the future outlook of software and hardware inventory in your network.
- Monitor scale conformance status for onboarded fabrics.

Conformance Report displays the summary of conformance status for software, hardware, and scale for selected fabrics.

In the Conformance report, for hardware and software conformance switches are classified into 3 severities based on the software release or hardware platform EoL dates and end of PSIRT dates. The severities include:

- Critical: End of PSIRT date or Last Date of Support occurs in the past.
- Warning: EoL date for software release or EoS for hardware release occurs in the past.
- Healthy: End of PSIRT date, or Last Date of Support and EoL date or software release or EoS for hardware release occurs in the future, or EoL for software release or EoS for hardware release is not announced.

The End of SW Maintenance Releases Date in the End-of-Sale and End-of-Life Announcement and the end of PSIRT date is used as reference milestone to classify the inventory into a category of Critical, Warning, or Healthy.

In the Conformance report, the scale conformance status for fabrics is based on Cisco’s Verified Scalability Guidelines for the software version running in switches and controllers when applicable. The severities include:

- Conformant: All metric values are under 90%.
- Approaching limits: One or more metric values are between 90% and 100%.

- Violated Limits: One or more metric values are over 100%.

Access Conformance Report

Navigate to **Analyze** > **Analysis Hub** > **Conformance**.

Select a fabric from the dropdown menu.

OR

Navigate to **Operate** > **Fabrics**.

Select a Fabric.

In the General section, click **Conformance**.

Click **View Report**.

View Conformance Report



You can save conformance report as a PDF with the browser print option (Only supported on Chrome and Firefox).

1. Navigate to a Conformance Report. See Access Conformance Report.
2. Select a fabric or All Fabrics from the dropdown menu.
3. Select a Current month or a previous month from the dropdown menu. You can select a previous month only if previous month reports are available.

   Conformance Report displays conformance summary, hardware and software conformance, and scale conformance.

4. The Summary page displays devices by hardware conformance status, devices by software conformance status and scale conformance status for fabrics or switches. Click View Conformance Criteria to learn more.
5. The Hardware or Software page displays conformance status, conformance outlook, and device details.
   a. In the Conformance Outlook section, click **Overall**, or **Software**, or **Hardware** to view the conformance for software and hardware, software only or hardware only.
   b. The Device Details lists details for hardware and software.
   c. The details for hardware include device name, fabric name, hardware conformance status, model, role, hardware end of vulnerability support for a particular device. Click device name to view additional details.
   d. The details for software include device name, fabric name, software conformance status, model, software version, role, software end of vulnerability support for a particular device. Click device name to view additional details.
   e. Use search to filter by attributes such as device, fabric, hardware conformance status, software conformance status, model, software version, and role.

f. Use the gear icon to customize the columns in the table.

6. The Scale page displays all fabrics summary, scale conformance, and scale metrics.
    a. The All Fabrics Summary section displays overall scale conformance level, top 5 switches by scalability metric violations, scalability metrics for controller and switches, and total scalability metrics violations.
    b. Click View Conformance Criteria to learn more.
    c. The Scale Conformance section displays the scale conformance for controller and switch in the last 6 months if the scale reports for previous months are available.
    d. The All Scale Metrics section displays the scale metrics details for fabrics and switches. The All Scale Metrics section is displayed, if you select All fabrics from the drop-down menu.
        i. The details for fabrics include fabric name, type, software version, controller metrics conformance, switch metrics conformance. Click fabric name to view additional details.
        ii. The details for switches include switch name, fabric name, software version, model, forward scale profile, metrics conformance. Click switch name to view additional details.
        iii. Use search to filter by attributes such as fabric, type, software version.
        iv. Use the gear icon to customize the columns in the table.
    e. The Fabric Level Scale Metrics and Switch Level Scale Metrics displays the scale metrics details for a fabric and switches associated with the fabric. These sections are dispayed, if you select one fabric from the drop-down menu.
        i. The details for a fabric include metric, conformance status, and resource usage,
        ii. The details for switches include switch name, fabric name, software version, model, forward scale profile, metrics conformance. Click switch name to view additional details.
7. From the Actions menu, click **Run Report** to run an on-demand report.

Connectivity Analysis

Connectivity Analysis

Connectivity Analysis allows you to analyze flows between two different endpoints, provide insight into how your endpoints are connected, and helps you spot where problems might be occurring.

Connectivity Analysis detects and isolates offending nodes in the network for a given flow and includes the following functionalities:

- Traces all possible forwarding paths for a given flow across source to destination endpoints.
- Identifies the offending device with issue, resulting in the flow drop.
- Helps troubleshoot to narrow down the root cause of the issue, including running forwarding path checks, software and hardware states programming inconsistencies through consistency-checks, and further details related to packets walkthrough.

Connectivity Analysis Options

- Embedded Logic Analyzer Module (ELAM) - ELAM is a diagnostic tool that helps troubleshoot ethernet traffic flows. It captures the packet from an active flow and analyzes the ethernet frames for packet drops. ELAM requires an active flow between the source and destination hosts. You can enable this option to analyze an available active flow.
- Operations, Administration, and Maintenance (OAM) - OAM is a protocol for monitoring and troubleshooting ethernet networks. You can enable this option to locate potential drops for active hosts or to track details such as reachability and probable route of the flow in a VXLAN EVPN based fabric topology, without the need of active traffic between the hosts. OAM is supported only on VXLAN fabrics.
- Consistency Checker - Consistency Checker ensures system consistency and aids in root cause analysis and fault isolation by verifying the alignment between software and hardware tables. These checks are performed within each switch between data plane and control plane for all the networking entities related to the chosen endpoint conversation. You can enable this option to detect control plane and data plane configuration and operational inconsistencies along the flow between specified endpoints or routes.

Layer 2 ToR Support

With Layer 2 ToR support, Connectivity Analysis offers the following capabilities:

- Incorporate the device into the topology of a connectivity analysis job.
- Provide detailed node-level flow information, including ingress interfaces and egress paths.
- Initiate ELAM (Embedded Logic Analyzer Module) and capture packet details on ToR switches.
- Conduct consistency-check validations on ToR switches.

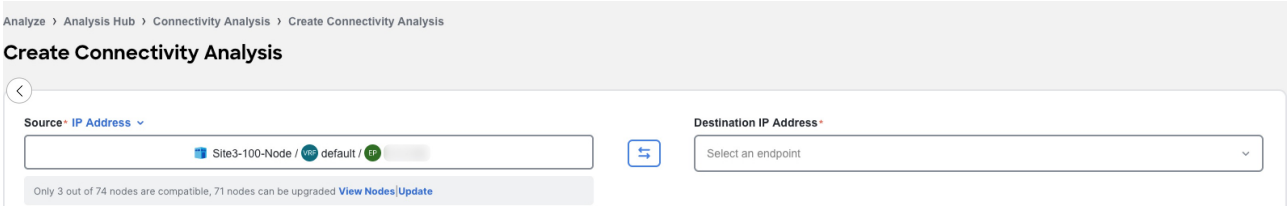
Supported topologies

- ToR switch with port channel directly connected to leaf switch.
- ToR switch connected to leaf switches in a vPC pair.

- ToR switches with port channels connected to leaf switches individually. The leaf switches are in a vPC pair.
- ToR switches in vPC with leaf switches along with ToR switches connected to hosts in a vPC pair.

Guidelines and Limitations

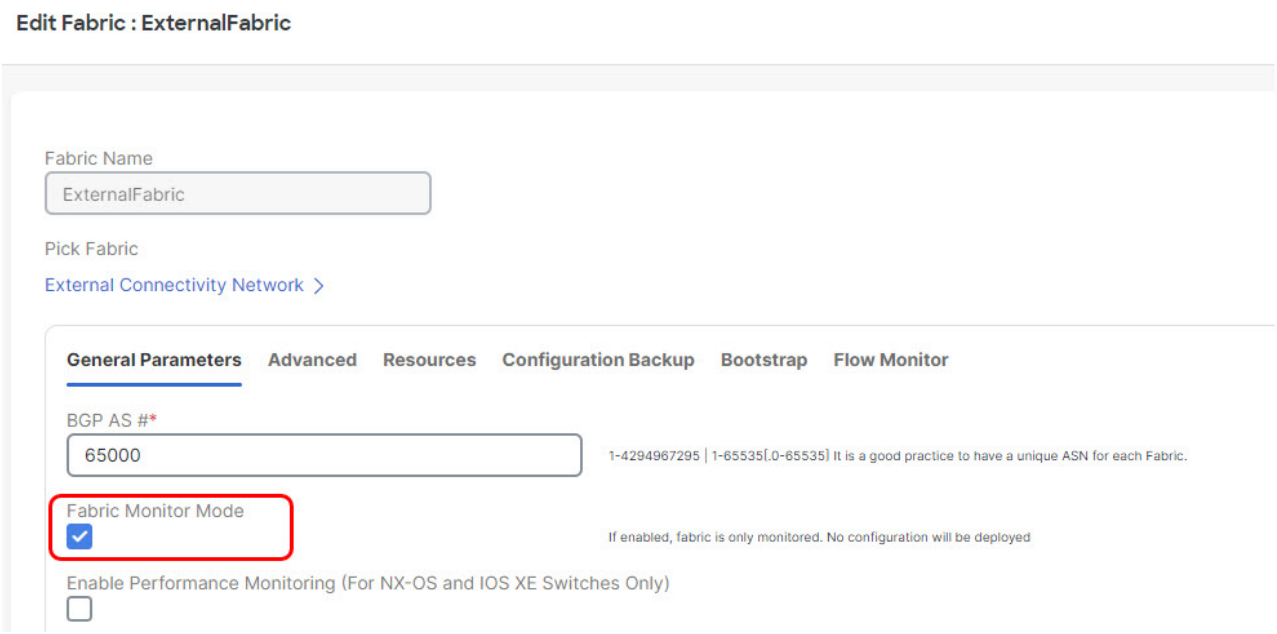
- You can submit up to 10 jobs per fabric.
- At any point of time, you can run only 1 Connectivity Analysis job per fabric. You can stop a job in the queue and run another job.
- Connectivity Analysis is supported on Cisco NX-OS release 9.3(7a) and later.
- Connectivity Analysis job is not triggered if all onboraded devices are shown as incompatible.
- You must upgrade to the latest available RPM. Upgrading the RPM has no impact on traffic forwarding or on the switch and switch reload is not required. The View Nodes banner displays the number of nodes that are compatible and up to date. Click **Update** to upgrade. After the upgrade is completed, in the Node page, click **Refresh** to view the status.



- OAM is only supported on VXLAN fabrics.
- OAM is only supported between VTEPS and as a result the OAM path will be displayed between Layer 3 networks.
- You can run Connectivity Analysis only on online fabrics.
- Connectivity Analysis requires endpoints to be local to the fabric.

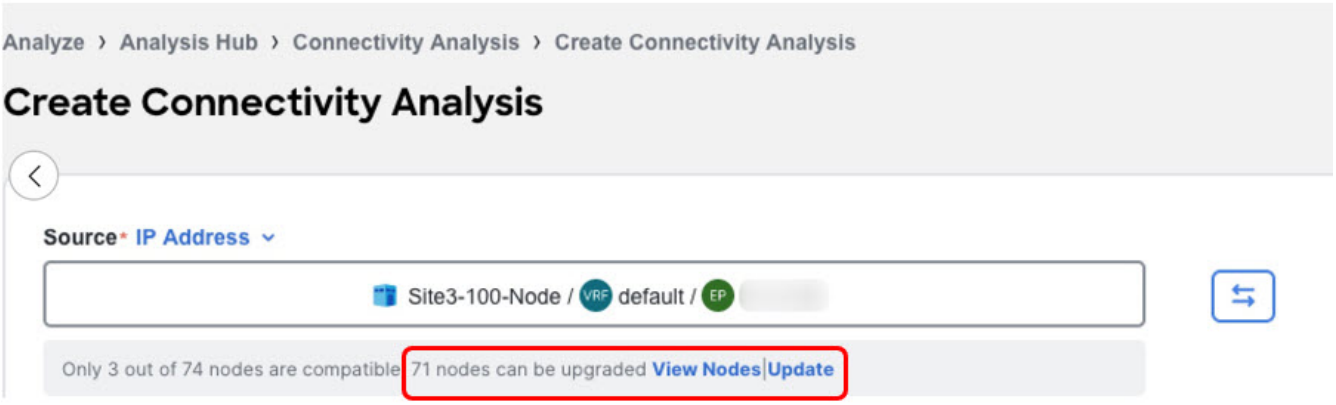
Additional Guidelines for NDFC Fabrics in Monitor Mode

- NDFC has two fabric types (Classic LAN and External Connectivity Network) which support the Fabric Monitor Mode. Fabric Monitor Mode disables the ability to make any changes to the corresponding fabric.
- Connectivity Analysis depends on switch-side RPMs to function. These RPMs typically ship installed on the switches, but when updates become available, they must be deployed from Nexus Dashboard Insights.
- If a fabric has **Fabric Monitor Mode** enabled, Nexus Dashboard Insights cannot push the RPM updates as required.



Attempting to install RPM updates from Nexus Dashboard Insights to NDFC switches with Fabric Monitor Mode enabled will result in a failed task.

- If Connectivity Analysis shows an RPM update available for the switches, you will need to first disable the Fabric Monitor Mode for the respective fabric from NDFC, then perform the RPM update from Connectivity Analysis on Nexus Dashboard Insights.



- Once the update is completed, you can re-enable Fabric Monitor Mode on NDFC to use Connectivity Analysis with the switches.

Supported Topologies

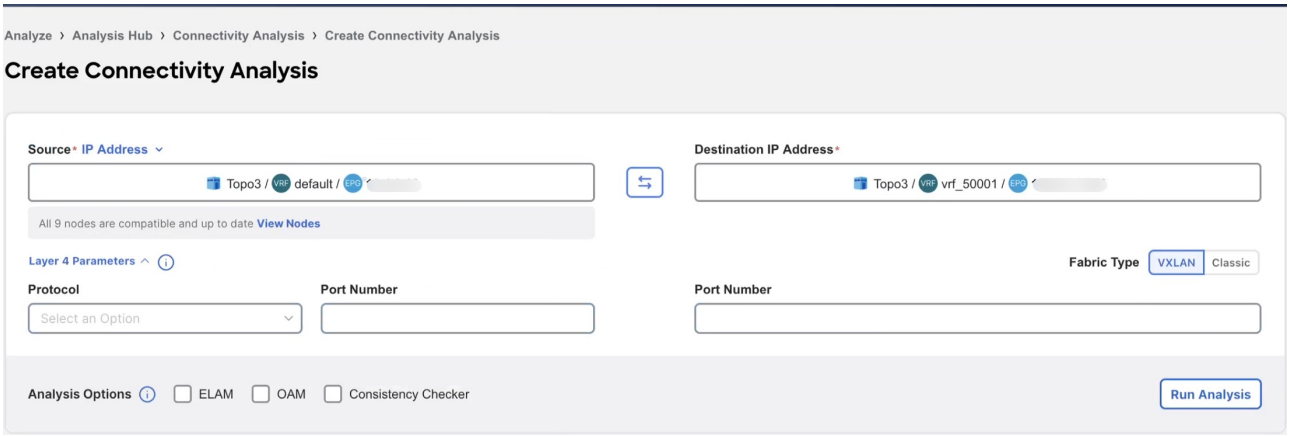
- Endpoint combinations:
  - EP-EP
  - EP - L3OUT
  - L3Out - EP
  - L3Out - L3Out
- Conversation types:
  - L2, L3, L4 (TCP/UDP)
  - V4 and V6 support

- Transit and Proxy flows
- Shared Service

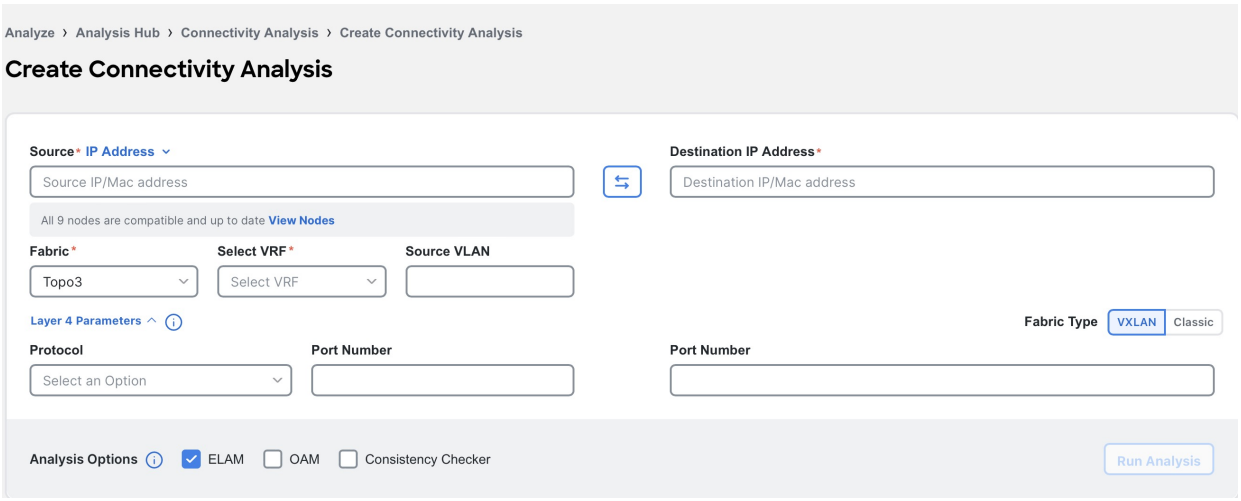
- Topologies:
  - VXLAN
  - vPC
  - Classic LAN

Create Connectivity Analysis.

