Cisco Network Insights for Resources for Cisco DCNM User Guide, Release 2.2.2

Table of Contents

First Published: 2020-07-26

Last Modified: 2020-11-17

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

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 figuresincluded in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbersin illustrative content is unintentional and coincidental.

The Cisco Network Insights for Resources for Cisco DCNM User Guide

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.

Table 1. New Features and Changed Behavior in the Cisco Network Insights for Resources application in Cisco DCNM

Feature	Description	Release	Where Documented
Flow Analytics UI enhancements	The Network Insights setup page provides access to the onboarded sites with additional switch status summary, which displays the monitored and managed sites, health state of the nodes, and software telemetry and flow telemetry configurations.	2.2.2	Network Insights Setup
Flow Ingest	The flow statistics are collected from flow telemetry collector and flow telemetry correlator to determine the health of the flow when the flow threshold is reached. The system status page lists the active system anomalies and flow thresholds.	2.2.2	System Status
Multicast protocols PIM, IGMP, and IGMP Snoop	Support for PIM, IGMP, and IGMP Snoop IPv4 multicast operational and statistical data in the Protocol Statistics tab.	2.2.2	Multicast Protocol Statistics

Feature	Description	Release	Where Documented
Software based Micro-Burst support	The Interface Statistics tab displays the anomalies that are raised based on the number of micro-bursts on the interface for Cisco Nexus 9000 series switches.	2.2.2	Micro-Burst Support for Interface Statistics
Dashboard Topology (Beta)	The topology view represents the stitching between the nodes connected to the Cisco DCNM site. The Early Access Mode in the Network Insights Setup page lets you enable beta Network Insights features and enhancements. Once the beta features are enabled they cannot be disabled.	2.2.2	Topology Dashboard
Dashboard Devices	The detailed view of the nodes with a graphical representation of top nodes and top resources.	2.2.2	Browse Nodes
Telemetry Manager REST API	REST based APIs to configure software telemetry and flow telemetry on the switches.	2.2.2	Cisco NIR DCNM REST API Examples
Endpoint Analytics	The Endpoint Analytics provides detailed analytics of endpoints learnt in the fabric. The anomalies detected as part of endpoint analytics include duplicate IP address, rapid endpoint moves across nodes, interface, and endpoint groups.	2.2.2	Endpoint Analytics

Feature	Description	Release	Where Documented
Hardware support	Support for Cisco Nexus 7000 series switches, Cisco Nexus 3000 series switches, Cisco Nexus 9504 and 9508 with -R and -RX lines cards, and Cisco Nexus 3600 platform switches.	2.2.2	Release Notes

```
Note: See the Cisco NIR for Cisco DCNM Release Notes for Hardware Requirements,
Compatibility, and Verified Scalability information.
```

Cisco Network Insights for Resources Installation

About Cisco Network Insights for Resources

Cisco Network Insights for Resources (Cisco NIR) applications consist of monitoring utilities that can be added to the Cisco Data Center Network Manager (Cisco DCNM).

Downloading Cisco NIR from the Cisco App Center

Before you begin

You must have administrative credentials to download applications in Cisco DCNM.

Procedure

Use this procedure to download Cisco NIR app in the Cisco DCNM in preparation for installation.

1. Log in to the Cisco DCNM GUI with admin privileges. If you don't have admin privileges, you can log in to the Cisco App Center to download the application.
2. Choose **Applications**.
3. Click **Browse App Center** on the far-right side of the screen.
4. Search for Cisco Network Insights for Resources application on the search bar.
5. Select the Cisco Network Insights for Resources application you want to download and click **Download** for that app to begin the process of downloading the app to your local machine.
6. Review the license agreement and, if OK, click **Agree and download**. The Cisco NIR app is downloaded to your local machine. Note the download location of the Cisco NIR app file on your local machine.
7. Make sure the downloaded file can be accessed by the Cisco DCNM. If it cannot, move the file to a device and/or location where it can be installed on the Cisco DCNM.

Installing Cisco NIR Application in Cisco DCNM

Use this procedure to install Cisco NIR app in the Cisco DCNM.

Before you begin

Before you begin installing a Cisco NIR app, make sure the following requirements are met:

Procedure

1. You must have administrator credentials to install Cisco NIR application.
2. You must have three compute servers installed and in the "Joined" state. For more information

regarding the installation, discovery, and addition of compute servers, refer to the following sections:

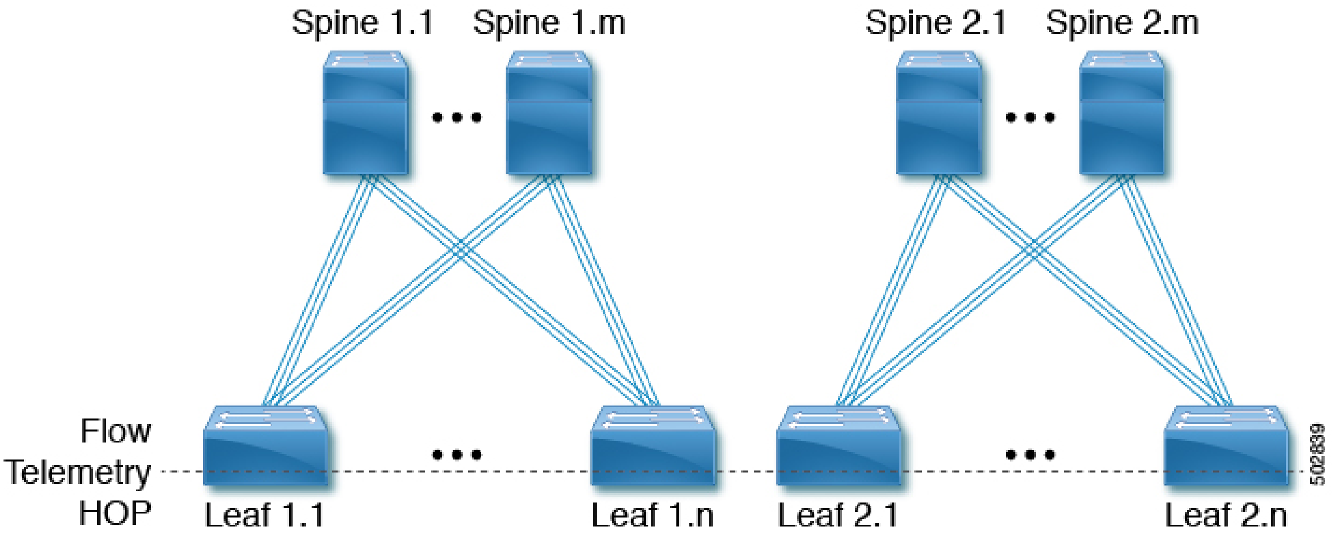
- Compute Installation: For details on compute installation, refer to Installing a DCNM Compute section.
- DVS Security Settings: For details on DVS security settings, refer to Networking Policies for OVA Installation section.
- Subnet Requirements for OOB and IB pool: For details on subnet requirements for OOB and IB pool, refer to Subnet Requirements section.
- Creating a Compute Cluster: For details on creating a compute cluster, refer to Enabling the Compute Cluster section.
- Adding Computers in Web UI: For details on adding computers in web UI, refer to Adding Computers into the Cluster Mode section.

3. When the installation is complete, the application opens to a Welcome dialog where initial setup is performed. Continue with the setup of the Cisco NIR app. See Cisco NIR App Initial Setup.