1. Navigate to **Analyze** > **Analysis Hub** > **Connectivity Analysis**.
2. Click **Create Connectivity Analysis**.



3. Complete the following for Layer2 and Layer 3 parameters.
   a. From the Source drop-down list choose **IP address** or **MAC address** to analyze the flow between two endpoints.
   b. Choose the source IP or MAC address from the drop-down list or enter the source IP or MAC address. A maximum of 20 IP or MAC addresses are displayed at a given time.
   c. You can also manually populate the Layer2 and Layer 3 parameters. Click **Edit Details Manually** to enter the source IP or MAC address, destination IP or MAC address, fabric type, VRF, and source VLAN.



   d. The View Nodes banner displays the number of nodes that are compatible and up to date.

Click **View Nodes** to view the list of nodes and details such as name, serial number, device version, current and latest CA version, platform, fabric, compatibility, and status. Click **Update** to upgrade the Cisco Nexus Insights Cloud Connector (NICC) RPM of the switches. After the upgrade is completed, in the Node page, click **Refresh** to view the status.

e. From the Destination drop-down list choose IP address or MAC address to analyze the flow between two endpoints.

f. Choose the destination IP or MAC address from the drop-down list or enter the destination IP or MAC address.

4. Choose VXLAN or Classic fabric type.
5. Complete the following for Layer 4 parameters.
   a. From the Protocol drop-down menu, choose TCP or UDP protocol.
   b. Enter the source and destination port number.
6. Select the Analysis Option.
   a. Check ELAM option to analyze an available active flow.
   b. Check OAM option to locate potential drops for active hosts or to track details such as reachability and actual route of the flow in a VXLAN EVPN based fabric topology, without the need of active traffic between the hosts. OAM is supported only on VXLAN Fabric.
   c. Check Consistency Checker option to detect control plane and data plane configuration and operational inconsistencies along the flow between specified endpoints or routes.



You cannot select both ELAM and OAM options for Connectivity Analysis.

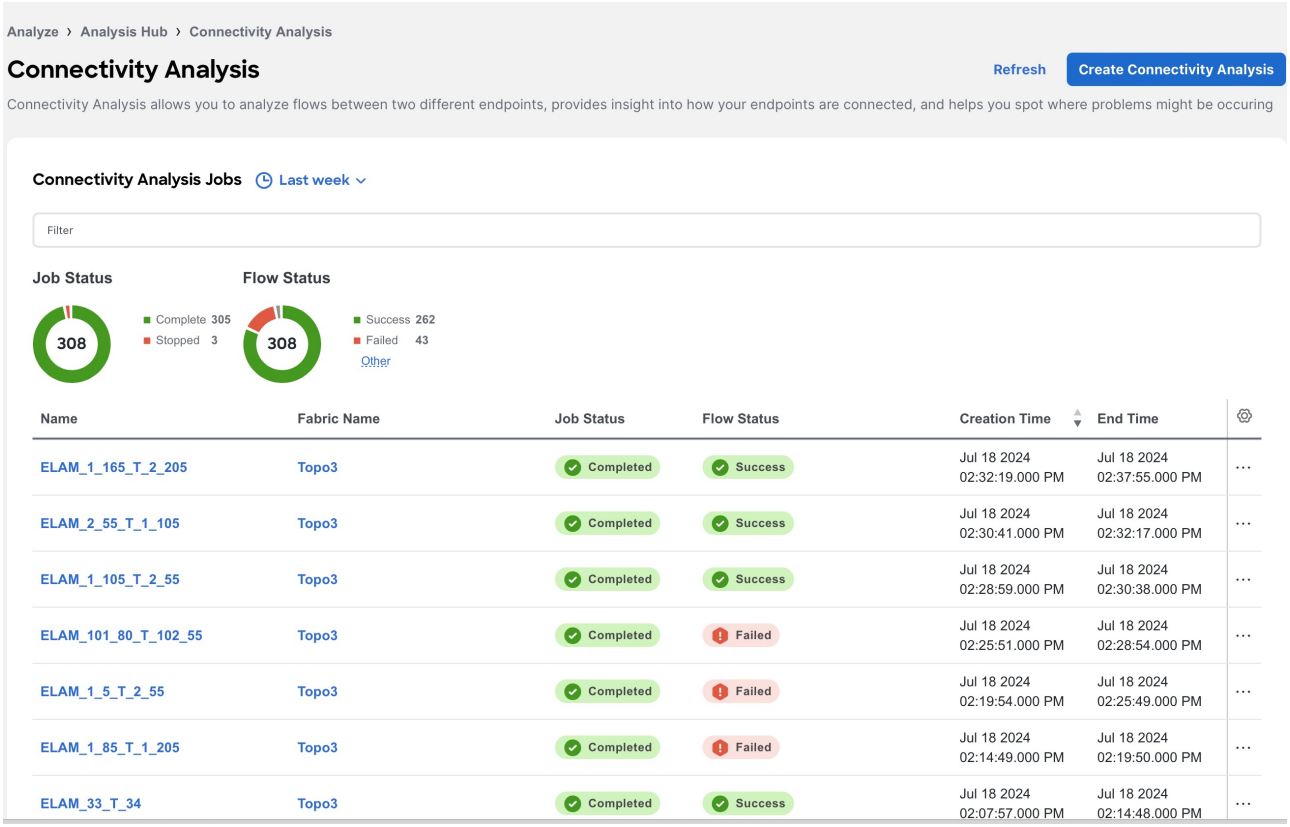
7. Click **Run Analysis**.
8. After the Connectivity Analysis is completed, the analysis is displayed in the **Connectivity Analysis Jobs** table. Navigate to **Analyze** > **Analysis Hub** > **Connectivity Analysis** to view the Connectivity Analysis Jobs. The Analysis is assigned a default name and you can rename the analysis.
   a. Select the analysis and then from the Actions drop-down menu click **Rename Analysis** to rename.

OR

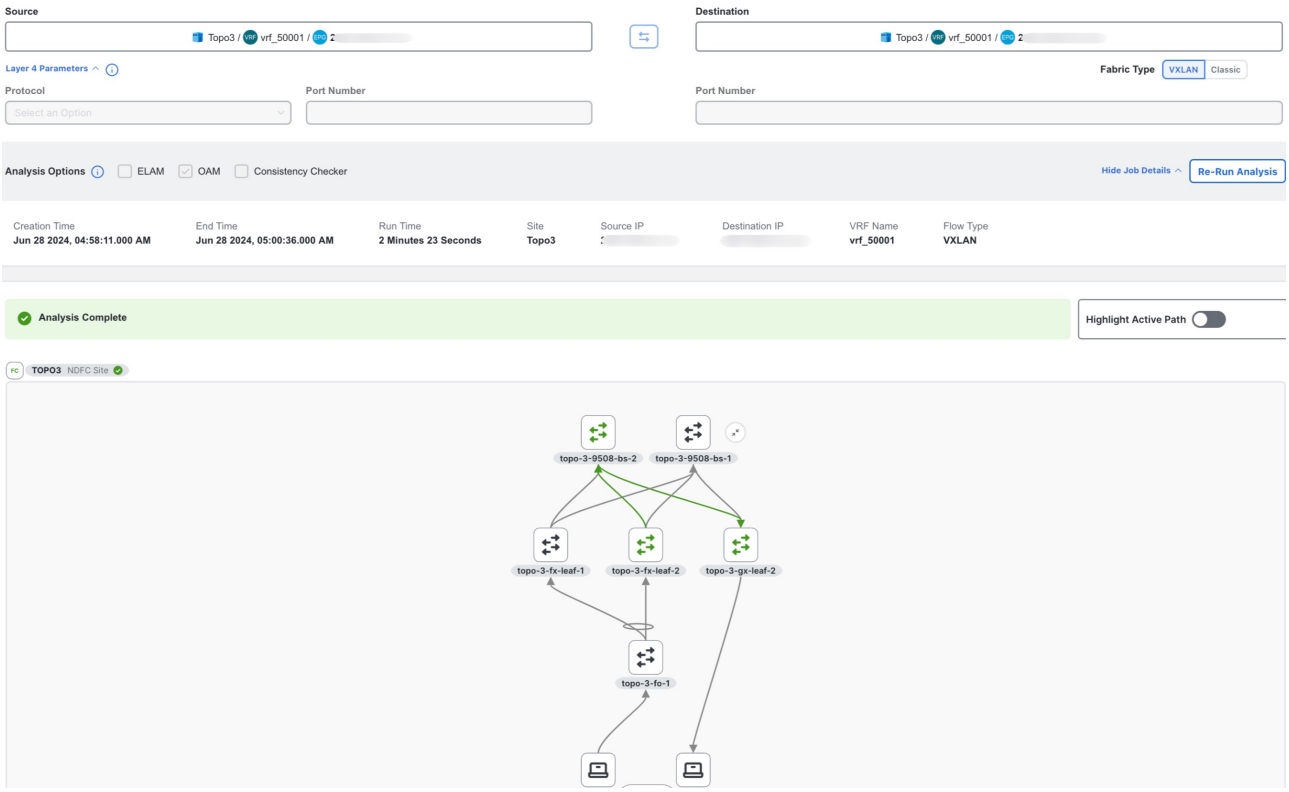
a. Click on analysis name. In the View Connectivity Analysis page, from the Actions drop-down menu click **Rename Analysis** to rename.

View Connectivity Analysis

1. Navigate to **Analyze** > **Analysis Hub** > **Connectivity Analysis**. The Connectivity Analysis jobs are displayed.



2. Choose a time range from the drop-down menu.
3. The Summary area displays the overall status of the Connectivity Analysis jobs and the flow status.
4. Use the filter bar to filter the analysis. The Connectivity Analysis table displays filtered jobs.
   a. Click the column heading to sort the jobs in the table.
   b. Click the gear icon to configure the columns in the table.
   c. Hover around a failed Flow Status to learn more.
5. Click **Name** to view Connectivity Analysis details. The View Connectivity Analysis page displays the input parameters you had entered for the job, the job details, and topology.

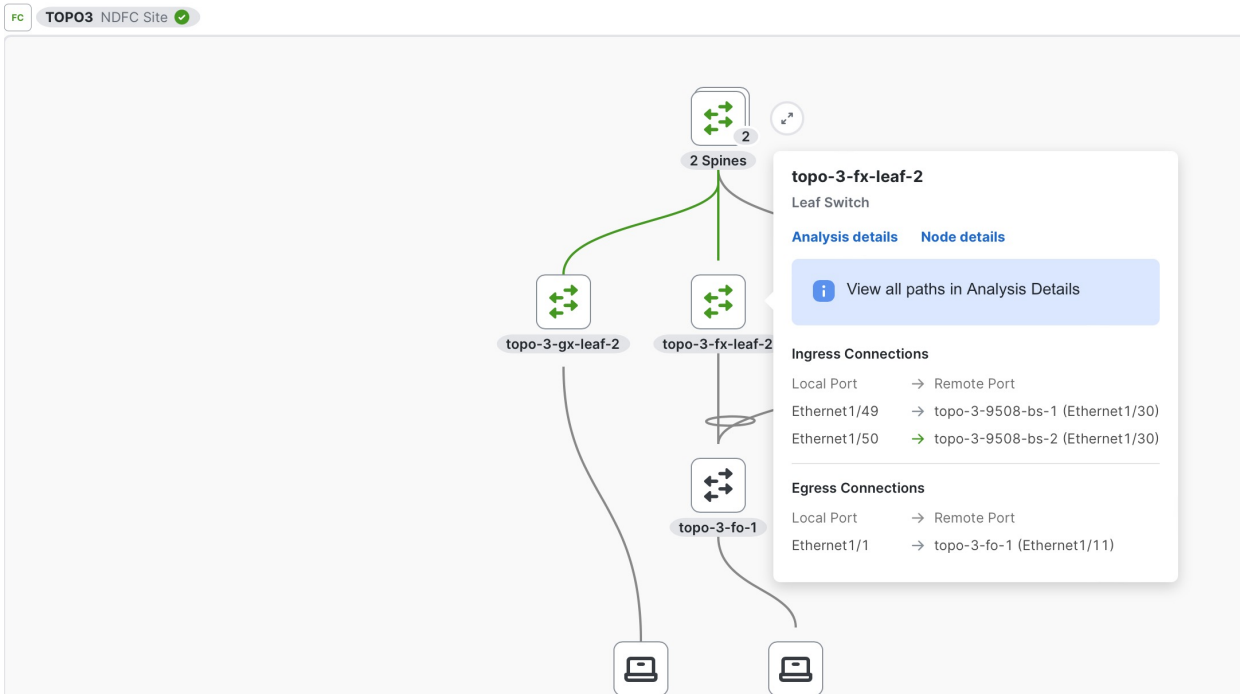


a. Click **Show Job Details** to view the job details such as creation time, end time, run time, fabric, source IP, destination IP, VRF name, source port, destination port, protocol, and flow type. The banner displays the status of the job. A green banner represents a successful analysis and a red banner represents a failed analysis.

b. Use toggle enable or disable **Highlight Active Path**. When you enable **Highlight Active Path**, all the OAM paths in the topology are highlighted.

c. Click **Re-run Analysis** to run the analysis again.

d. In the topology area, you can visualize hierarchial view of the fabric. You can double-click on the node to view interconnections of the nodes in the fabric. The active path between nodes is highlighted in green color. See Topology.



e. Click a node to view the tooltip. The tooltip displays the node name, node type, and the ingress and egress connections for that node, and OAM information if applicable. In the ingress and egress connections, only physical interfaces are displayed and egress information is not displayed on the first VTEP node.

f. Click **Analysis Details** to view the path and data plane information.

   i. Click **Paths** to view path details such as ingress and egress information, and OAM information if applicable. In the ingress and egress connections area logical interfaces are displayed.

   ii. Click **Data Plane** to view the analysis options results.

   iii. Click **ELAM** to view the ELAM report. Click **View Full Report** to download the report.

Analysis Results for topo-3-fx-leaf-1

Paths | Data Plane

Data Plane Details

ELAM

Basic Information

Incoming Interface	**Ethernet1/1**

Outer L2 Header

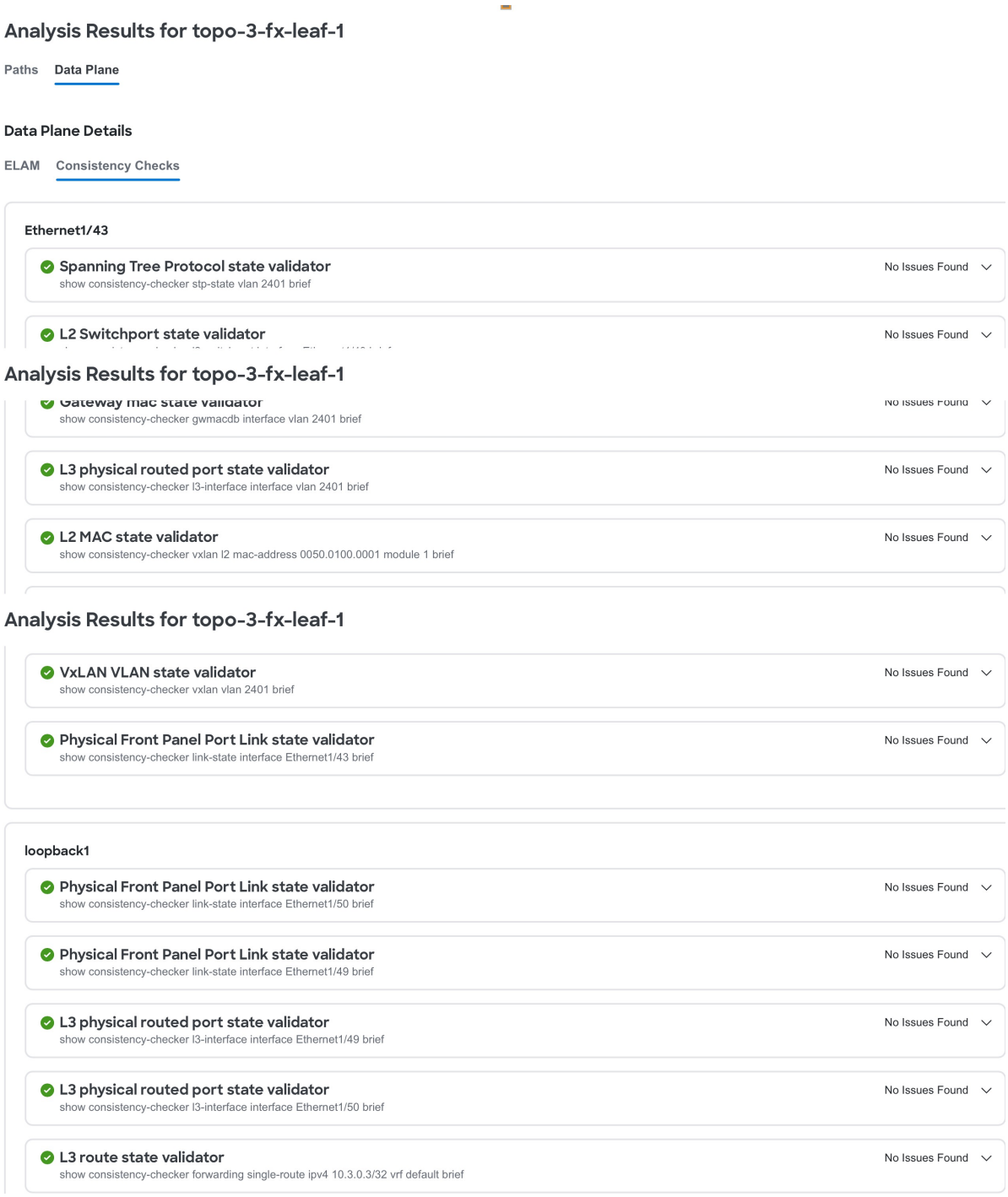
802.1Q tag is valid	**yes(0x1)**
Access Encap VLAN	**2301(0x8FD)**
CoS	**0(0x0)**
Destination MAC	**0017.0100.0001**
Source MAC	**0011.0100.0001**