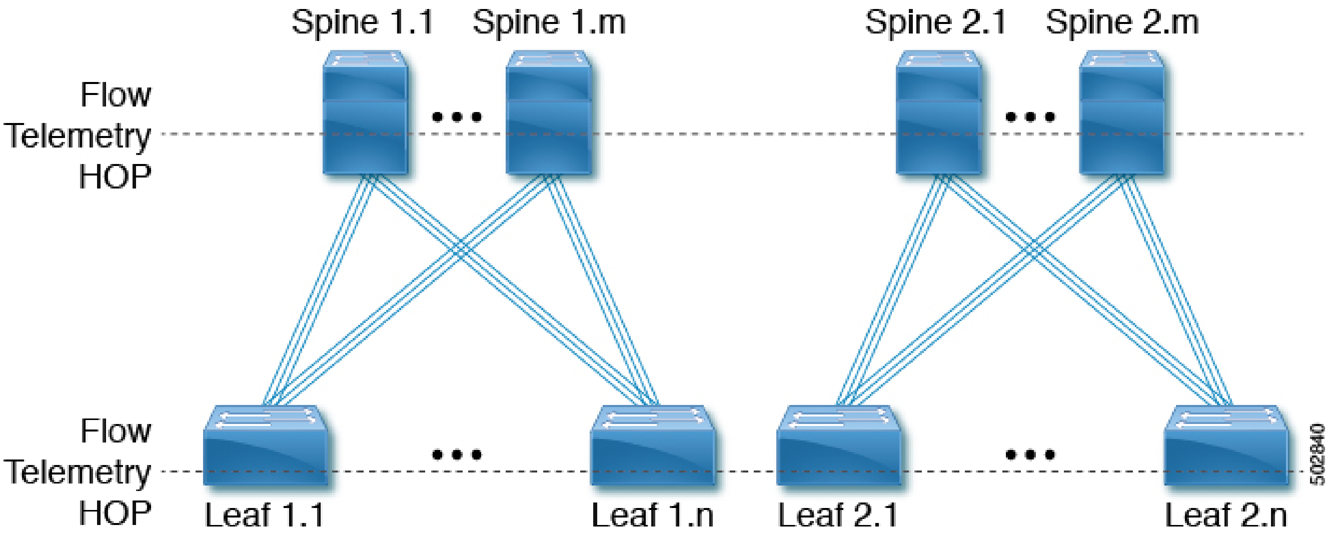
Cisco Network Insights for Resources Setup and Settings

Cisco Network Insights for Resources Topology

The following figure describes the Leaf switch-Spine switch topology for 1-HOP or 2-HOP flow telemetry correlation.



The following figure describes the Leaf switch-Spine switch topology for 3-HOP or 4-HOP flow telemetry correlation.



Supported Scenarios

The Cisco Network Insights for Resources topology supports the following scenarios.

VXLAN

- vPC on leaf switch
- vPC on spine (towards leaf) switch

- Double sided vPC on spine-leaf switch
- Border spine switch
- Border leaf switch
- IR or Multicast underlay
- EBGP or IBGP
- IPv4 underlay
- IPv4 or IPv6 overlay

Legacy spine switch or leaf switch

- vPC on leaf switch
- vPC on spine (towards leaf) switch
- Double sided vPC on spine-leaf switch
- IPv4 or IPv6

Cisco Network Insights for Resources Components in Cisco DCNM

The Cisco Network Insights for Resources (Cisco NIR) is a real-time monitoring and analytics application.

The Cisco NIR app consists of the following components:

- **Data Collection** —The streaming of telemetry data is done by the Operating System on the site nodes. As each data source is different and the format in which data is streamed is different, there are corresponding collectors running analytics that translate the telemetry events from the nodes into data records to be stored in the data lake. The data stored in the data lake is in a format that the analytics pipeline can understand and work upon.

  The following telemetry information is collected from various nodes in the site:

  - Resources Analytics—This includes monitoring software and hardware resources of site nodes on Cisco DCNM.
  - Environmental—This includes monitoring environmental statistics such as fan, CPU, memory, and power of the site nodes.
  - Statistics Analytics—This includes monitoring of nodes, interfaces, and protocol statistics on Cisco DCNM and site nodes.
  - Flow Analytics—This includes detecting anomalies in the flow such as average latency,

packet drop indication, and flow move indication across the site.

  - Endpoint Analytics—This includes monitoring endpoints on the Cisco Site nodes for rapid endpoint moves across nodes, interface, and endpoint groups, and duplicate IP address.

- **Resource Utilization and Environmental Statistics** —Resource analytics supports configuration, operational and hardware resources. Environmental covers CPU, memory, temperature, and fan speed. System analytics also covers, Anomalies, and trending information of each resource and graphing of parameters which help Network operators to debug over period of time.
- **Predictive Analytics and Correlation** —The value-add of this platform is predicting failures in the site and correlating internal site failures to the user-visible/interested failures.
- **Anomaly Detection** —Involves understanding the behavior of each component while using different machine learning algorithms and raising anomalies when the resource behavior deviates from the expected pattern. Anomaly detector applications use different supervised and unsupervised learning algorithms to detect the anomalies in the resources and they log the anomalies in an anomaly database.

Guidelines and Limitations

- The Cisco NIR app installation on Cisco DCNM requires that the DNS server is valid and reachable.
- After upgrading Cisco DCNM or Cisco NIR app to new version and before starting Cisco NIR app, make sure the following are set:
  - Navigate to **Applications** > **Preferences** from Cisco DCNM Configuration page and modify **Telemetry Network Configuration** to the desired value.

    ```
    Note: The `Out-of-Band` is a default value for the interface, which may not be
    what you set prior to the upgrade.
    ```

  - Click Submit.
- When you did not modify the network settings post Cisco DCNM or Cisco NIR app upgrade and enabled telemetry on any sites from Cisco NIR, then the application is not enabled and configured properly.
  - Login to Cisco DCNM active node using SSH client as `root`. Incase you are already logged into Cisco DCNM active node, change to `root`.
  - Execute the following command.

    ```
    ----
    curl -d '{"AppName": "NIR"}' http://127.0.0.1:9595/telemetry/force_cleanup_app
    ----
    ```

  - Execute the following command.

```
----
curl -d '{"AppName": "NIR"}'
http://127.0.0.1:9595/telemetry/force_cleanup_hw_app
----
```

  - After few minutes all the sites in Cisco NIR configuration page show a disabled state.
  - Once the status is disabled, modify the Telemetry Network Configuration in Cisco DCNM to the desired value.
  - Enable telemetry on the sites from the Cisco NIR Configuration page.

- Cisco DCNM allows `network-admin` and `network-operator` roles to assign read or write access for fabrics. Cisco NIR app displays all the fabrics even though you do not have permission to modify. Any operation on a fabric fails without read or write access to the fabric. Cisco NIR app does not enforce the RBAC roles configured in Cisco DCNM, the operations that telemetry manager generates are filtered or enforced by Cisco DCNM according to the RBAC rules configured.
- The Telemetry Manager takes about 10 minutes to detect the site mode changes in Cisco DCNM from managed mode to monitored mode or vice versa.
- To enable telemetry on monitored site through Cisco NIR app, you must first delete all existing telemetry configurations on all the nodes in the monitored site before you enable this site from Cisco NIR app. The telemetry then assigns the receiver IP addresses to these nodes, which the Data Collection Setup page displays. The telemetry configuration will not push any telemetry configurations to the nodes because they are monitored. Therefore you have to check the receiver IP addresses from the Data Collection Setup page and must configure the nodes manually.
- For flow telemetry the Cisco NIR app captures the maximum anomaly score for a particular flow, for the entire cycle of the user specified time range. This anomaly score calculation is inconsistent with the other resources anomaly calculation.
- After enabling telemetry in Cisco NIR app in managed mode, to upgrade or downgrade a switch follow these steps:
  - Perform the upgrade or downgrade of the switch.
  - Remove and add the switch back to the site. Cisco NIR will then push the configurations to the switch.
- Cisco NIR app does not support software telemetry and flow telemetry data from switches to the flow collector running on Cisco DCNM compute nodes over IPv6.
- The Cisco NIR application requires that physical servers hosting Cisco DCNM computes as VMs are atleast Cisco C220-M4 category. It is also required that a compute be hosted on a data store with a dedicated hard disk of atleast 500GB. See Cisco NIR Release notes Compatibility Information section.
- For instances where one or more sites do not recover from disabling state, you must stop and restart the Cisco NIR application in Cisco DCNM. This will recover the failed disable state.
- The vPC domain ID for different vPC pair can not be the same across a fabric, when the Cisco NIR app is in managed or monitored mode on Cisco DCNM.

- Cisco Nexus 7000 switches support only software telemetry in default VDC. Software telemetry fails to get enabled if the default VDC does not have modules and interfaces.