Outer L3 Header

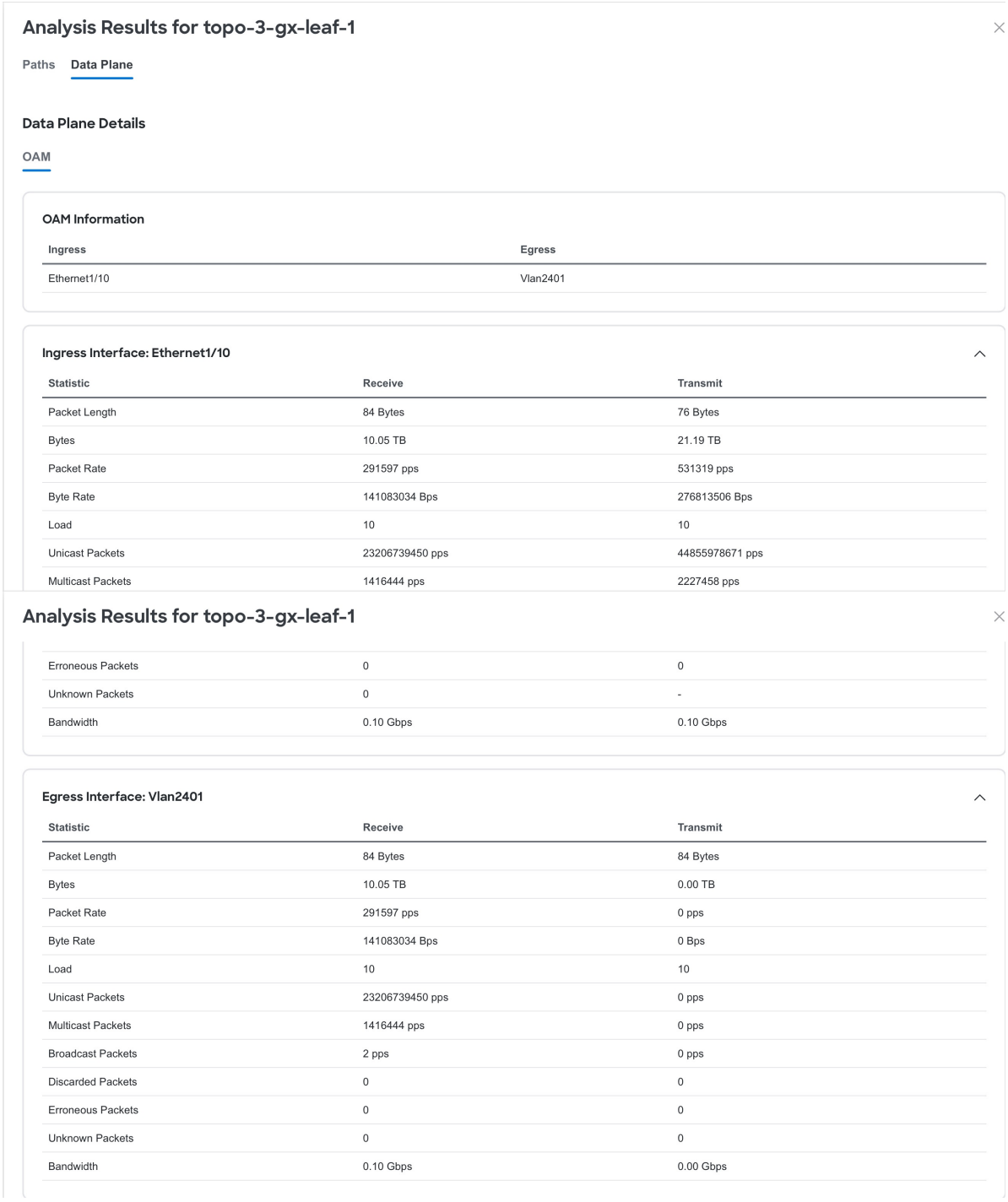
DSCP	**0**
Destination IP	**182.31.1.165**
Don't Fragment Bit	**not set**
IP CheckSum	**2927(0xB6F)**
IP Packet Length	**106(= IP header + IP payload)**
IP Protocol Number	**undefined**
IP Version	**4**
L3 Type	**IPv4**
Source IP	**182.31.1.5**
TTL	**64**

View Full Report

iv. Click **Consistency Checks** to view the consistency check results.



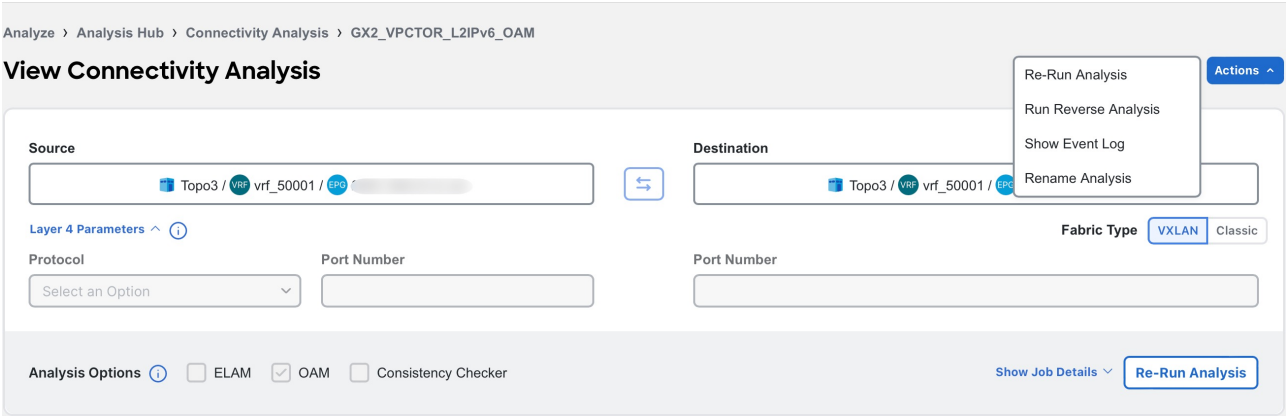
v. Click **OAM** to view the OAM report.



g. Click **Node Details** to view the node details in inventory. See Inventory.

Manage Connectivity Analysis

1. Navigate to **Analyze** > **Analysis Hub** > **Connectivity Analysis**.
2. Click **Name** to view Connectivity Analysis details.



3. From the Actions drop-down menu choose **Re-Run Analysis** to run the analysis again.
4. From the Actions drop-down menu choose **Run Reverse Analysis** to run the analysis in the reverse direction.
5. From the Actions drop-down menu choose **Show Event Log** to view the logs for the analysis. In the event log, you can view the error message for a failed analysis.
6. From the Actions drop-down menu choose **Rename Analysis** to rename the analysis.

Filtering Information

In some cases, you might be able to filter results to find information more easily.

For example, you might have a situation where there a large number of endpoints under a single leaf switch, but you are only interested in endpoints that have a certain VLAN value.

You could filter the information to show only those specific endpoints in this situation.

Use the following operators for the filter refinement:

Operator	Description
==	With the initial filter type, this operator, and a subsequent value, returns an exact match.
!=	With the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
contains	With the initial filter type, this operator, and a subsequent value, returns all that contain the value.
!contains	With the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.
<	With the initial filter type, this operator, and a subsequent value, returns a match less than the value.

Operator	Description
< =	With the initial filter type, this operator, and a subsequent value, returns a match less than or equal to the value.
>	With the initial filter type, this operator, and a subsequent value, returns a match greater than the value.
> =	With the initial filter type, this operator, and a subsequent value, returns a match greater than or equal to the value.

Log Collector

Log Collector

The Log Collector feature enables you to collect and upload the logs for the devices in your network to Cisco Intersight Cloud. It also enables Cisco TAC to trigger on-demand collection of logs for devices on the fabric and pulls the logs from Cisco Intersight Cloud.

The Log Collector has two modes:

- User initiated - The user collects the logs for devices on the fabric and then uploads the collected logs to Cisco Intersight Cloud after the log collection job is completed. You can automatically upload the log files to Cisco Intersight Cloud after the log collection job is completed.
- TAC initiated - Cisco TAC triggers on-demand collection of logs for specified devices and pulls the logs from Cisco Intersight Cloud.

Device Connectivity Notifier for TAC Initiated Collector

Nexus Dashboard Insights uses the device connectivity issue notifier on Cisco Nexus Dashboard to communicate with the devices. The notifier checks for TAC triggered on-demand collection of logs. In case the fabric is not configured properly to communicate with the device, Nexus Dashboard Insights notifies the following:

- The device is not configured for node interaction.
- You can not run a Log Collector job on the device.
- Nexus Dashboard Insights cannot connect to the device.

If the node interaction is not healthy on the device, you cannot choose the device for Log Collector to collect logs. In the GUI, the device is greyed out.

Guidelines and Limitations

- If you see the error message Unable to Add Fabric when you try to create a new log collector job, this can sometimes occur if the local time is not synchronized properly on the PC where you are accessing the Nexus Dashboard Insights GUI. Synchronize the local time on your PC and attempt to create the log collector job again to resolve the issue.

Uploading logs to Cisco Intersight Cloud

- Ensure that Nexus Dashboard Insights is connected to Cisco Intersight Cloud.
- Ensure that Nexus Dashboard Insights is connected to Cisco Intersight Device Connector.

Choose **Analyze** > **Analysis Hub** > **Log Collector** > **Create Log Collector Job**.

1. Enter the name.
2. Click **Select Fabric** to choose a fabric.
3. (Optional) Check **Auto Upload Log Files** to automatically upload the log files to Cisco Intersight Cloud after the log collection job is completed.

4. Click **Next**.
5. Click **Add Nodes** and then choose the nodes from the **Select Nodes** menu.
6. Click **Add**. The nodes are displayed in the **Select Nodes** table.
7. Click **Start Collection** to initiate the log collection process.

   When the job is complete, the new job appears in the **Log Collector** table.
8. Click the job in the table to display additional job details.
9. Click the icon to display **Log Collection** status.
10. Choose the node and click  icon.
11. Click **Upload File to TAC Assist** to upload a single file for the chosen node manually.
12. Click **Upload** to upload all the log files generated for the chosen node manually.

    The status of the upload is displayed in the **Selected Nodes** table.

Guidelines and Limitations

- If the upload logs fails for some of the nodes and succeeds for the rest of the nodes, then in the **Selected Nodes** table, the status is displayed as Completed.
- If the collection fails for some of the nodes, then the collection will continue for other nodes. After the collection is completed, the upload will start. In the **Selected Nodes** table, the combined status is displayed in the Status column.
- If the collection succeeds for some of the nodes, but the upload fails, then in the **Selected Nodes** table, the status is displayed as Failed.
- **Auto Upload Log Files** can be performed only on one node at a time.

Log Collector Dashboard

Navigate to **Analyze** > **Analysis Hub** > **Log Collector**.

The **Log Collector** Dashboard displays a graph of Logs by Job status for a particular fabric and displays the latest log collections.

The filter bar allows you to filters the logs by status, name, type, node, start time, and end time.

Use the following operators for the filter refinement:

Operator	Description
==	With the initial filter type, this operator, and a subsequent value, returns an exact match.
!=	With the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.

Operator	Description
contains	With the initial filter type, this operator, and a subsequent value, returns all that contain the value.
!contains	With the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

The page also displays the log collection jobs in a tabular format. The jobs are sorted by status. Choose the log collection job in the table to view additional details.

General

This displays the status of the job along with a graph showing the number of devices by status.

Details

The following information is listed:

- Creation Time
- End Time
- Nodes
- Job ID

Selected Nodes

This displays the list of nodes in a tabular form along with the status of each job and the upload status for the files uploaded.

Upload All Files allows you to upload all the files.

... allows you to Download each file separately.

TAC Initiated Log Collector

The TAC initiated log collector enables Cisco TAC to trigger on-demand collection of logs for specified user devices in the Cisco Intersight Cloud to the Device Connector.

When the TAC assist job is complete, the new job appears in the **Log Collector** table. Choose the log collection job in the table to display additional details. The **Log Collection** status displays information such as status, general information, and node details.

You can save TAC assist job details as a PDF with the browser print option (Only supported on Chrome and Firefox).

Traffic Analytics

Traffic Analytics

Traffic Analytics enables you to monitor your network's latency, congestion, and drops.

Traffic Analytics automatically discovers services running in your network by matching well-known Layer 4 ports to their corresponding service endpoint categories. Nexus Dashboard Insights then assesses service performance based on thresholds for the following metrics:

- Latency: Measures the overall time in microseconds it takes a packet to go from one place to another.
- Congestion: Measures network bandwidth utilization and quality of service (QoS) activation mechanisms to determine if a service is experiencing network congestion.
- Drops: Measures the score or number of dropped packets versus transmitted packets considering factors such as CRC errors, faulty cables, and other devices.

An anomaly is raised if there is any deviation in the performance metrics such as latency, congestion, and drops. The performance score is calculated for each conversation and aggregated to the service endpoint or endpoint level to raise anomalies.

The performance score is calculated based on the following:

- Congestion – Consistent congestion avoidance active between endpoints is calculated.
- Latency – Deviation from the average latency of the previous conversations is calculated.
- Drops – Directly correspond to an issue with the conversation or service.

Using Traffic Analytics you can:

- Monitor traffic pervasively.
- Report performance issues using anomalies raised for performance metrics.
- Sort top talking services and clients and determine the top talkers in the system.
- Determine the SYN or RST counts per service.
- Troubleshoot conversations or flows on-demand.

Traffic Analytics conversations

A TCP conversation is a 4-tuple including source IP address, destination IP address, destination port, and protocol. A non-TCP conversation is a 3-tuple including source IP address, destination IP address, and protocol. In case a single client establishes multiple communication flows initiated by multiple source ports towards a service endpoint, all related statistics would be aggregated as a single entry in the Traffic Analytics table. A service endpoint is defined by an IP address, a port, and a protocol.

An anomaly is raised after the conversation rate limit is exceeded. Navigate to **Admin** > **System Settings** > **Flow Collection**. In the Traffic Analytics status for the last hour area, you can view if the conversation rate approaches or exceeds the limits. You can also view if there are any Traffic Analytics record drops.

Traffic Analytics scale limits

The table shows the Traffics Analytics scale limits.

Traffic Analytics scale limits

Nexus Dashboard cluster	Unique conversations per minute	Concurrent troubleshoot jobs
6 physical	100,000	8
3 physical	50,000	5
1 physical	5,000	1
6 virtual	10,000	5
3 virtual	5,000	1

Guidelines and limitations for Traffic Analytics

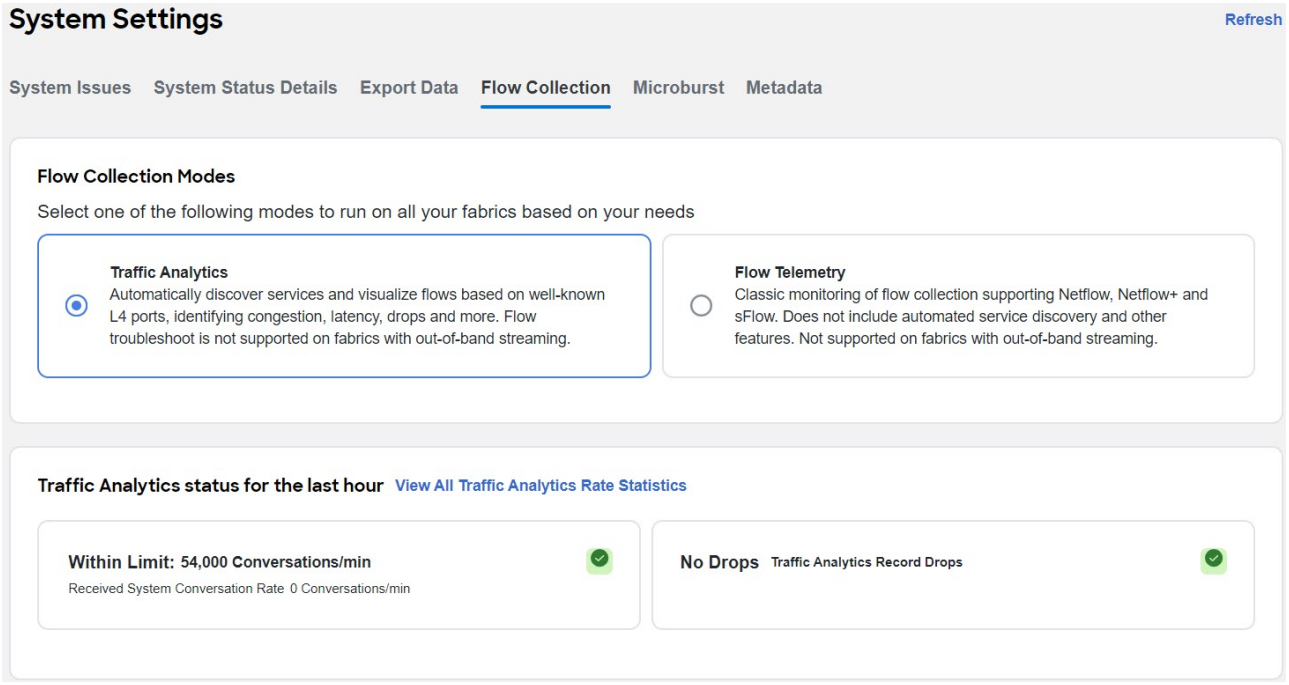
- Traffic Analytics is supported on Cisco NX-OS release 10.4(2)F and later.
- Traffic Analytics is not supported for Layer 4 to Layer 7 Services.
- Traffic Analytics is not supported for Multi-Site.
- Before enabling Traffic Analytics on Cisco NDFC fabrics with a Netflow configuration, you must add a freeform policy to the leaf switches. This ensures that if Traffic Analytics is disabled from Nexus Dashboard Insights, the Netflow configuration is not removed.
- Multicast is not supported for Traffic Analytics.
- Traffic Analytics is only available for traffic flows between IPv4 or IPv6 endpoints that are contained within the fabric. These endpoints should be visible in the **Manage** > **Fabrics** > **Connectivity** > **Endpoints** page. If the source or destination endpoint exists outside the fabric, then the Traffic Analytics conversation will not be displayed in the Traffic Analytics table.
- Traffic Analytics configurations or export is not supported on Cisco Nexus 9500 modular chassis, however flow troubleshoot jobs is supported for FX platform switches and Cisco Nexus 9500 modular chassis.
- Navigate to **Analyze** > **Analysis Hub** > **Traffic Analytics** to view information about TCP services and clients/conversations. Go to the **Endpoint Traffic Analytics** tab to view information about non-TCP services and clients/conversations.
- Traffic Analytics may display partial data when the VRF instance is configured with the new L3VNI mode. For more information about the new L3VNI mode, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide.
- Ensure that you have configured NTP and enabled PTP on NDFC. See Cisco Nexus Dashboard Insights Deployment Guide and Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights for more information. You are responsible for configuring the switches with external NTP servers for Cisco NDFC fabrics.
- Traffic Analytics is only supported on VxLAN fabrics for standalone NX-OS and NDFC fabrics.
  - Prior to NDI release 6.5.2, Traffic Analytics on Classic LAN fabrics is not supported.
  - Beginning with NDI release 6.5.2, Traffic Analytics on Classic LAN fabrics is supported, but

only over out-of-band (OOB) management ports, and Flow Troubleshoot is not supported for Classic LAN. In addition, the two-tier Collapsed Core topology is supported, along with other validated topologies, if any. See the "Supported Legacy/Classic Network Topologies" section in Managing Legacy/Classic Networks in Cisco Nexus Dashboard Fabric Controller for more information.