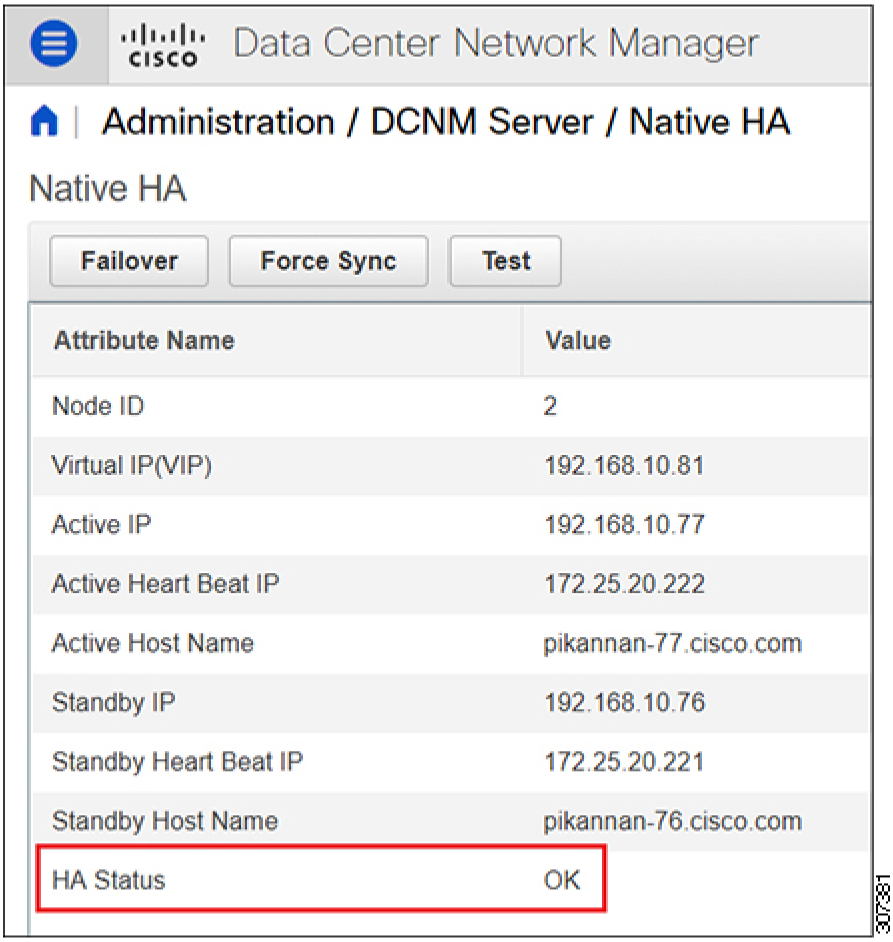
Cisco NIR App Initial Setup

The first time you launch the Cisco NIR app, you are greeted with a **Welcome to Network Insights** dialog. Follow these steps to complete the initial setup of Cisco NIR app:

Before you begin

Before you begin the initial set up of the Cisco NIR application in the Cisco DCNM, make sure the following prerequisites are met:

- The primary and standby hosts (HA) return a status of OK:
  1. In Cisco DCNM, click **Administration**.
  2. Under Cisco DCNM Server, click **Native HA**.
  3. Check the **HA Status** attribute as shown in the following

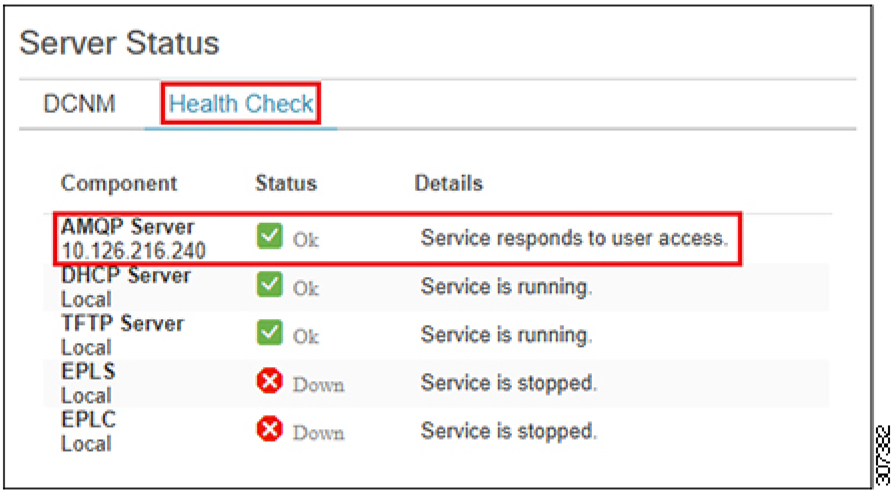

Data Center Network Manager
Administration / DCNM Server / Native HA
Native HA
Failover
Force Sync
Test
307381

Attribute Name	Value
Node ID	2
Virtual IP(VIP)	192.168.10.81
Active IP	192.168.10.77
Active Heart Beat IP	172.25.20.222
Active Host Name	pikannan-77.cisco.com
Standby IP	192.168.10.76
Standby Heart Beat IP	172.25.20.221
Standby Host Name	pikannan-76.cisco.com
HA Status	OK

It may take some time for both hosts to be recognized. Once the OK status is displayed, AMQP notifications can begin. Check the AMQP server status below.

- The AMQP Server returns a status of OK:
  1. In Cisco DCNM, click **Dashboard**.

2. In the *Server Status* tile, click **Health Check**.
3. Check the status of the **AMQP Server** component as shown in the following



Component	Status	Details
AMQP Server 10.126.216.240	✓ Ok	Service responds to user access.
DHCP Server Local	✓ Ok	Service is running.
TFTP Server Local	✓ Ok	Service is running.
EPLS Local	☒ Down	Service is stopped.
EPLC Local	☒ Down	Service is stopped.

- Precision Time Protocol (PTP) must be configured on all nodes you want to support with Cisco NIR. In both managed and monitor site mode, the user must ensure PTP is correctly configured on all nodes in the site. To ensure Precision Time Protocol is setup correctly:
    - For details about Precision Time Protocol Easy Fabric, refer to Precision Time Protocol for Easy Fabric.

      Ensure PTP is enabled in Cisco DCNM easy site setup. The **Advanced** tab on Cisco DCNM site setup, check the box for *Enable Precision Time Protocol (PTP)*. For details, refer to Add/Edit Fabric.

Procedure

1. On the welcome dialog, click **Begin First Time Setup**.

   The *Network Insights Setup* window appears.

2. On the *Network Insights Setup* window, click **Configure** to configure the **Data Collection Setup**.

   The following steps enable the site to be monitored by Cisco NIR application.

3. In the list of available sites, choose a site you want to monitor with Cisco NIR.
4. In the **VXLAN** / **Classic** column, choose the site type:
    - **VXLAN**: Identifies the site as a VXLAN site type.

      If your network is a VXLAN site and you want to see VXLAN-specific information in the Cisco NIR application, you must select this option.

    - **Classic**: Identifies the site as a Classic LAN site.
5. In the **Mode** column, choose the mode you want to use for the site selected:
    - **Managed** : Cisco DCNM monitors and manages the configuration of the nodes in the selected site. This option allows Cisco NIR app to push the telemetry configuration to the nodes in the chosen site.

- **Monitored** : Cisco DCNM does not deploy configuration to the nodes. Cisco DCNM discovers the nodes and displays them in the topology (read-only). Cisco NIR app will not send telemetry configuration to the nodes.

> If this option is chosen, telemetry **must** be configured directly on the nodes in order for Cisco NIR app to receive data. The following configuration must be added on the NX-OS switches to stream telemetry data to Cisco NIR app when the site is configured to be in *Monitored* mode:

The REST API software_telemetry_config() and flow_telemetry_config() can be used in managed mode and monitor mode; however, monitor mode has the best use case. See Cisco NIR DCNM REST API Examples for details.

Example:

```
configure terminal

{

feature ntp
ntp server <IP address> prefer use-vrf management

feature lldp
feature icam
feature telemetry

telemetry
  destination-profile
  use-vrf management
destination-group 500
    ip address <IP address of> port 57500 protocol gRPC encoding GPB
    use-chunking size 4096
destination-group 501
    ip address <IP address of> port 57500 protocol gRPC encoding GPB-compact
    use-chunking size 4096
sensor-group 506
    data-source NX-API
    path "show system routing mode" depth unbounded
sensor-group 511
    data-source DME
    path sys/intf depth unbounded filter-condition
or(and(updated(ethpmAggrIf.operSt),eq(ethpmAggrIf.operSt,"down")),and(updated(et
hpmAggrIf.operSt),eq(ethpmAggrIf.operSt,"up")))
sensor-group 500
    data-source NX-API
    path "show icam scale" depth unbounded
    path "show environment temperature" depth unbounded
    path "show spanning-tree summary" depth unbounded
    path "show processes cpu" depth unbounded
    path "show processes memory physical" depth unbounded
    path "show system resources" depth unbounded
    path "show module" depth unbounded
    path "show processes log" depth unbounded
sensor-group 502
    data-source DME
    path sys/intf depth 0 query-condition query-target=subtree&target-subtree-
class=ethpmPhysIf,rmonEtherStats,rmonIfIn,rmonIfOut,ethpmAggrIf,l1PhysIf,pcAggrI
f,ethpmPortCap
sensor-group 503
    data-source DME
    path sys/intf depth 0 query-condition query-target=subtree&target-subtree-
class=eqptFcotLane,eqptFcotSensor
sensor-group 504
    data-source NX-API
    path "show routing ip summary cached vrf all" depth unbounded
    path "show routing ipv6 summary cached vrf all" depth unbounded
    path "show ip mroute summary vrf all" depth unbounded
    path "show ipv6 mroute summary vrf all" depth unbounded
    path "show vpc" depth unbounded
    path "show vrf all" depth unbounded
    path "show mac address-table count" depth unbounded
    path "show nve vni" depth unbounded
    path "show nve peers detail" depth unbounded
    path "show vlan summary" depth unbounded
    path "show system internal icam app hardware internal forwarding table
utilization" depth unbounded query-condition show-output-format=json
    path "show system internal icam app system internal access-list resource
utilization" depth unbounded query-condition show-output-format=json
sensor-group 505
    data-source NX-API
    path "show environment power" depth unbounded
    path "show system internal flash" depth unbounded
    path "show clock" depth unbounded
    path "show feature" depth unbounded
    path "show environment fan detail" depth unbounded
sensor-group 501
    data-source NX-API
    path "show lacp counters detail" depth unbounded
    path "show lacp interface" depth unbounded
    path "show port-channel summary" depth unbounded
    path "show lldp traffic interface all" depth unbounded
sensor-group 507
    data-source DME
    path sys/cdp depth 1 query-condition query-target=subtree&target-subtree-
class=cdpIf,cdpAdjEp,cdpIfStats
    path sys/bgp depth 1 query-condition query-target=subtree&target-subtree-
class=bgpEntity,bgpInst,bgpDom,bgpDomAf,bgpPeer,bgpPeerEntry,bgpPeerEntryStats,b
gpPeerEvents,bgpPeerAfEntry
    path sys/lldp depth 1 query-condition query-target=subtree&target-subtree-
class=lldpIf,lldpAdjEp,lldpIfStats
sensor-group 508
```

```
    data-source DME
    path sys/intf depth 1 query-condition query-target=subtree&target-subtree-class=pcAggrIf&query-target-filter=deleted()
sensor-group 509
    data-source NX-API
    path "show ip igmp interface vrf all" depth unbounded
    path "show ip igmp groups vrf all" depth unbounded
    path "show ip igmp snooping statistics" depth unbounded
    path "show ip igmp snooping" depth unbounded
    path "show ip igmp snooping groups" depth unbounded
    path "show ip igmp snooping groups summary" depth unbounded
    path "show ip igmp snooping groups detail" depth unbounded
    path "show ip pim statistics vrf all" depth unbounded
    path "show ip pim interface vrf all" depth unbounded
    path "show ip pim neighbor vrf all" depth unbounded
    path "show ip pim rp vrf all" depth unbounded
    path "show ip pim route vrf all" depth unbounded
    path "show queuing burst-detect detail" depth unbounded
sensor-group 510
    data-source NATIVE
    path adjacency
    path mac-all
subscription 500
    dst-grp 500
    snsr-grp 506 sample-interval 3600000
    snsr-grp 511 sample-interval 0
    snsr-grp 500 sample-interval 59000
    snsr-grp 502 sample-interval 60000
    snsr-grp 503 sample-interval 62000
    snsr-grp 504 sample-interval 61000
    snsr-grp 505 sample-interval 300000
    snsr-grp 501 sample-interval 60000
    snsr-grp 507 sample-interval 65000
    snsr-grp 508 sample-interval 0
    snsr-grp 509 sample-interval 63000
subscription 501
    dst-grp 501
    snsr-grp 510 sample-interval 0
end
```

6. Click **Save**.

7. Click **Done**.

   The second time you launch the Cisco NIR application, click **Review First Time Setup** to review the setup. Check **Do not show on launch** for the splash screen welcome dialog to not appear again.

Cisco NIR App Settings

Once Cisco NIR app is installed, the following need to be configured for the application to be fully set up:

- Data Collection Setup—Click **Edit Configuration** for a list of sites, status, enable, disable, and delete sites. The site status is disabled by default.
- The Early Access Mode lets you enable beta Network Insights features and enhancements. Once the beta features are enabled, they cannot be disabled.

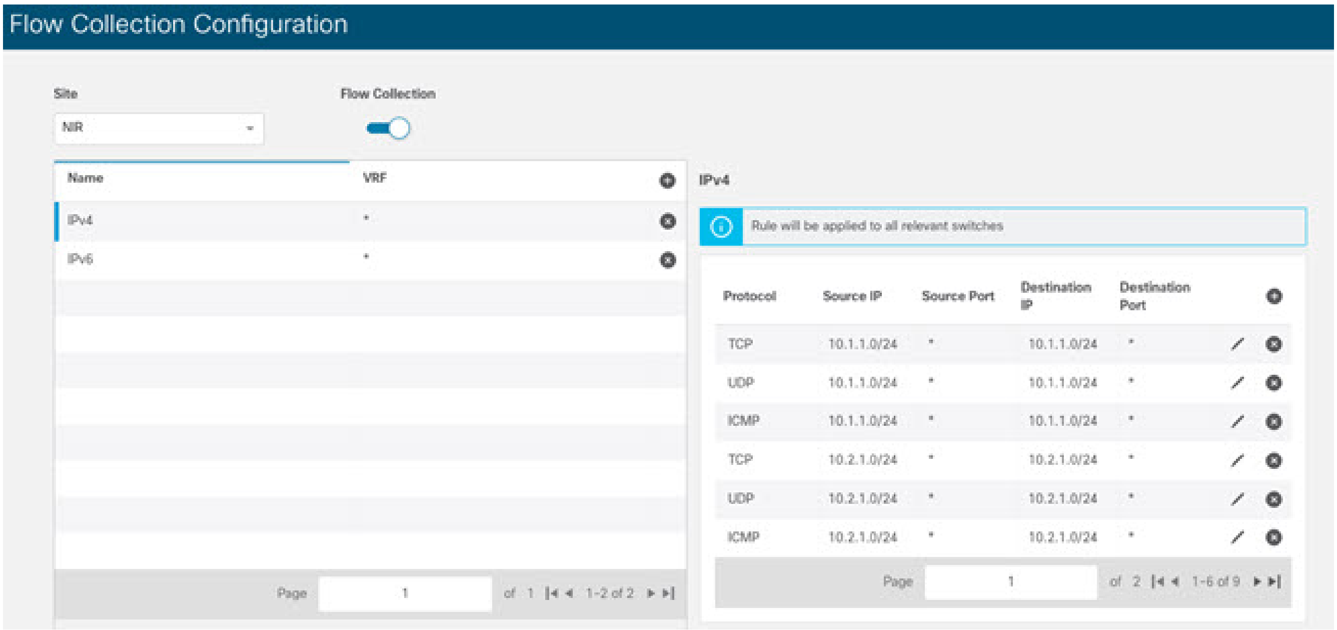
If there are Faults present in the application, they will show on the Faults tab. In the **Settings** menu click **Collection Status**, you should see the green circles in the table indicating the nodes where information is being transmitted. The collection status displays the data for the last hour.

Property	Description
Time Range	Specify a time range for the summary table to display the data that is collected during the specified interval.
Site	Choose a site containing the nodes from which to collect telemetry data.