- When Traffic Analytics across multiple fabrics is enabled, you can observe these issues with flow latency computation:
  - When the border device role is Border Gateway Spine or Border Gateway Super-spine, no traffic analytics configuration is pushed to the border router because no end hosts are expected to be connected. This results in Nexus Dashboard Insights showing a blank (-) for the Rx average/maximum latency.
  - If ttag-strip is configured on the DCI interfaces, then Nexus Dashboard Insights displays only the intra-fabric flow latency; that is, the latency between the border router and the internal flow endpoint. The end-to-end latency is not displayed in this case.
  - If PTP is configured on the DCI interfaces and the IPN network supports PTP, then Rx latency will show the end-to-end inter-fabric latency, while Tx latency shows only the intra-fabric flow latency.

Configure Traffic Analytics

1. Navigate to **Admin** > **System Settings** > **Flow Collection**.
2. In the **Flow Collection Modes** area, choose **Traffic Analytics**.



If you want to enable Traffic Analytics, ensure that there are no pre-existing Netflow configurations on the switches. If there are any pre-existing configurations, the switch configuration may fail with a system anomaly stating, invalid command match IP source address. To resolve this, you should disable Traffic Analytics, remove the Netflow configuration from the switches, and then re-enable Traffic Analytics.

3. In the **Flow Collection per Fabric** table, choose the fabric.
4. Click the ellipsis icon and then click **Enable** to enable Traffic Analytics.



If flow telemetry is already enabled on the fabric, you must first disable flow telemetry for all the fabrics and remove all flow rules before enabling Traffic Analytics.

5. You can view the Flow Collection status for each node in the **Switch Configuration Status** column.
   - Green – Flow collection is successfully enabled.
   - Red – Flow collection is not enabled.
   - Orange – Flow collection is partially enabled.
   - Gray – Flow collection is not supported or data cannot be found. If a switch is in disabled state, it will included in the Grey category.
6. In the Traffic Analytics Status For The Last Hour area you can see the number of conversations that are over limit and Traffic Analytics drops. You must make sure that you do not exceed the maximum conversation rate limit. If you exceed the maximum conversation rate limit you will see drops in flows records and it will impact the visibility.
7. Click **View All Traffic Analytics Rate Statistics** to view the statistics for each switch in a fabric.

Apply Traffic Analytics Configuration

For NDFC fabric in Monitored mode, Nexus Dashboard Insights will not deploy Traffic Analytics configuration to all switches in the fabric. You must apply the Traffic Analytics configuration to every switch.

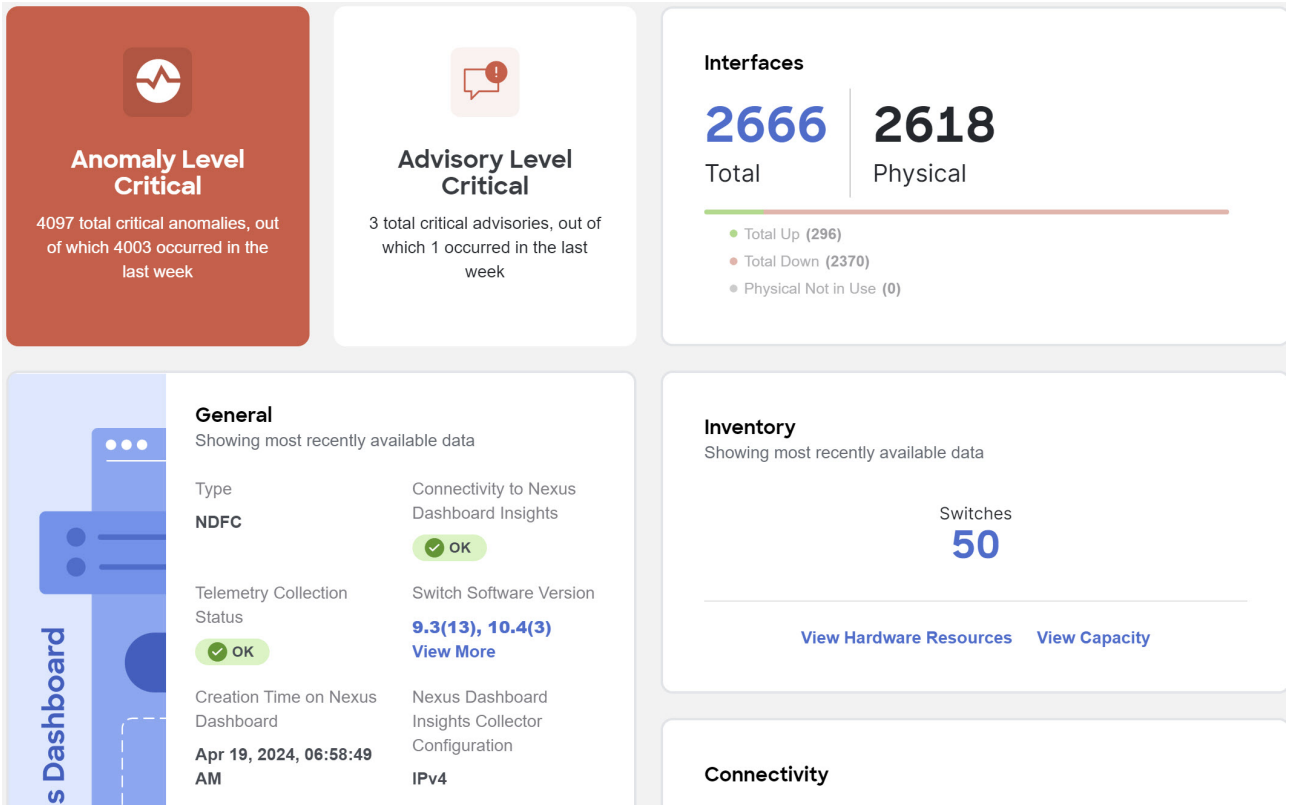
1. Navigate to **Admin** > **System Settings** > **System Status Details**.
2. Choose a fabric.
3. Click the ellipsis icon and then click **Expected Configuration**.
4. From the **Expected Configuration** area, you can view and copy configurations under **Software Telemetry** and **Flow Telemetry**.
5. Using the command line, log in to the switch.
6. Enter the following commands:

```
switch# configure terminal
switch(config)# copy running-config startup-config
```

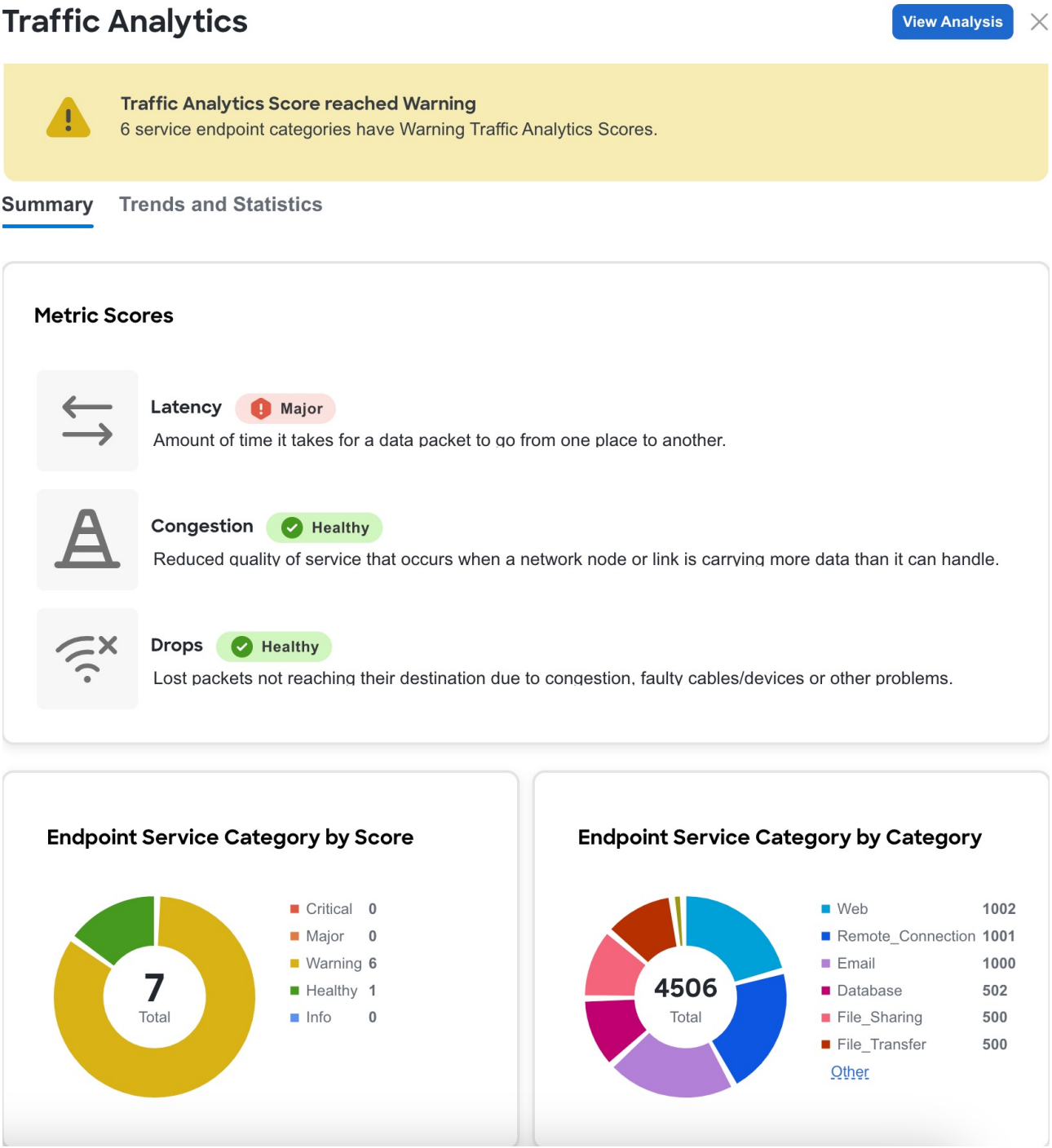
View Traffic Analytics

View Traffic Analytics for an Individual Fabric

1. Navigate to **Manage** > **Fabrics**.
2. Click the fabric name.



3. Choose a time range from the dropdown menu. By default the Current time (last 2 hours) is chosen.
4. In the General area, click **Traffic Analytics** to view Traffic Analytics details for that fabric. In the Traffic Analytics page all the information is grouped as service categories for that fabric.



5. The Summary area displays the Traffic Analytics Score and how the metrics is determined. You can view the traffic profile for endpoint service category by score and category.
6. Click **Trends and Statistics** to view Traffic profile, Top Endpoint Service Score Changes, and Top Endpoint Categories.

Traffic Analytics

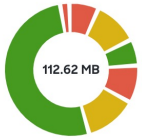
View Analysis

Traffic Analytics Score reached Warning
6 service endpoint categories have Warning Traffic Analytics Scores.

Summary | Trends and Statistics

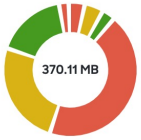
Traffic Profile

Tx



Database	6.85 MB
Email	11.69 MB
File_Sharing	5.91 MB
File_Transfer	9.36 MB
Other	

Rx



Database	8.69 MB
Email	11.70 MB
File_Sharing	5.91 MB
File_Transfer	177.97 MB
Other	

Top Endpoint Service Score Changes

Categories	Score Change	Affecting Metric
Database	Warning → Healthy	Latency ↘
File_Transfer	Warning → Healthy	Latency ↘
Remote_Connection	Warning → Healthy	Latency ↘
Email	Warning → Warning	Latency →
File_Sharing	Warning → Warning	Latency →
RoCE	Unknown → Healthy	-
Web	Warning → Warning	Latency →

7 items found

Rows per page 10 | 1

Top Endpoint Categories by Rx Latency

Categories	Average	Trend
File_Transfer	2.01 us	↗ 3%
Remote_Connection	2 us	↗ 1%
Database	2 us	↘ 0%
Email	2 us	↘ 0%
File_Sharing	2 us	→
RoCE	0 us	→
Web	2 us	↘ 0%

a. In the Traffic Profile area you can view the traffic amount for the endpoint service category.

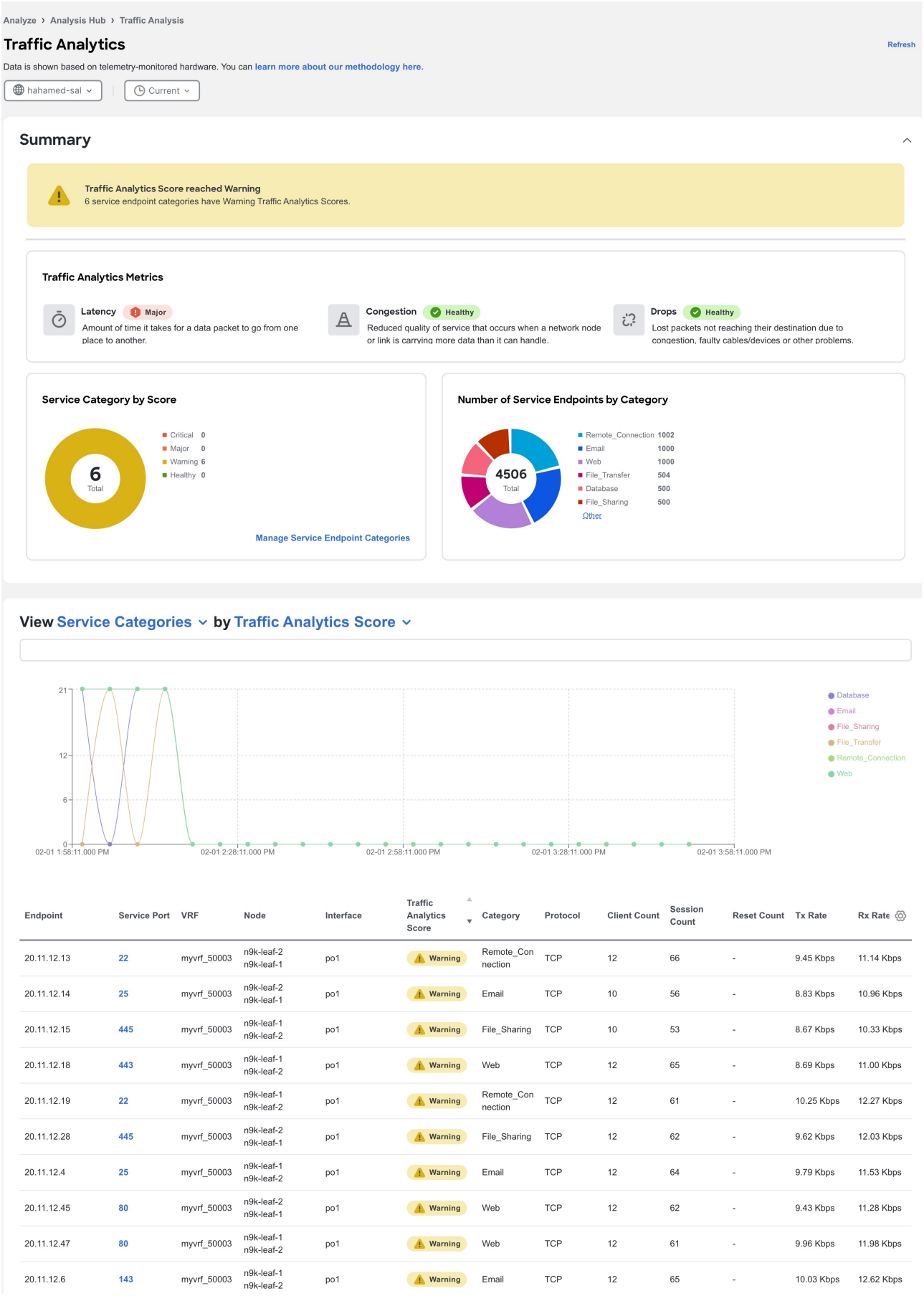
b. In the Top Endpoint Service Score Changes area, you can view the anomaly score change across 2 hours and the metrics (such as latency, congestion, drops) affecting the score change.

c. In the Top Endpoint Categories by area you can see the top categories by Rx and Tx Latency, Congestion Score, and Drop Score.

7. Click **View Analysis** to view Traffic Analytics for all the fabrics.

View Traffic Analytics for all fabrics

1. Navigate to **Analyze** > **Analyze Hub** > **Traffic Analytics**.
2. Choose a fabric from the drop-down menu.
3. Choose a time range from the dropdown menu. By default the Current time (last 2 hours) is chosen. When you choose the Current time, any issues observed in the Traffic Analytics score over the last 2 hours is displayed.

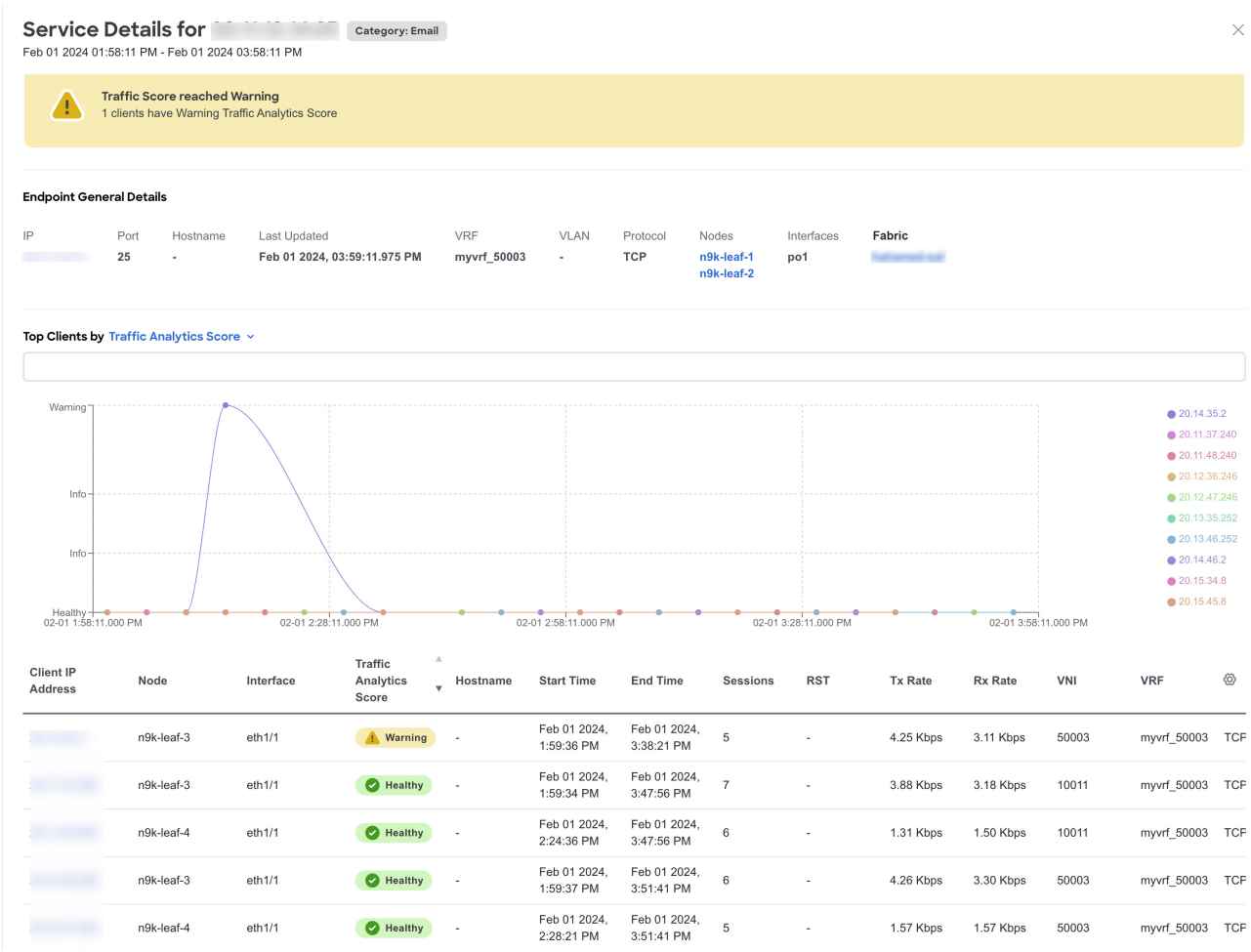


Endpoint	Service Port	VRF	Node	Interface	Traffic Analytics Score	Category	Protocol	Client Count	Session Count	Reset Count	Tx Rate	Rx Rate
20.11.12.13	22	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Remote_Connection	TCP	12	66	-	9.45 Kbps	11.14 Kbps
20.11.12.14	25	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Email	TCP	10	56	-	8.83 Kbps	10.96 Kbps
20.11.12.15	445	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	File_Sharing	TCP	10	53	-	8.67 Kbps	10.33 Kbps
20.11.12.18	443	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	65	-	8.69 Kbps	11.00 Kbps
20.11.12.19	22	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Remote_Connection	TCP	12	61	-	10.25 Kbps	12.27 Kbps
20.11.12.28	445	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	File_Sharing	TCP	12	62	-	9.62 Kbps	12.03 Kbps
20.11.12.4	25	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	64	-	9.79 Kbps	11.53 Kbps
20.11.12.45	80	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Web	TCP	12	62	-	9.43 Kbps	11.28 Kbps
20.11.12.47	80	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	61	-	9.96 Kbps	11.98 Kbps
20.11.12.6	143	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	65	-	10.03 Kbps	12.62 Kbps

4. The Summary area displays the Traffic Analytics Score and how the metrics are determined. Next you can view the information for a Service Endpoint Category by Score and Category. Service endpoint categories consists of ports that have been assigned to categories based on standard networking defaults and any categories you may have created. These categories are dynamic and

can be updated any time. See Manage Service Endpoint Categories.

5. Next use the drop-down list to view the Service Categories or Service Endpoints information for attributes such as Traffic Score, Congestion Score, Latency Score, Drop Score, and others in a graphical format. When you choose Service Endpoints, you can also view the top 10 endpoints for various attributes such as Traffic Analytic Score, Latency Score, Congestion Score, Drop Score, Session Count, Reset Count, TX Rate, and Rx Rate. For Current Time, when you choose view **Service Categories** for **Traffic Analytics Score**, you can use the graph to view the transition between healthy and unhealthy score.
6. In the Traffic Analytics table, you can view the Service Categories or Service Endpoints information. The Traffic Score information for service categories or endpoints is a combination of congestion score, latency score, and drop score. When the score is calculated, congestion score has the lowest weighage, and drop score has the highest weighage.
   a. You can hover on the Traffic Analytics Score column to view the Traffic Analytics Score breakdown for the service.
   b. Use the search bar to filter by Service Categories or Service Endpoints values.
   c. Click the gear icon to configure the columns in the Traffic Analytics table.
7. Click **Service Port** to view additional details for the particular service.



   a. In the Overview area you can view the endpoint details and client details such as top clients and conversation between a client and service.
      i. In the Endpoint General Details, click Client IP Address to view endpoint details. You can view all the services hosted on that endpoint and connections to other services and IP addresses from this endpoint.

ii. Use the drop-down list to view the information for Top Clients by Traffic Analytics Score, Latency Score, Drop Score and others.

iii. In the Clients table, hover on the Traffic Analytics Score to view the Traffic Analytics Score breakdown for that service.

b. In the Trends and Statistics area you the view the trends for values such clients, service, latency and others for that service.

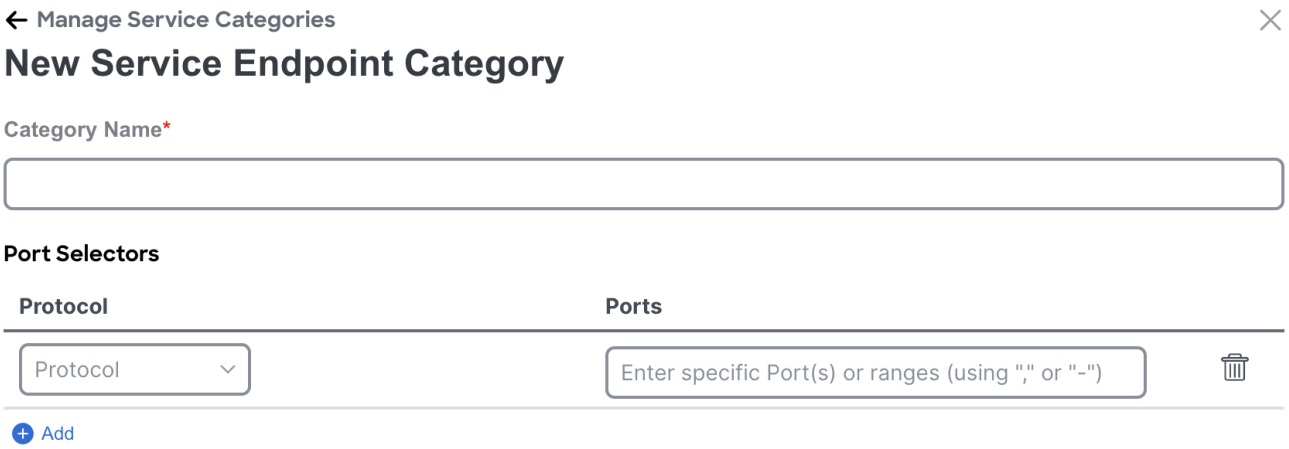
c. In the Anomalies area, you can view the anomalies for the particular service endpoint based on traffic score.

d. In the Flow Collections area, you can view the flow collections for that service.

Manage Service Endpoint Categories

In the Manage Service Endpoint Categories area you can view the ports that have been assigned to categories based on standard networking defaults and any categories you may have created. If a port has not been assigned to a category, you can assign it to one of the existing categories or create a new category. This helps you to organize and manage your network ports more efficiently.

1. Navigate to **Analyze** > **Analyze Hub** > **Traffic Analytics**.
2. Choose a fabric from the drop-down menu.
3. Choose a time range from the drop-down menu. By default the Current time (past 2 hours) is chosen.
4. In the Service Category by Score area click **Manage Service Endpoint Categories**.
5. To create a new category, click **New Categories**.

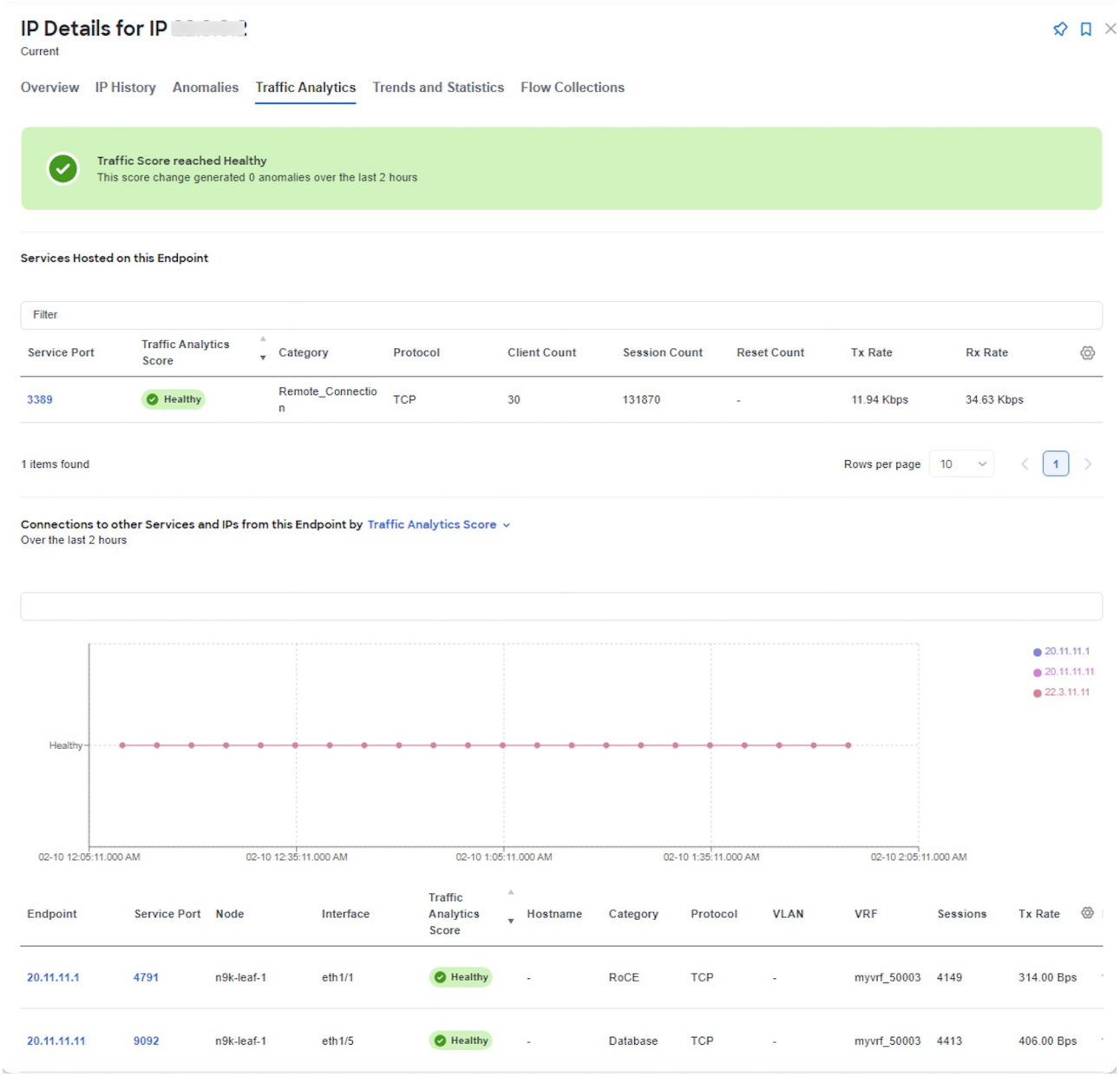


6. Enter the name of the category.
7. From the Protocol drop-down list, choose the protocol.
8. In the Ports field, enter the ports or port range.
9. Click **Add** to add additional protocols.
10. Click **Save**.
11. To edit a category, click the ellipsis icon and choose edit.
    a. Edit the values and click **Save**.

12. To delete a category, click the ellipsis icon and choose delete.
    a. Click **Confirm**.

View Traffic Analytics for Endpoints

1. Navigate to **Manage** > **Fabrics**.
2. Click fabric name.
3. Navigate to **Connectivity** > **Endpoints**.
4. In the Endpoint table click an IP address.
5. In the IP Details page, click **Traffic Analytics** to display the Traffic Analytics view for endpoints.