Property	Description
⚙	Clicking this icon allows you to alter the following: - **Flow Collection Configuration**—Lets you assign a previously configured site. Create a VRF flow collection rule configuration per site: ◦ Choose the site from the drop-down menu. ◦ Select the switch to create a flow collection rule. ◦ Click **Save**. ◦ Toggle **Flow Collection** to enable flow telemetry on the switches. - **System Status**—Displays software, hardware, operational, and capacity usage of the application on the compute cluster. - **Collection Status**—Displays data collection of System Metrics, Software Telemetry, and Flow Telemetry information per node for the last hour. - **Network Insights Setup**—Lets you configure the application setup. - **About Network Insights**—Displays the application version number.
?	Clicking this icon allows you to view the following: - **Quick Start Guide**—An overview of Cisco NIR application. - **Welcome Screen**—The splash screen to start the Cisco NIR application from the beginning. - **User Guide**—The documentation for installation, configuration, and use of Cisco NIR application.

Flow Collection Configuration

Click **Settings** > **Flow Collection Configuration** to display the following page.



Flow Collection Configuration

Site: NIR

Flow Collection: on

Name	VRF
IPv4	*
IPv6	*

Page 1 of 1 1-2 of 2

IPv4

Rule will be applied to all relevant switches

Protocol	Source IP	Source Port	Destination IP	Destination Port
TCP	10.1.1.0/24	*	10.1.1.0/24	*
UDP	10.1.1.0/24	*	10.1.1.0/24	*
ICMP	10.1.1.0/24	*	10.1.1.0/24	*
TCP	10.2.1.0/24	*	10.2.1.0/24	*
UDP	10.2.1.0/24	*	10.2.1.0/24	*
ICMP	10.2.1.0/24	*	10.2.1.0/24	*

Page 1 of 2 1-6 of 9

System Status

Click **Settings** > **System Status** to display the following page.

The system status page displays the health of flows. When there are system alerts over a recent time duration, click **Show All Alerts**.

The health container periodically monitors the statistics and raises system anomalies when it detects abnormalities.

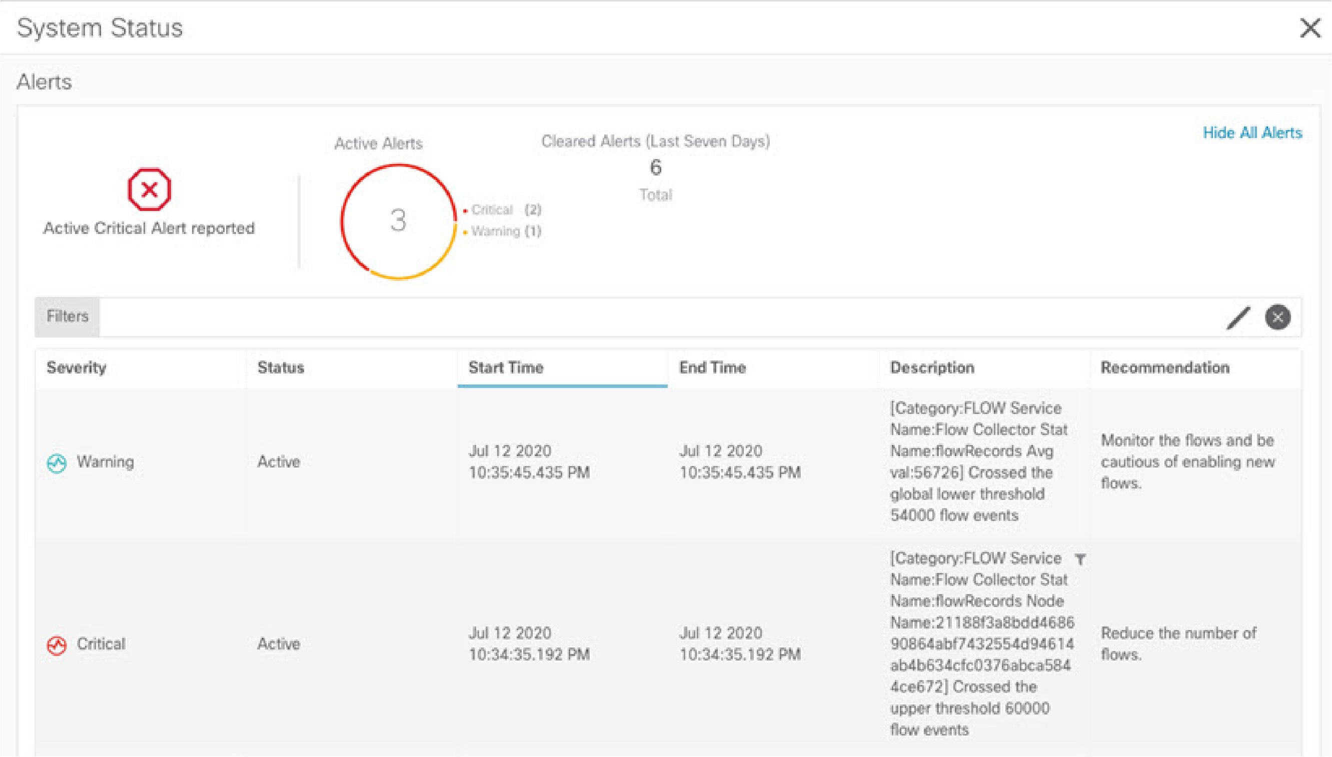
The summary table lists the system anomalies or alerts raised over a duration, severity set to either warning or critical, status, description, and recommendation. Statistics are collected from the flow telemetry collector and flow telemetry correlator.

The following system anomalies are summarized.

- **Flow Telemetry Collector**—Flow collector reports the number of flow telemetry records known as flow events averaged over 30 seconds and specifies two thresholds; global threshold and compute threshold. The compute thresholds are per compute and global threshold are for all computes in the Cisco DCNM. The collector container is stressed because it is processing more flow telemetry records than its threshold.
- **Flow Telemetry Correlator**—Flow correlator reports the stitched flows averaged over 30 seconds and specifies two thresholds; Global Lower and Global Upper threshold breached over a period of time. The threshold occurs when the number of unique flows have increased and the system is under pressure.

When a lower threshold is breached then a warning system anomaly is raised and when the upper threshold is crossed then a critical anomaly is raised.

Flow Collector Anomalies



System Status

Alerts

Active Critical Alert reported

Active Alerts

3

• Critical (2)
• Warning (1)

Cleared Alerts (Last Seven Days)

6

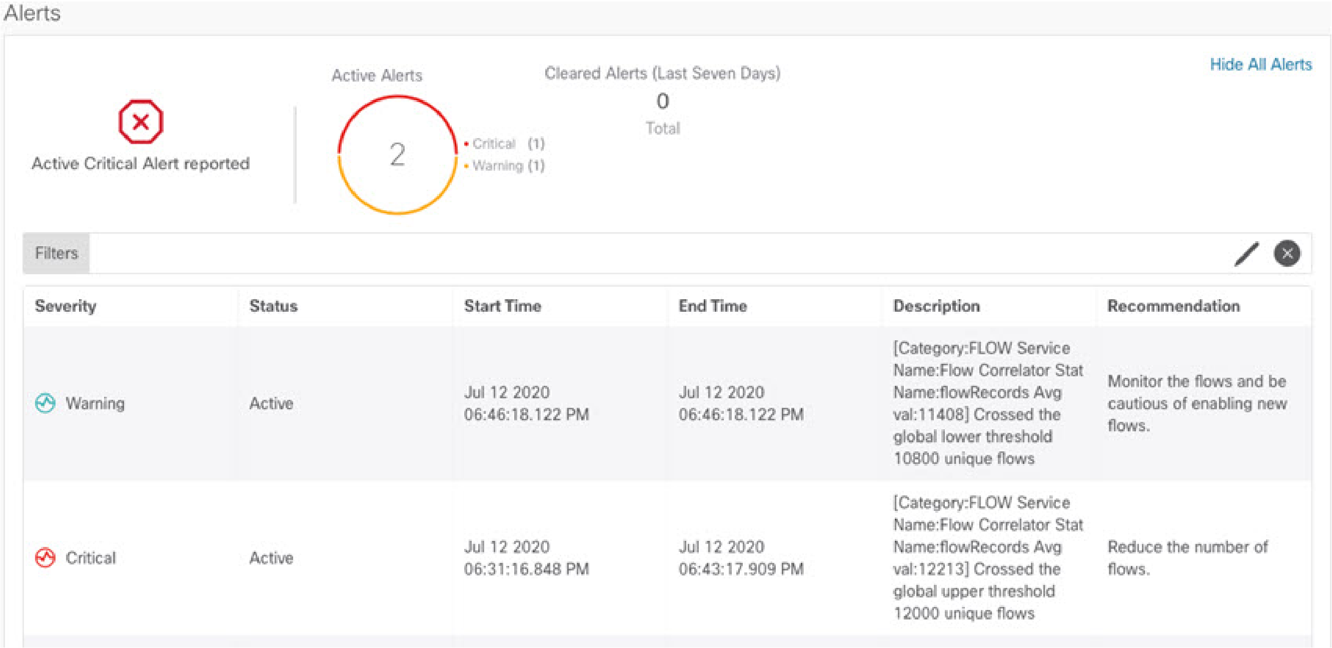
Total

Hide All Alerts

Filters

Severity	Status	Start Time	End Time	Description	Recommendation
Warning	Active	Jul 12 2020 10:35:45.435 PM	Jul 12 2020 10:35:45.435 PM	[Category:FLOW Service Name:Flow Collector Stat Name:flowRecords Avg val:56726] Crossed the global lower threshold 54000 flow events	Monitor the flows and be cautious of enabling new flows.
Critical	Active	Jul 12 2020 10:34:35.192 PM	Jul 12 2020 10:34:35.192 PM	[Category:FLOW Service Name:Flow Collector Stat Name:flowRecords Node Name:21188f3a8bdd468690864abf7432554d94614ab4b634cfc0376abca5844ce672] Crossed the upper threshold 60000 flow events	Reduce the number of flows.

Flow Correlator Anomalies



Alerts

Active Critical Alert reported

Active Alerts

2

• Critical (1)
• Warning (1)

Cleared Alerts (Last Seven Days)

0

Total

Hide All Alerts

Filters

Severity	Status	Start Time	End Time	Description	Recommendation
Warning	Active	Jul 12 2020 06:46:18.122 PM	Jul 12 2020 06:46:18.122 PM	[Category:FLOW Service Name:Flow Correlator Stat Name:flowRecords Avg val:11408] Crossed the global lower threshold 10800 unique flows	Monitor the flows and be cautious of enabling new flows.
Critical	Active	Jul 12 2020 06:31:16.848 PM	Jul 12 2020 06:43:17.909 PM	[Category:FLOW Service Name:Flow Correlator Stat Name:flowRecords Avg val:12213] Crossed the global upper threshold 12000 unique flows	Reduce the number of flows.

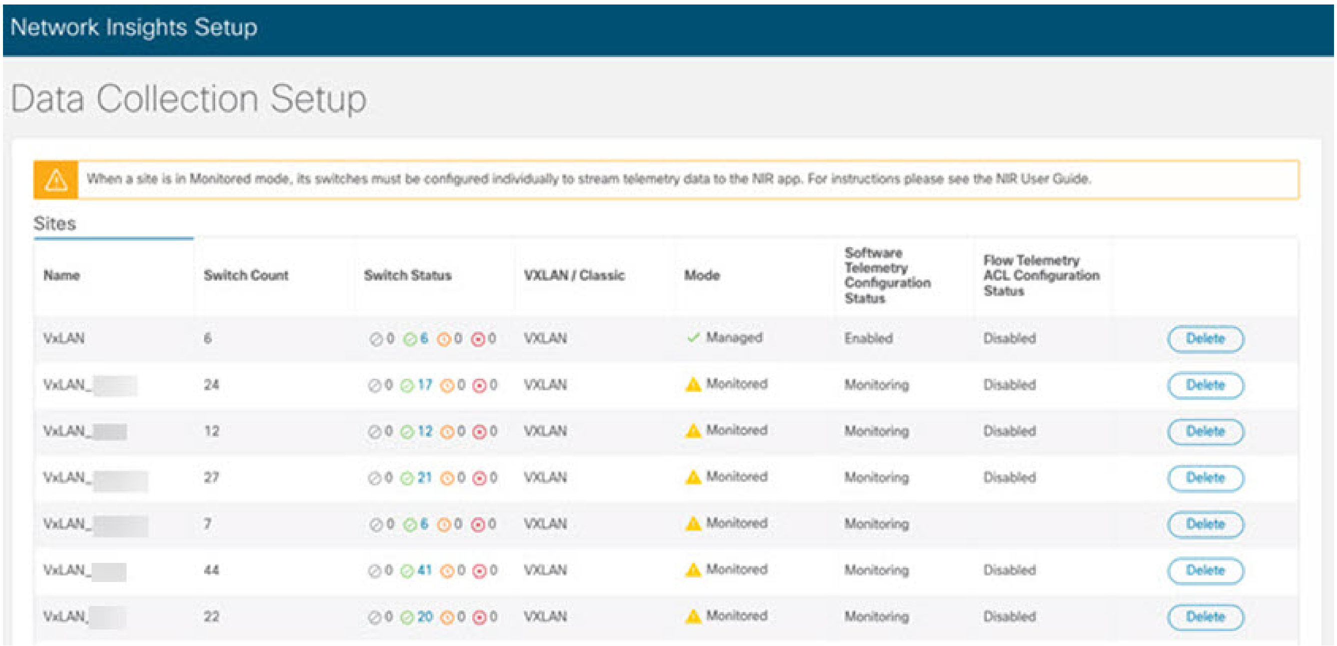
Service Level Thresholds

System Anomalies	Description
Flow Telemetry Collector	The following are flow thresholds: • Lower Threshold—54000 • Global Lower Threshold—54000 • Upper Threshold—60000 • Global Upper Threshold—60000

System Anomalies	Description
Flow Telemetry Correlator	The following are flow thresholds: • Global Lower Threshold—10800 • Global Upper Threshold—12000

Network Insights Setup

Click **Settings** > **Network Insights Setup** > **Edit Configuration**. The following page displays the onboarded sites on Cisco DCNM.



Network Insights Setup

Data Collection Setup

⚠ When a site is in Monitored mode, its switches must be configured individually to stream telemetry data to the NIR app. For instructions please see the NIR User Guide.