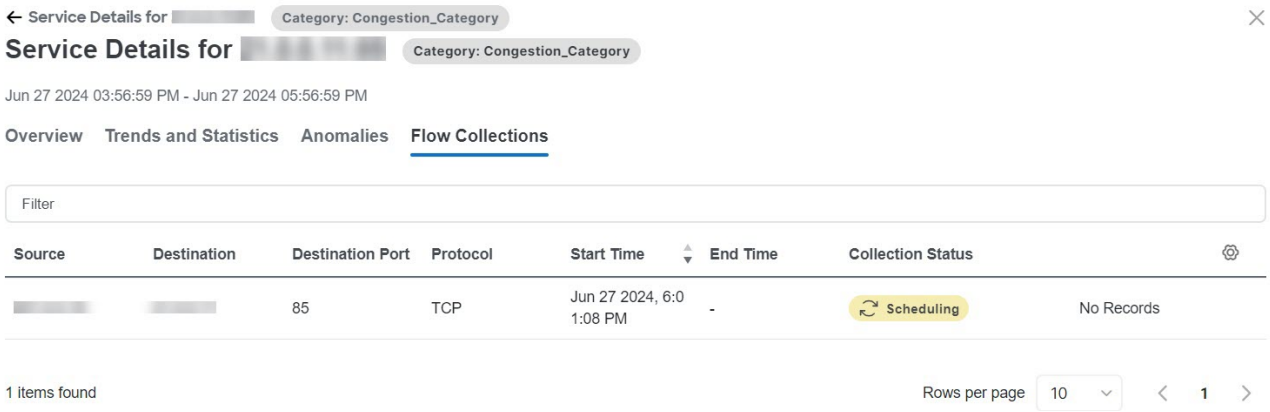


Flow Troubleshoot Workflow

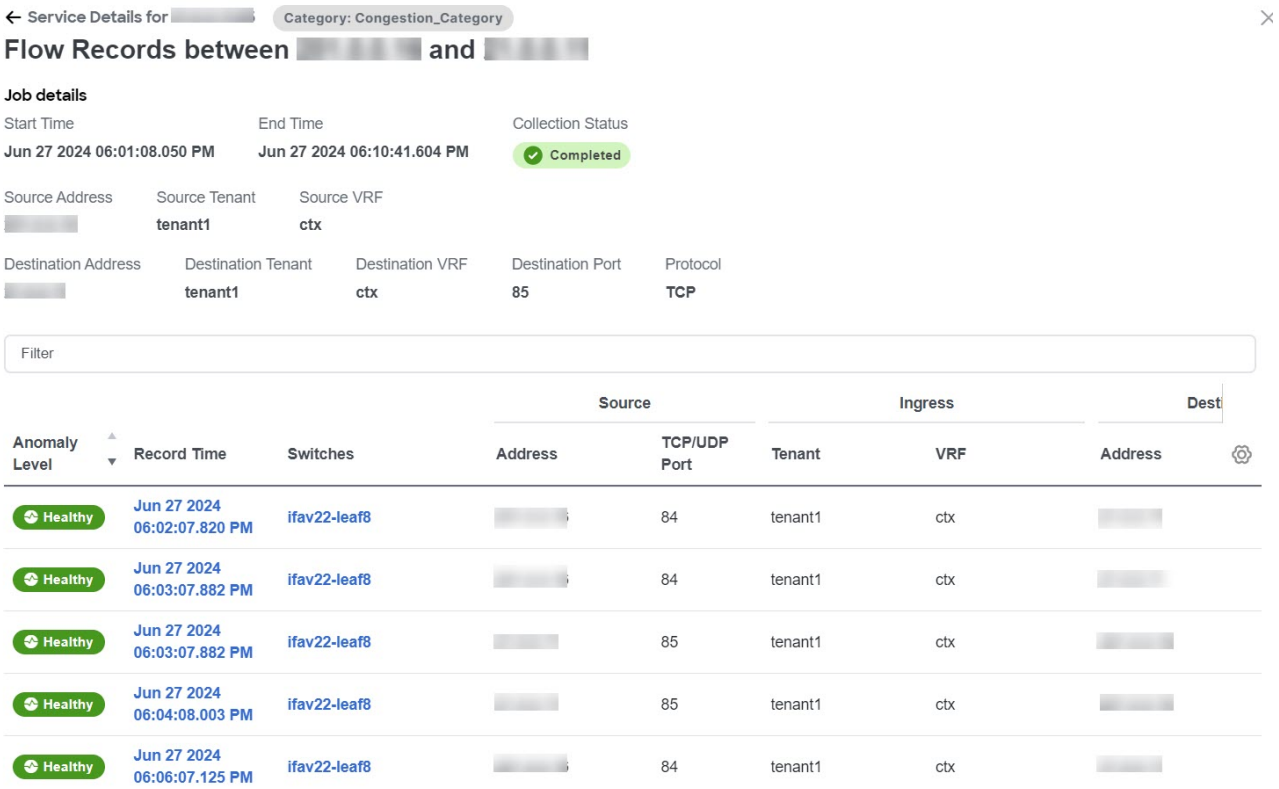
The flow troubleshoot workflow enables you to collect all the flow records between two endpoints. Nexus Dashboard Insights allows you to specify the duration for flow collection and then collect records between specific endpoints for the specified duration. As a result you can view the path

visualization, 5-tuple flow information, and any issues seen on individual flows.

1. Navigate to **Analyze** > **Analyze Hub** > **Traffic Analytics**.
2. Choose a fabric from the drop-down menu.
3. Choose a time range from the drop-down menu. By default the Current time (last 2 hours) is chosen.
4. In the **View by** area, choose **Service Endpoints** from the first drop-down menu. By default, **Service Categories** is chosen.
5. In the **View by** area's table, choose an endpoint and click the endpoint's port number under **Service Port**.
6. In the Service Details page, click the ellipsis icon for a client IP address and choose **Start Flow Collection**. You might need to scroll all the way to the right in the table of client IP addresses to see the ellipsis icon.
7. Choose the duration to collect flow records for a specific time period. Click **Start and go to Flow Collections Tab**.



8. After the Collection Status displays Completed, click **View Records** to view the flow record details for that specific service endpoint.



To view the flow collection for a fabric, navigate to **Manage** > **Fabrics**. Choose a fabric. Click **Connectivity** > **Flow Collections**.

Flow troubleshoot may not show all the switches through which packet traverses for each record in the following scenarios:

- When there are flow drops in Nexus Dashboard Insights
- When there are table collisions in the hardware

Sustainability Report

Sustainability Report

The Cisco Nexus Dashboard Insights sustainability report helps you monitor, predict, and improve your network's energy usage, its related carbon emissions, and its total energy cost. The sustainability report enables you to get insights on energy utilization, CO2 emissions, and energy cost for all your fabrics on a monthly basis.

The report is generated by calculating the monthly values for Power Consumption and by summing the usage data across all of your devices at each of your fabrics for every single day in the chosen month. This data is then combined with the Cisco Energy Manager to provide greater insight into what that usage means in terms of energy cost, estimated emissions, and estimated switch power consumption. For more information about the Cisco Energy Manager, see Cisco Energy Manager.

The summary area of the report contains information such as estimated cost, estimated switch power consumption, sources of emission, and estimated emissions.

- Estimated Cost gives you insight into any expected increase or decrease in your fabrics' energy bills based on your monthly energy use.
- Estimated Switch Power Consumption gives you insight into how efficiently your switches are using electricity. Estimated PDU Power Consumption gives you insight into how much electricity your devices or Panduit power distribution units (PDUs) are using.
- Estimated Emissions gives you insight into the sustainability your fabrics have on your total CO2 emissions, based on the sources and amount of energy used.

If you have Panduit PDUs onboarded to Nexus Dashboard, you can use the **Data Source** toggle to see two different electricity values on the sustainability report: one for switches only, and one for PDUs.

- Switch Data: Uses only the electricity data reported by individual switches added to a fabric.
- PDU Data: Uses the electricity data reported by a supported PDU, which could include switches, fans, and any other devices physically plugged into the PDU.

Depending on which value you choose in the **Data Source** toggle, the values calculated for your other metrics, including estimated cost and emissions, will vary.

Using the sustainability report, you can:

- Better anticipate increases in your fabrics' energy bills so that your budgets more accurately reflect real-world usage.
- Better follow the hourly energy usage of an individual fabric. By spreading out usage to avoid peak hours surcharges, you may be able to lower your electricity bill over time.
- See the direct sustainability impact running your fabric has on climate change. Following your emissions over time also gives you the ability to choose lower-carbon sources and track your progress toward meeting ESG goals.

The retention time for the sustainability report in Nexus Dashboard Insights is 12 months.

Cisco Energy Manager

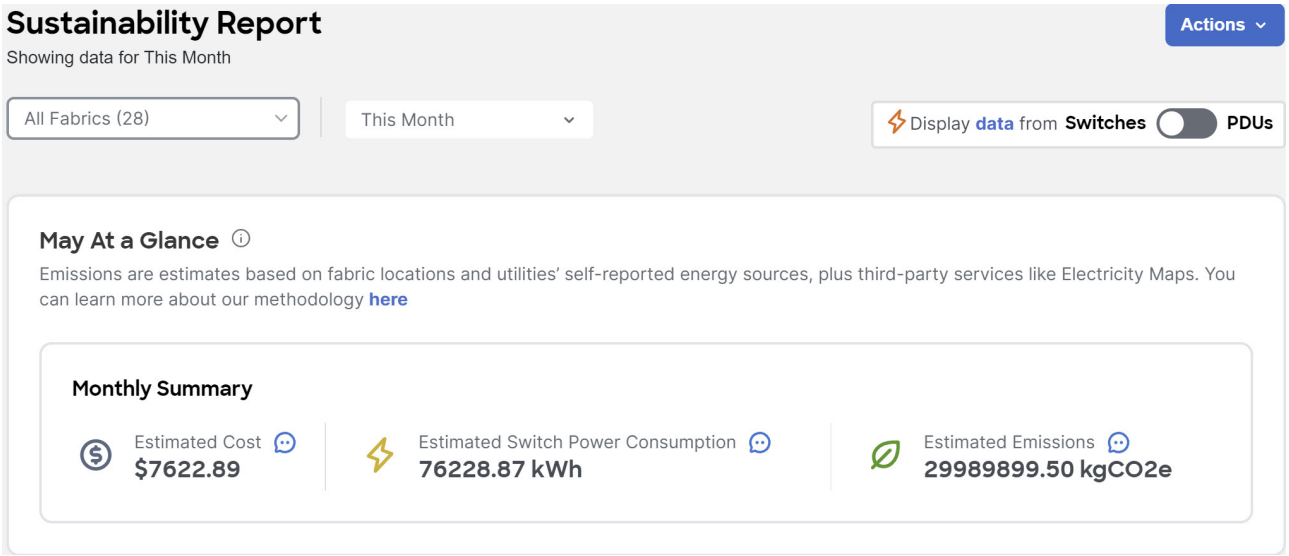
The Cisco Energy Manager is a service developed by Cisco that collects data from various data providers and consolidates the GHG emissions and the source of the energy from the data. The Cisco Energy Manager is hosted in a Cisco Intersight cloud.

View the sustainability report for switches

1. Navigate to **Analyze** > **Analysis Hub** > **Sustainability Report**.
2. Choose an online fabric or multiple online fabrics from the drop-down menu.
3. Choose a time range from the drop-down menu.
4. Use the Data Source toggle to display data from switches.
5. Click **Prepare Report**.

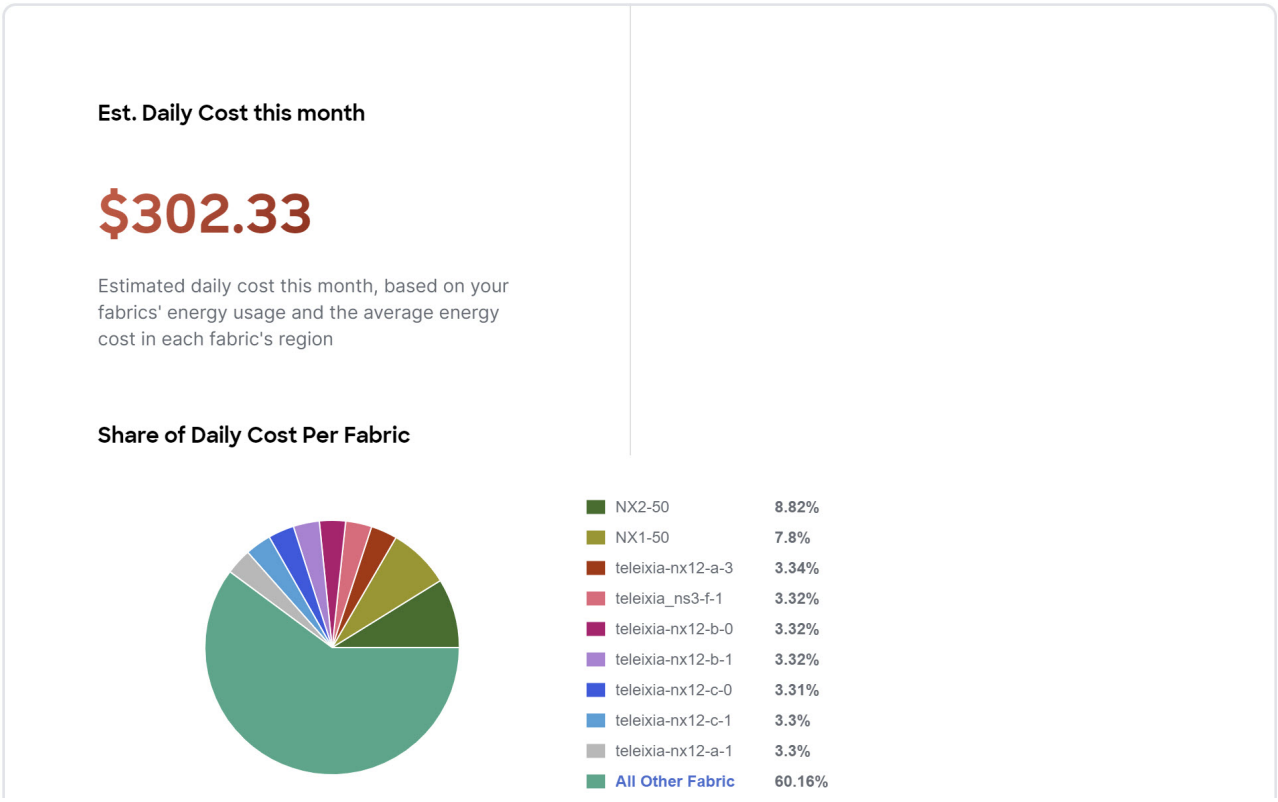
   The sustainability report displays At A Glance, Cost, Energy, and Emissions information for a particular fabric in the chosen month.

6. Examine the **At A Glance** area to see a summary of the estimated cost, estimated switch power consumption, and estimated emissions in the chosen month. Click the **Learn More** icon for more information.

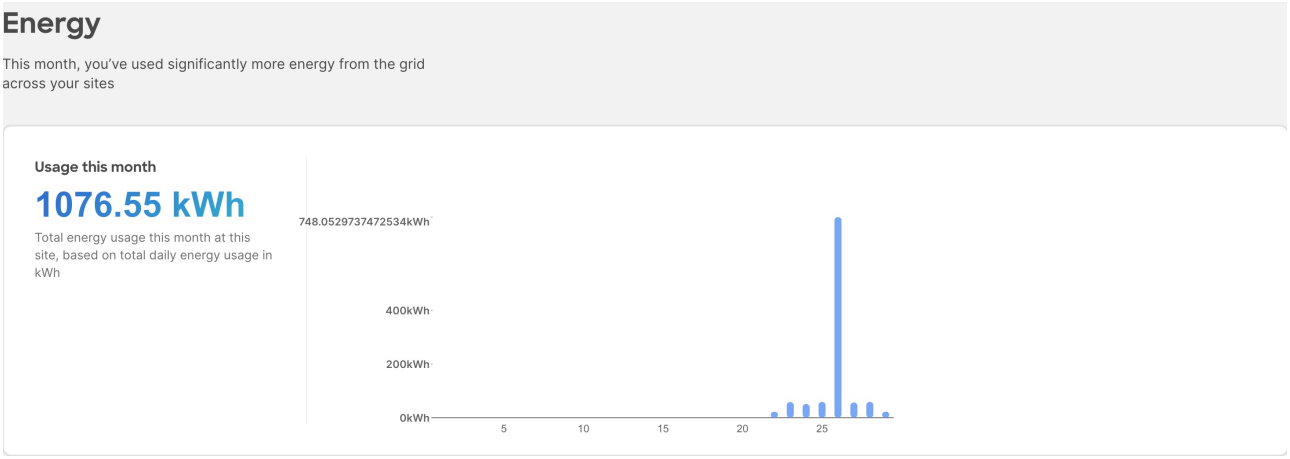


7. Examine the **Cost** area to see the estimated daily cost in the chosen month and share of daily cost per fabric.

Cost



8. (Optional) From the **Actions** menu, choose **Fabric Energy Settings** to customize your average cost for the current month for a more accurate estimate. To calculate cost estimates, Nexus Dashboard Insights uses values based on the average cost of grid energy for each region.
9. Examine the **Energy** area to see the energy usage in the chosen month in kWh.