Sites

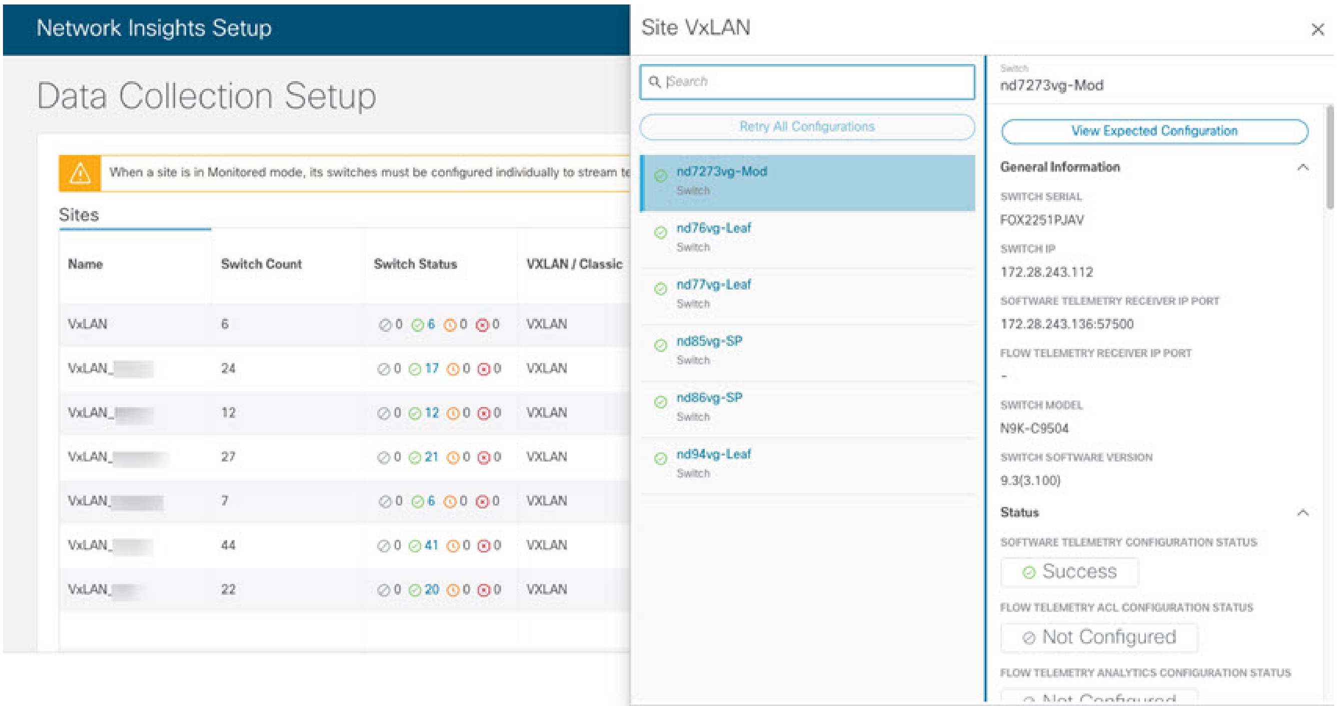
Name	Switch Count	Switch Status	VXLAN / Classic	Mode	Software Telemetry Configuration Status	Flow Telemetry ACL Configuration Status	
VxLAN	6	⊘0 ✓6 ⊙0 ⊙0	VXLAN	✓ Managed	Enabled	Disabled	Delete
VxLAN_[redacted]	24	⊘0 ✓17 ⊙0 ⊙0	VXLAN	⚠ Monitored	Monitoring	Disabled	Delete
VxLAN_[redacted]	12	⊘0 ✓12 ⊙0 ⊙0	VXLAN	⚠ Monitored	Monitoring	Disabled	Delete
VxLAN_[redacted]	27	⊘0 ✓21 ⊙0 ⊙0	VXLAN	⚠ Monitored	Monitoring	Disabled	Delete
VxLAN_[redacted]	7	⊘0 ✓6 ⊙0 ⊙0	VXLAN	⚠ Monitored	Monitoring		Delete
VxLAN_[redacted]	44	⊘0 ✓41 ⊙0 ⊙0	VXLAN	⚠ Monitored	Monitoring	Disabled	Delete
VxLAN_[redacted]	22	⊘0 ✓20 ⊙0 ⊙0	VXLAN	⚠ Monitored	Monitoring	Disabled	Delete

Double click **Switch Status** for the side pane to display the onboarded switch configurations, status, and additional details.

The following are the switch status:

- **Grey**—Nodes are in initial state and unconfigured.
- **Green**—Nodes configured successfully.
- **Orange**—Nodes are currently being configured.
- **Red**—Nodes that failed configuration.

```
Note: When you enable the telemetry configuration for a site and if Red Count is
greater than 0, it implies that the initiated operation is not successful for
enabling or disabling the site. Click Count and then click Retry for configuration
to be pushed again to nodes. Click Any Counts to view expected configurations. You
can exit the Network Insights Setup screen and return for immediate refresh of the
screens.
```



Network Insights Setup

Data Collection Setup

When a site is in Monitored mode, its switches must be configured individually to stream te

Sites

Name	Switch Count	Switch Status	VXLAN / Classic
VxLAN	6	⊘ 0 ✓ 6 ◷ 0 ⊗ 0	VXLAN
VxLAN_[redacted]	24	⊘ 0 ✓ 17 ◷ 0 ⊗ 0	VXLAN
VxLAN_[redacted]	12	⊘ 0 ✓ 12 ◷ 0 ⊗ 0	VXLAN
VxLAN_[redacted]	27	⊘ 0 ✓ 21 ◷ 0 ⊗ 0	VXLAN
VxLAN_[redacted]	7	⊘ 0 ✓ 6 ◷ 0 ⊗ 0	VXLAN
VxLAN_[redacted]	44	⊘ 0 ✓ 41 ◷ 0 ⊗ 0	VXLAN
VxLAN_[redacted]	22	⊘ 0 ✓ 20 ◷ 0 ⊗ 0	VXLAN

Site VxLAN

Switch
nd7273vg-Mod

General Information

SWITCH SERIAL
FOX2251PJAV

SWITCH IP
172.28.243.112

SOFTWARE TELEMETRY RECEIVER IP PORT
172.28.243.136:57500

FLOW TELEMETRY RECEIVER IP PORT
-

SWITCH MODEL
N9K-C9504

SWITCH SOFTWARE VERSION
9.3(3.100)