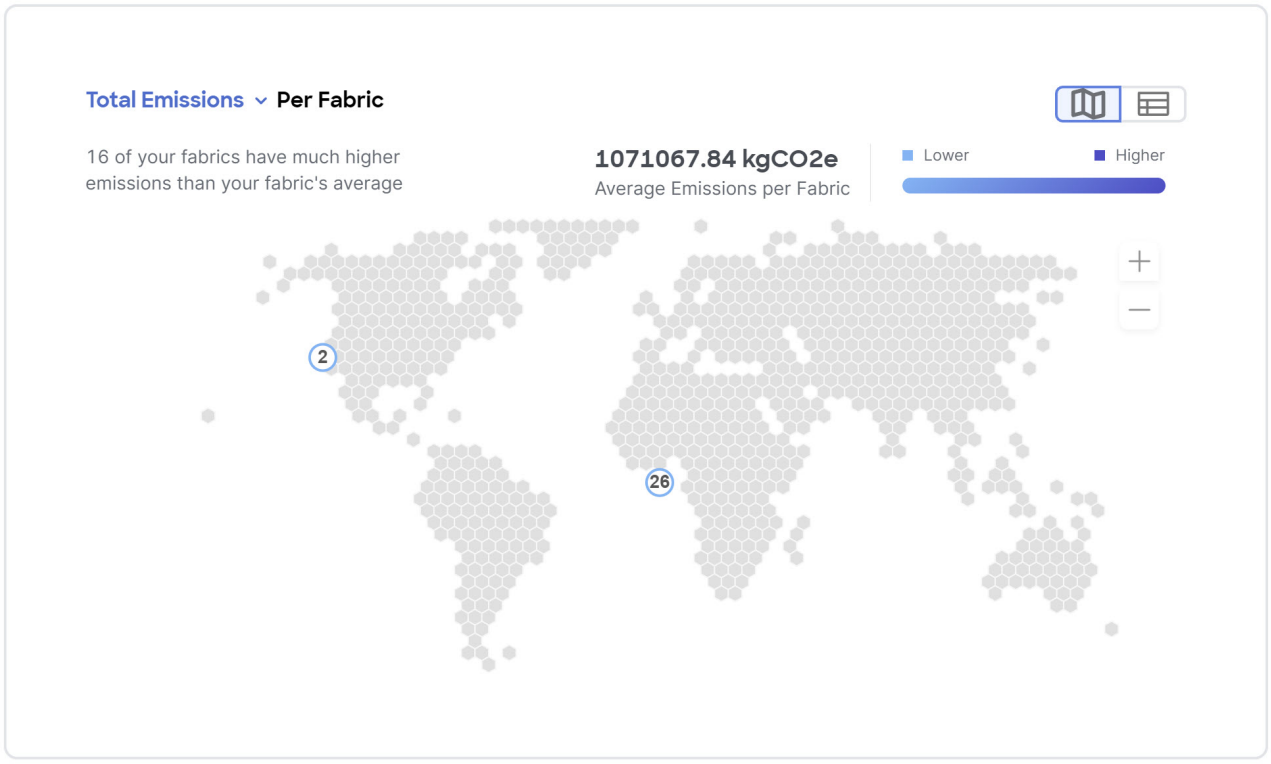


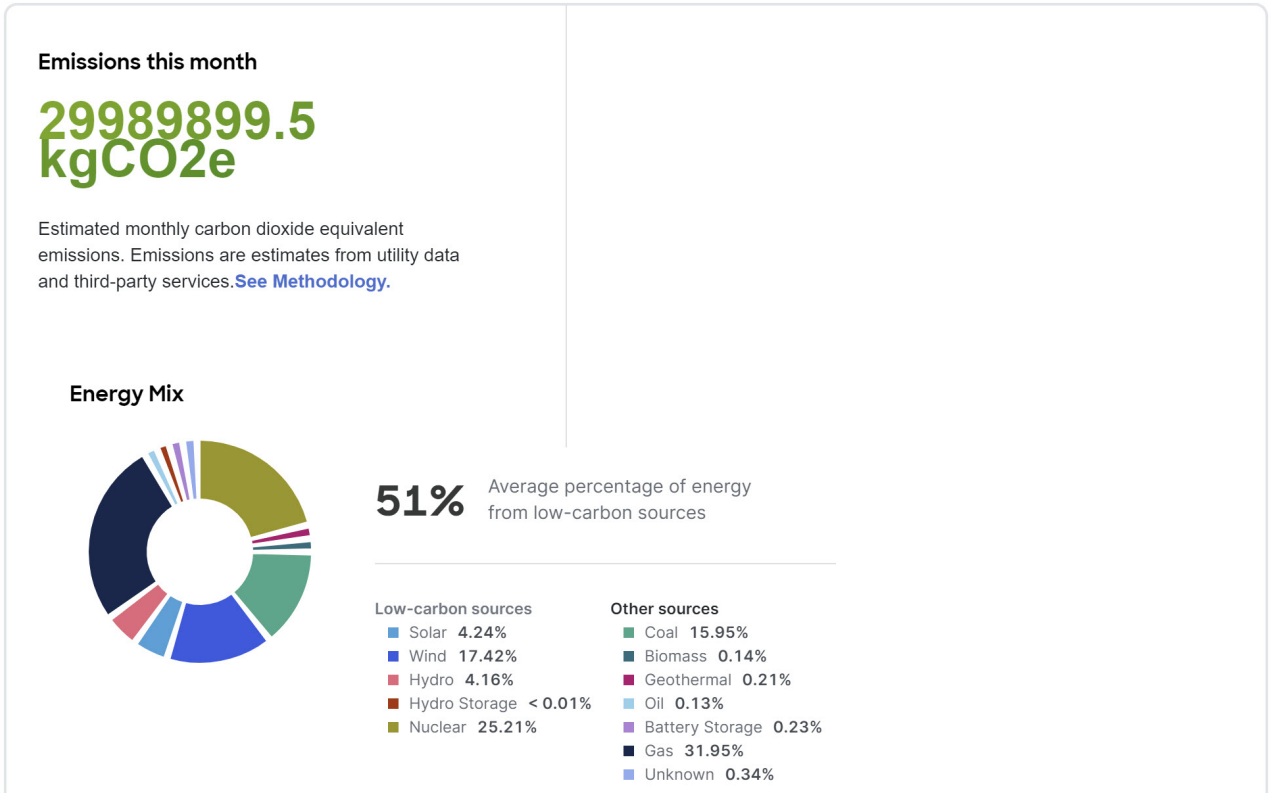
10. Examine the **Emissions** area to see the total emissions or efficiency index per fabric, estimated monthly carbon dioxide equivalent emissions, average percentage of energy from low-carbon sources and other sources, and percent of total energy used during each three-hour reporting period by source over all of the days in the chosen month.

    For total emissions or efficiency index per fabric, use the toggle to view the information in graphical format or tabular format.

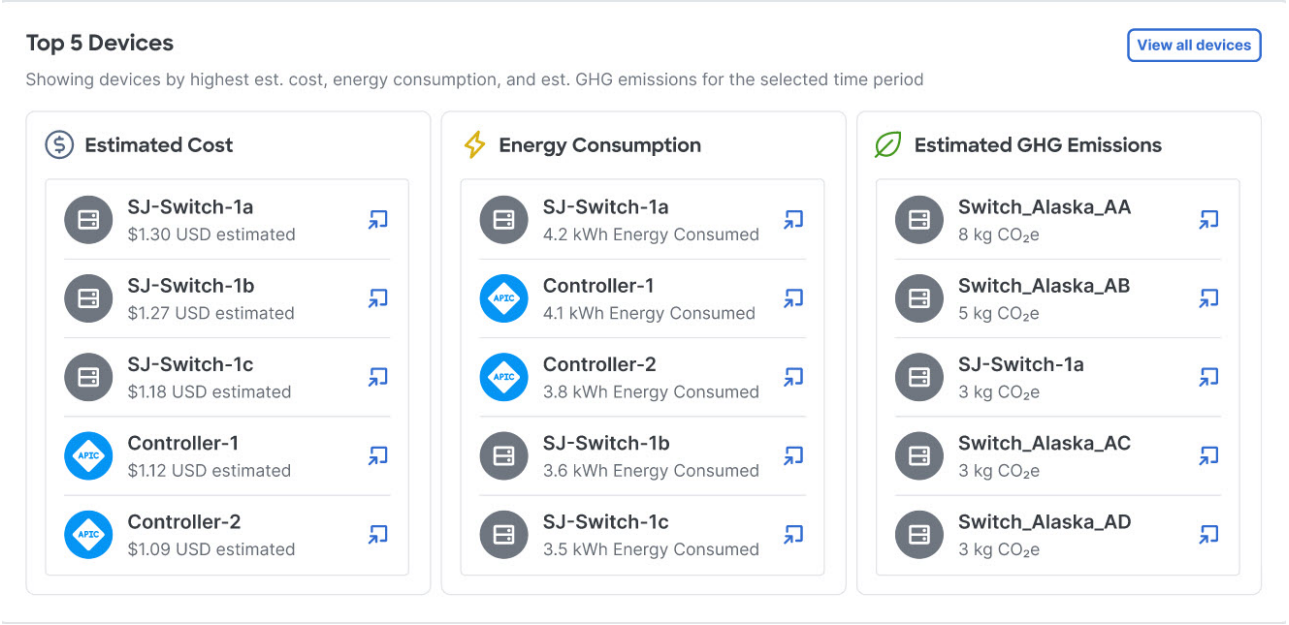
Emissions

About 51% of your energy this month came from low-carbon sources on average with nuclear making up the majority





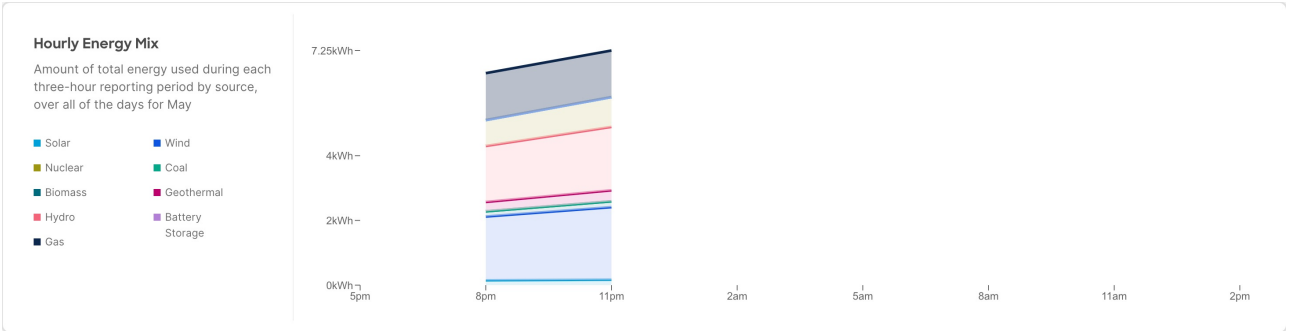
11. Examine the **Top 5 Devices** area to see the top 5 devices for the highest estimated cost, most energy consumed, and highest estimated greenhouse gas (GHG) emissions.



Click **View all devices** to see the data for all devices, not just the top 5.

12. Choose a fabric from the fabric drop-down menu to view the hourly energy mix.

    Hourly energy mix displays the amount of total energy used during each three-hour reporting period by source, over all of the days in the chosen month. The minimum period before you can generate the next report is 3 hour.



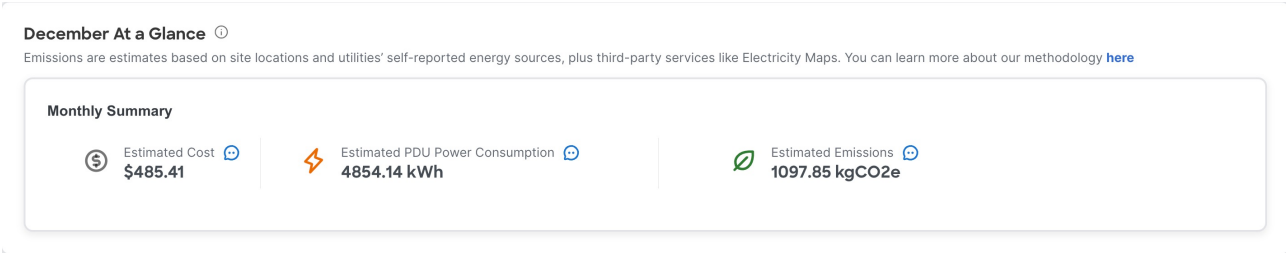
The minimum period before you can generate the next report is 3 hour.

View the sustainability report for PDUs

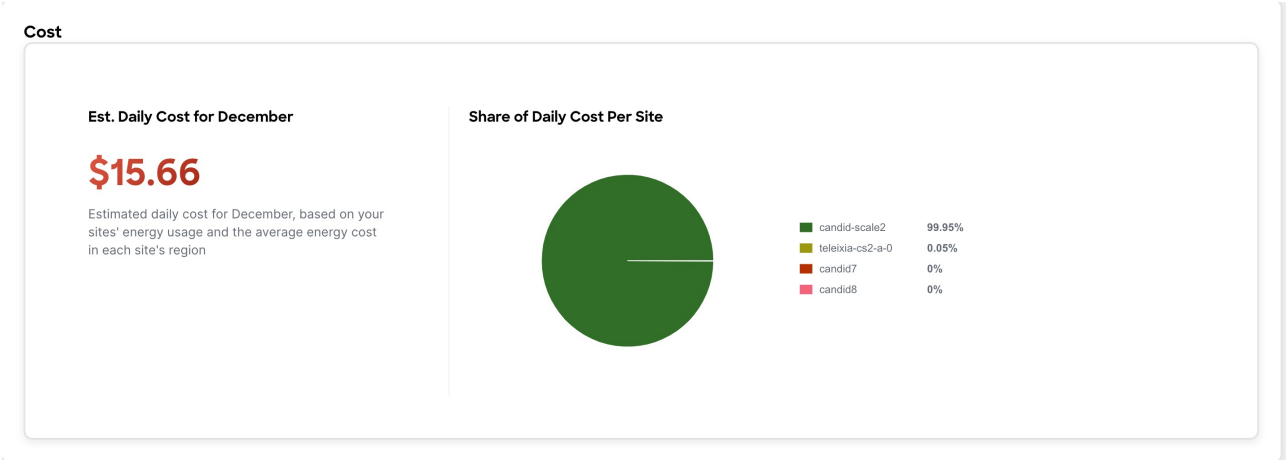
1. Navigate to **Analyze** > **Analysis Hub** > **Sustainability Report**.
2. Choose an online fabric or multiple online fabrics from the drop-down menu.
3. Choose a time range from the drop-down menu.
4. Use the Data Source toggle to display data from PDUs.
5. Click **Prepare Report**.

   The sustainability report displays At A Glance, Cost, Energy, and Emissions information for a particular fabric in the chosen month.

6. Examine the **At A Glance** area to see a summary of the estimated cost, estimated switch power consumption, and estimated emissions in the chosen month. Click the **Learn More** icon for more information.



7. Examine the **Cost** area to see the estimated daily cost in the chosen month and share of daily cost per fabric.



8. (Optional) From the **Actions** menu, choose **Fabric Energy Settings** to customize your average cost for the current month for a more accurate estimate. To calculate cost estimates, Nexus Dashboard Insights uses values based on the average cost of grid energy for each region.
9. Examine the **Energy** area to see the energy usage in the chosen month in kWh.

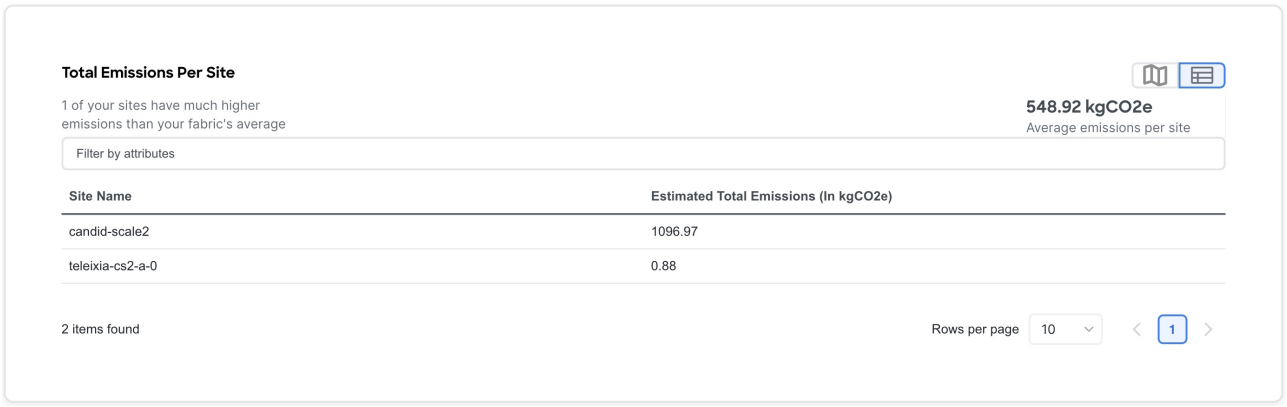


10. Examine the **Emissions** area to see the total emissions per fabric, estimated monthly carbon dioxide equivalent emissions, average percentage of energy from low-carbon sources and other sources, and percent of total energy used during each three-hour reporting period by source over all of the days in the chosen month.

    For total emissions per fabric, use the toggle to view the information in graphical format or tabular format.

Emissions

About 41 of your energy for December came from low-carbon sources on average with nuclear making up the majority

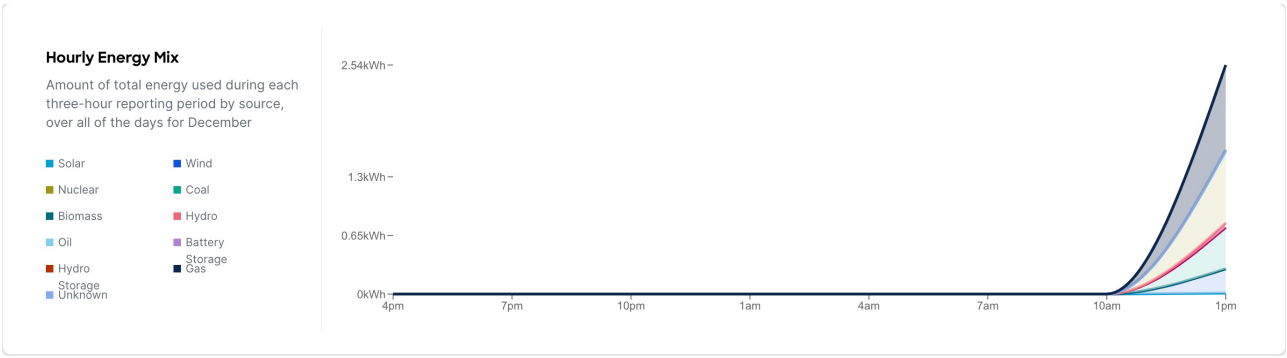


11. Examine the **Top 5 Devices** area to see the top 5 devices for the highest estimated cost, most energy consumed, and highest estimated greenhouse gas (GHG) emissions.

    Click **View all devices** to see the data for all devices, not just the top 5.

12. Choose a fabric from the fabric drop-down menu to view the Hourly energy mix.

    Hourly energy mix displays the amount of total energy used during each three-hour reporting period by source, over all of the days in the chosen month. The minimum period before you can generate the next report is 3 hour.



Delta Analysis

Delta Analysis

Nexus Dashboard Insights performs analysis of sites at regular intervals and the data is collected at an interval depending on the number of nodes.

Number of nodes	Interval
Fewer than 100	2 hours
100 to 400	3 hours
Greater than 400	12 hours

At each interval, Nexus Dashboard Insights captures a snapshot of the controller policies and the fabric run time state, performs analysis, and generates anomalies. The anomalies generated describe the health of the network at that snapshot.

Delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two snapshots.

Create Delta Analysis enables you to create a new delta analysis and manage existing analysis. See Create Delta Analysis.

Health Delta

Health Delta analyses the difference in the health of the fabric across the two snapshots.

See View Health Delta Analysis for more details.

Policy Delta for NDFC

Policy Delta for NDFC fabrics analyzes the changed nodes or switches across two snapshots and obtains a co-related view of what has changed in the NX-OS switches.

See View Policy Delta Analysis for more details.

Guidelines and Limitations for Delta Analysis

- The Delta Analysis functionality currently supports the local authentication domain only.
- While you are currently allowed to create more than one Delta Analyses at any given time, we recommend that you do not queue more than one Delta Analysis at any given time. In addition, we recommend that you wait for some time (approximately 10 minutes) between creating new analyses to avoid the risk of adversely impacting the run time of the concurrent online fabric analysis.

  The interdependency arises because the Delta Analysis results in an increased load on the database. Sustained high-database load from multiple back-to-back Delta Analyses may affect the run-time of the online analysis.

- When you choose a switch in the **Changed Nodes** area, in **Policy Delta**, the difference in the configuration between the two snapshots is displayed.
- For Policy Delta, **Audit Logs** is not currently supported.

Create Delta Analysis

Choose **Analyze** > **Analysis Hub** > **Delta Analysis** > **Create Delta Analysis**.

1. In the **Delta Analysis Name** field, enter the name. The name must be unique across all the analyses.
2. Click **Fabric** to choose the fabric.
3. Click **Choose Earlier Snapshot** and choose the first snapshot for the delta analysis. Click **Apply**.
4. Click **Choose Later Snapshot** and choose the second snapshot for the delta analysis. Click **Apply**.



The two snapshots chosen for the delta analysis must belong to the same fabric.

5. View the Summary of the Delta Analysis created in **Summary**.
6. Click **Save**. The status of the delta analysis is displayed in the **Delta Analysis** table. Post completion, you can **View Delta Analysis** or **Create another Delta Analysis**.

You can perform one delta analysis at a time. To perform another delta analysis, you must stop the current delta analysis and then start the another delta analysis.

1. (Optional) From the Status column, choose an In Progress or Scheduled analysis and click **STOP** in the "**...**" option to stop the delta analysis.
2. The **Delete** in the "**...**" allows you to delete the analysis created.



If there are any errors in the creation of a delta rule, it will be displayed on the summary page of the rule creation as a banner.

View Delta Analysis

The delta analysis page displays the analysis in a tabular form. The analysis are sorted by status. The **Create Delta Analysis** button lets you create a new delta analysis. Click any delta analysis to view more details.

The status of analysis can be either **Aborted**, **Pending**, **Scheduled**, **Stopped**, **Stopping**, **Success**, **Failed**, **Partially Failed**, **Queued**, **Completed** or **In progress**.

The filter bar allows you to filters the analysis by the following factors:

- status
- name
- submitter id
- fabric

The delta analysis dashboard displays general information along with health and policy delta.

- To view the results of health delta analysis, see View Health Delta Analysis.
- To view the results of policy delta analysis, see View Policy Delta Analysis.

View Health Delta Analysis

Health Delta analyses the difference in the health of the fabric across the two snapshots. The results are displayed in the following areas:

The toggle for 'Include Acknowledged Anomalies' allows you to filter out the acknowledged anomalies from the results displayed if enabled. If it is disabled, manually acknowledged anomalies are included in the Anomaly Count.

- **Anomaly Count**: Displays the difference in anomaly count per severity across the snapshots.

The first count represents the anomalies found only in the earlier snapshot. The second count represents the anomalies found only in the later snapshot.

Delta analysis now performs an object delta rather than a count delta. So along with the count, you can now view how many anomalies were cleared, how many are unchanged and how many are new anomalies.

The anomaly count also displays the difference for the different types of anomalies. It is displayed for **Critical**, **Major** and **Warning**.

- **Delta by Resources**: Displays the count of resources by type that are new, lost or unchanged. You can also specifically view the resources who's count has changed by clicking the **View Changed Only** toggle. The filter bar allows you to filter the data by resource. The gear icon allows you to customize the columns as per your view. The table also shows the count delta and the health delta. Count delta includes both healthy and unhealthy resources. Healthy resources will not have any anomalies associated with it if filtered. Health delta shows only unhealthy resources and will return anomalies if filtered by anomalies.

The analysis is available for the following resources :

- Interfaces
- Endpoints
- Spines
- Border Gateways
- Leafs
- Border Leafs
- VLANs
- VRFs
- SVIs
- L2VNIs
- L3VNIs

- VNIs
- VPCs

If you click any of the counts for the Count and Health Delta resources, you can view the list of resources along with the node information. For SVI, the node column provides the VNI association.

- **All Anomalies**: The **Grouped by title** view displays the delta status for grouped anomalies across the snapshots. The **Ungrouped by title** view displays the delta status for each anomaly across the snapshots.

The Anomalies can be listed for the following types:

- New
- Unchanged
- Cleared
- From Earlier Snapshot
- From Later Snapshot

The anomalies are displayed in a tabular form with the following fields:

- Title
- Level
- Category
- Count

> The gear icon allows you to customize the columns as per your view.

You can filter the results based on the following attributes:

- Border Gateways (Leaf)
- Border Leafs (Leaf)
- Interfaces
- L2VNIs
- L3VNIs
- Leafs
- Spines
- SVIs
- VLANs
- VNIs
- VPCs
- VRFs

Choose an anomaly to view the anomaly details.

View Policy Delta Analysis

Click **Policy Delta** to view the policy changes across the two snapshots.

Policy Delta includes 2 sections: Changed Policy Objects and Policy Viewer

- **Changed Policy Objects** displays the changed objects across the two snapshots.
- **Policy Viewer** displays the configuration across the earlier and later snapshots. The switch configuration for the earlier snapshot is called the earlier snapshot policy. The switch configuration for the later snapshot is called the later snapshot policy.
  - Click **Show More Code Above** or **Show More Code Below** to display more content.
  - Click the download icon to export the snapshot policy.
  - You can also view the only the changed configuration by clicking the **View Changed Only** toggle.

Bug Scan

Collecting information on bugs that might affect your network using Bug Scan

Nexus Dashboard Insights collects technical support information from all the devices and runs them against known set of signatures, and flags the corresponding defects and PSIRTs. Nexus Dashboard Insights also generates advisories for PSIRTs and anomalies for defects. See Anomalies and Advisories to learn more about Metadata support.

The Bug Scan feature collects technical support logs from devices in a fabric and scans them for bugs that could have been hit. If the CPU and memory usage is below the set threshold of 65% then the tech support logs are collected and the Bug Scan is carried out for the devices. If the CPU and memory usage is above the set threshold, the devices are excluded from the Bug Scan and eventually will be reconsidered for the next default Bug Scan or when you run an on-demand Bug Scan for that device.

If the node interaction is not healthy on the device, you cannot choose the device for Bug Scan to collect logs. The device cannot be selected to configure a job.

You can also run an on-demand Bug Scan for a fabric. For more information, see the On-Demand Analysis section in Getting Started.

Default Bug Scan

Bug Scan is run for all the fabrics onboarded to Nexus Dashboard Insights and is auto-scheduled every 7 to 14 days for each device, depending on the number of nodes and fabrics on the Nexus Dashboard cluster. This schedule is fixed and is not customizable.

Bug Scan is run on devices contained in a fabric either based on the last Bug Scan or the onboarding time if a Bug Scan has not been run before. Priority is given to devices with a longer time elapsed since the last Bug Scan. After a Bug Scan is run on a device, regardless of whether it succeeds or fails, another Bug Scan will not be run for the same device for the next 7 days.

Bug Scan is auto-scheduled to run on devices only if the CPU and memory metrics for the devices are streamed and the percentage usage is less than 65%.

However, on-demand Bug Scan is an exception and is prioritized over any auto-scheduled runs and does not consider the CPU and memory metrics as it is user-initiated. If auto-scheduled Bug Scan is in progress and on-demand Bug Scan is initiated, based on the available resources in the Nexus Dashboard nodes the on-demand Bug Scan will start while the current Bug Scan is in progress or after the current Bug Scan is completed.

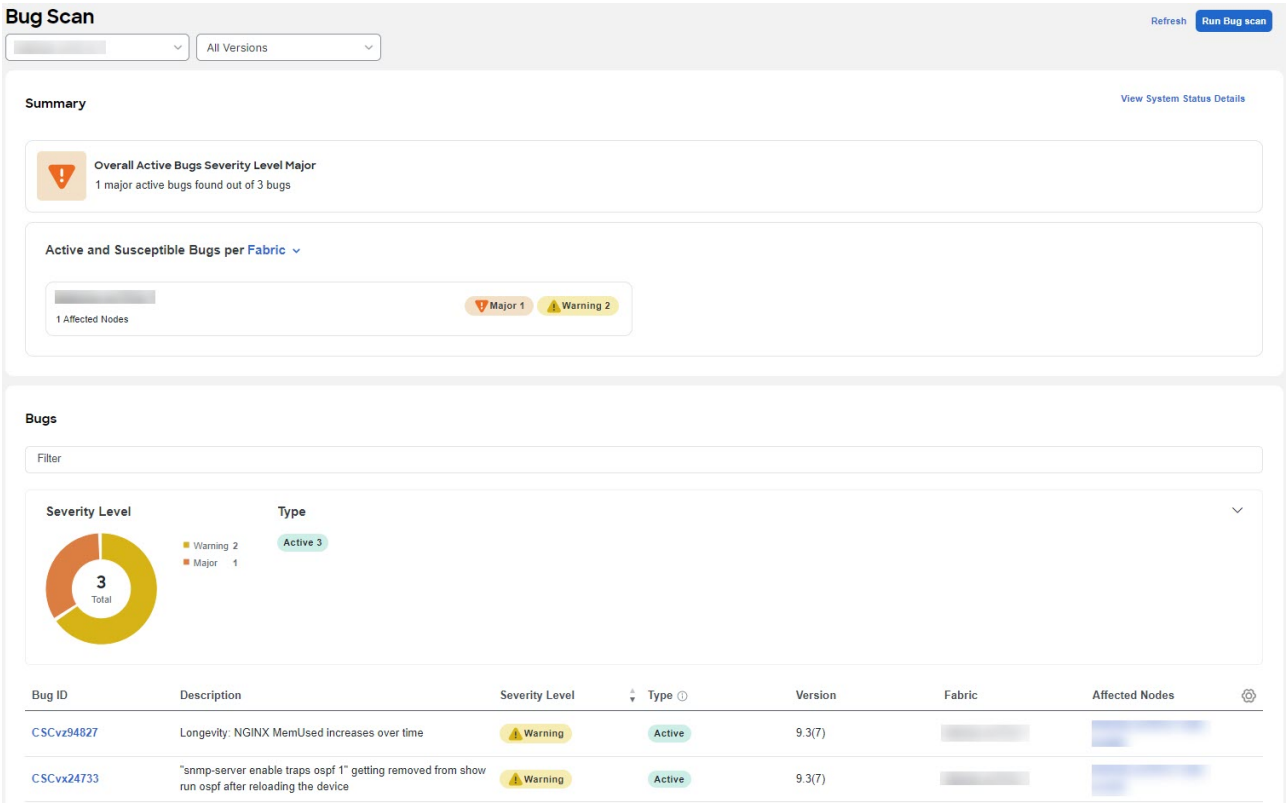
Only one Bug Scan at the time can run on a specific device. However, if you have one set of devices where Bug Scan is already in progress, a second (auto-scheduled or on-demand) Bug Scan can run only if Nexus Dashboard Insights has enough resources available. Otherwise it will be put on hold and started as soon as resources are available.

View Active and Susceptible Bugs

The Bug Scan feature collects technical support logs from devices in a fabric and scans them for bugs that could have been hit. You can view the active and susceptible bugs affecting your network after the Bug Scan is completed.

- Active Bugs - Bugs present in the software version that are detected in your network based on its configuration and tech support files. The signatures are developed with a confidence level. The confidence level indicates the percentage of confidence the signature has in detecting that bug accurately. Active bugs are chosen only when the confidence level of a signature is over 75%.
- Susceptible Bugs - Bugs present in the software version that may potentially impact your network.

1. Navigate to **Analyze** > **Analysis Hub** > **Bug Scan**.
2. Choose an online fabric or multiple online fabrics from the drop-down menu.
3. Choose the software version from the drop-down menu. The active and susceptible bugs for the chosen fabrics and software versions are displayed.



4. The Summary area displays the overall active bugs by severity. You can also view the Bugs per fabric or software version using the drop-down menu.
5. In the Bugs area, use the filter bar to filter the bugs by bug ID, description, severity level, type, and affected nodes.
6. View the **Severity Level** donut chart to see the total number of bugs of Critical, Major, and Warning severity.
7. View the bugs table to see the filtered bugs.

a. Click the column heading to sort the bugs in the table.

b. Click the gear icon to configure the columns in the table.

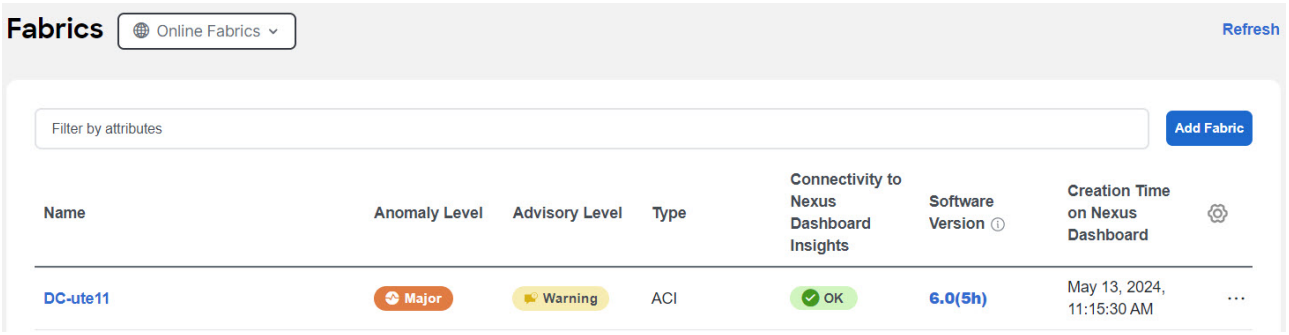
c. Click **Bug ID** to view bug details.

8. Click **Run Bug Scan** to run an on-demand Bug Scan. Choose a fabric and click **Run Now**. For more information, see the On-Demand Analysis section in Getting Started.

View Active and Susceptible Bugs for an Individual Fabric

In Nexus Dashboard Insights, you can also view the bugs for an individual fabric in the following ways:

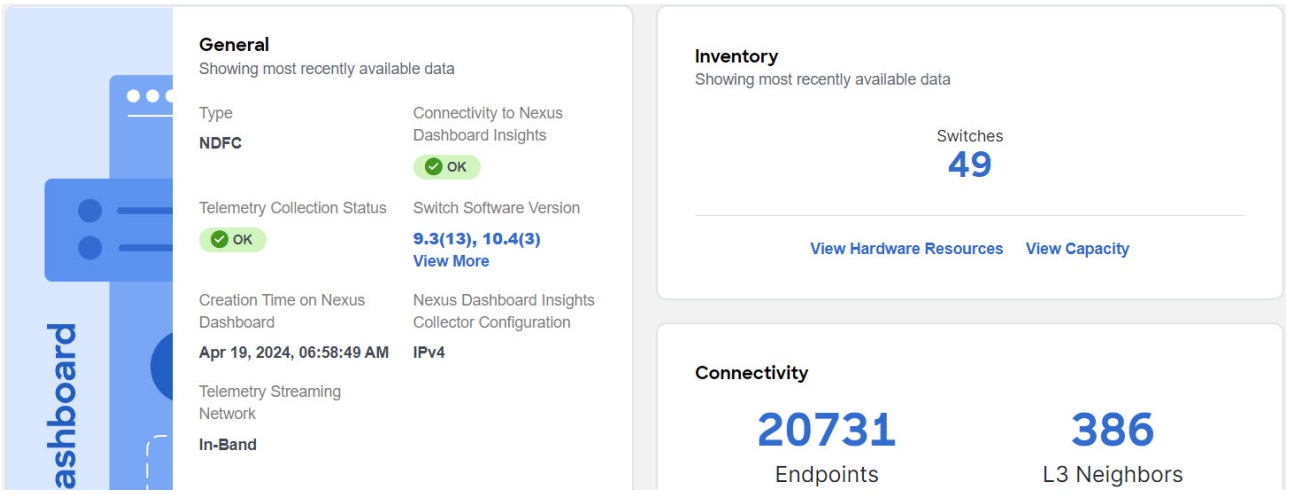
1. Navigate to **Mange** > **Fabrics**
2. Choose **Online Fabrics** from the drop-down menu.



3. In the Software Version column, hover on the software version and click **View Bugs** to view the active and susceptible bugs for that fabric.
4. From the Actions drop-down menu click **Run Bug Scan** to run an on-demand Bug Scan. For more information, see the On-Demand Analysis section in Getting Started.

OR

1. Navigate to **Manage** > **Fabrics**
2. Choose **Online Fabrics** from the drop-down menu.
3. Choose a fabric.



4. In the General area hover on the software version and click **View Bugs** to view the active and susceptible bugs for that fabric.

5. From the Actions drop-down menu click **Run Bug Scan** to run an on-demand Bug Scan. For more information, see the On-Demand Analysis section in Getting Started.

OR

1. Navigate to **Manage** > **Inventory**
2. Choose **Online Fabrics** from the drop-down menu.
3. In the Controllers table hover on the software version in the Software Version column and click **View Bugs** to view the active and susceptible bugs.
4. Click **Switches**. In the Switches table hover on the software version in the Software Version column and click **View Bugs** to view the active and susceptible bugs.
5. From the Actions drop-down menu click **Run Bug Scan** to run an on-demand Bug Scan.For more information, see the On-Demand Analysis section in Getting Started.

OR

1. Navigate to **Manage** > **Fabric Software Management**.
2. In the Software Management Jobs table click an analysis.
3. In the Firmware Summary area, hover on the Node Target Firmware and click **View Bugs** to view the active and susceptible bugs for that particular software version on that fabric.
4. From the Actions drop-down menu click **Run Bug Scan** to run an on-demand Bug Scan. For more information, see the On-Demand Analysis section in Getting Started.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2025 Cisco Systems, Inc. All rights reserved.