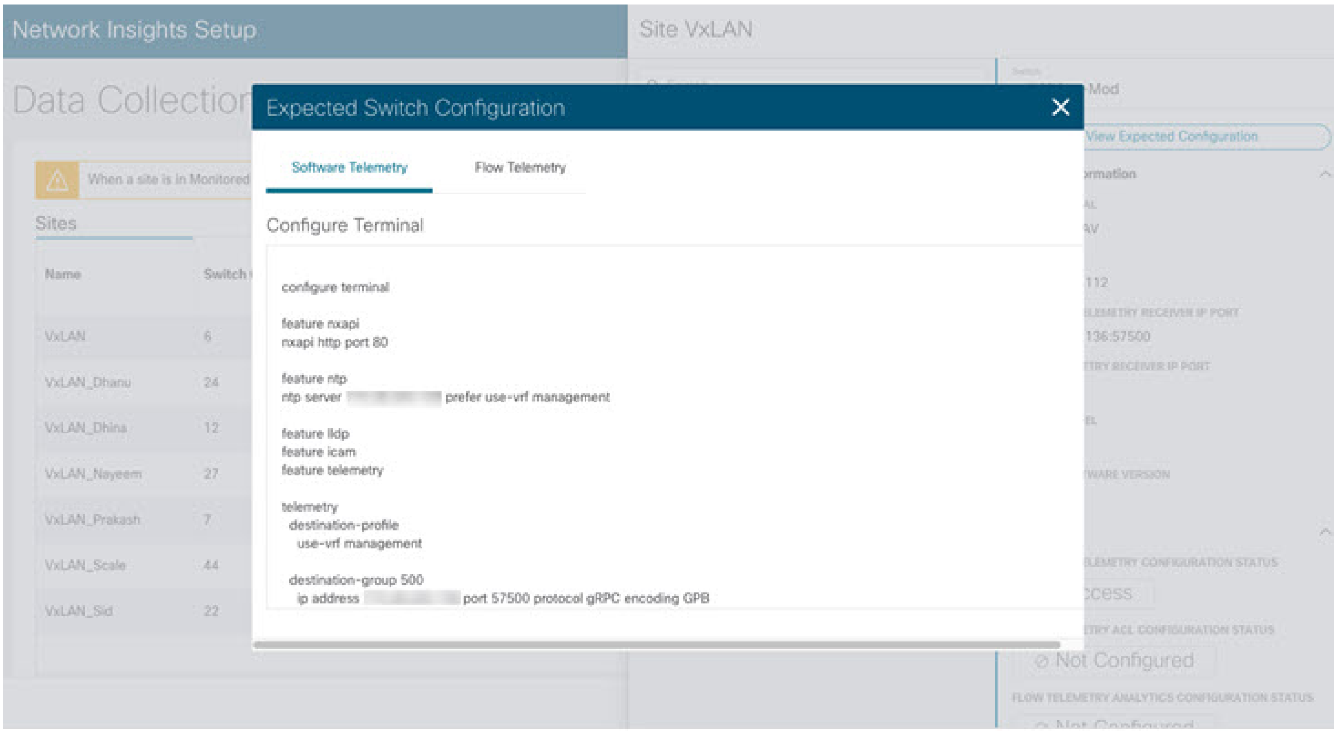
Status

SOFTWARE TELEMETRY CONFIGURATION STATUS
✓ Success

FLOW TELEMETRY ACL CONFIGURATION STATUS
⊘ Not Configured

FLOW TELEMETRY ANALYTICS CONFIGURATION STATUS
⊘ Not Configured

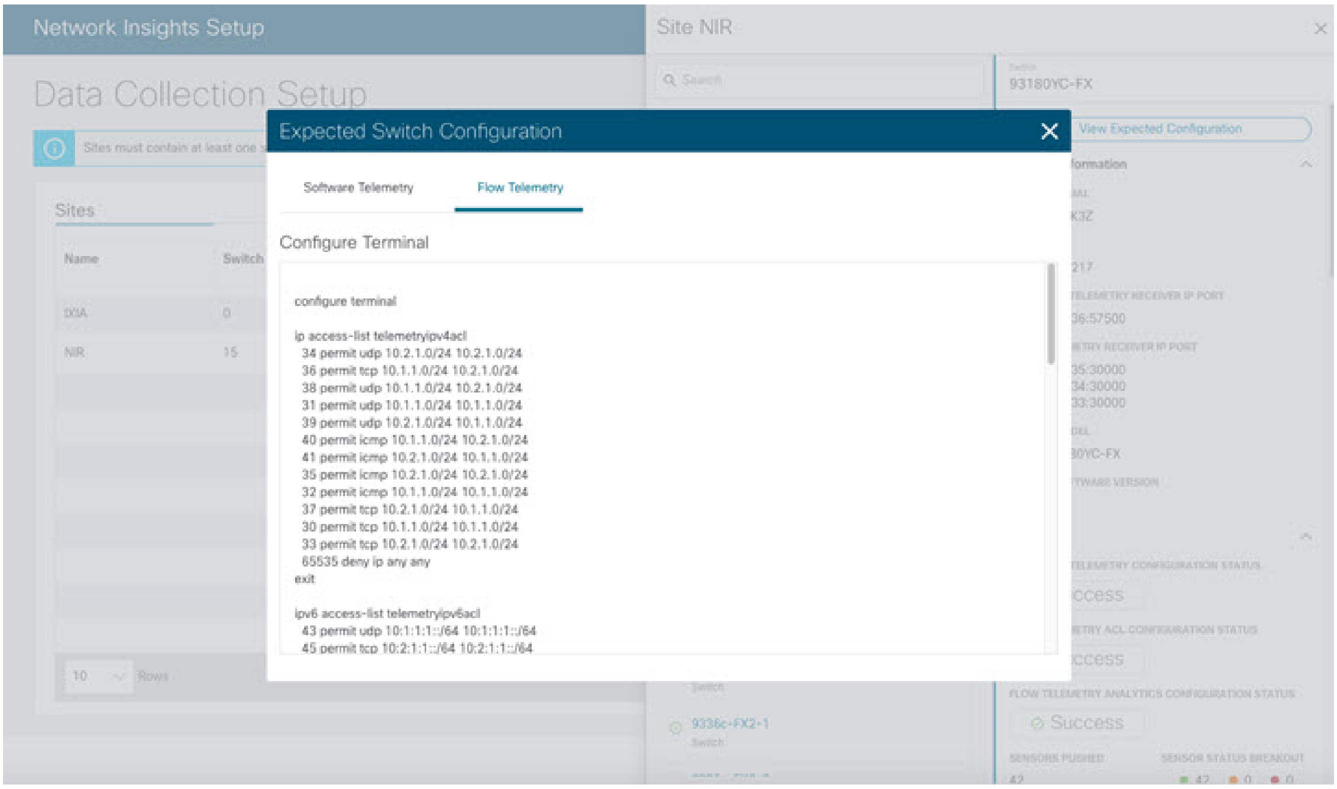
Click **View Expected Configuration** for Software Telemetry and Flow Telemetry health information using the REST API.



Expected Switch Configuration

Configure Terminal

```
configure terminal

feature nxapi
nxapi http port 80

feature ntp
ntp server [redacted] prefer use-vrf management

feature lldp
feature icam
feature telemetry

telemetry
 destination-profile
  use-vrf management

 destination-group 500
  ip address [redacted] port 57500 protocol gRPC encoding GPB
```



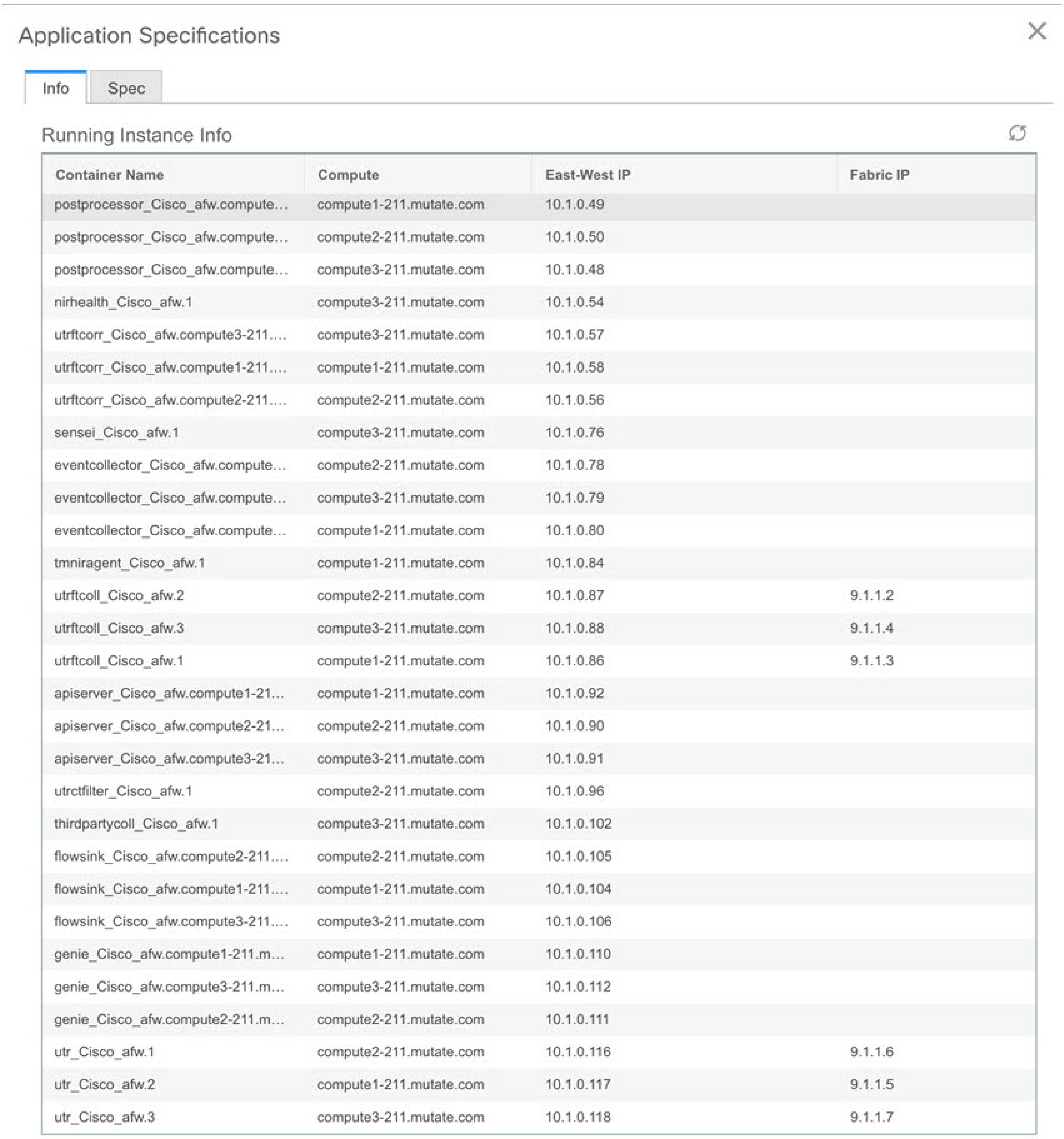
Configure Terminal

```
configure terminal

ip access-list telemetryipv4acl
  34 permit udp 10.2.1.0/24 10.2.1.0/24
  36 permit tcp 10.1.1.0/24 10.2.1.0/24
  38 permit udp 10.1.1.0/24 10.2.1.0/24
  31 permit udp 10.1.1.0/24 10.1.1.0/24
  39 permit udp 10.2.1.0/24 10.1.1.0/24
  40 permit icmp 10.1.1.0/24 10.2.1.0/24
  41 permit icmp 10.2.1.0/24 10.1.1.0/24
  35 permit icmp 10.2.1.0/24 10.2.1.0/24
  32 permit icmp 10.1.1.0/24 10.1.1.0/24
  37 permit tcp 10.2.1.0/24 10.1.1.0/24
  30 permit tcp 10.1.1.0/24 10.1.1.0/24
  33 permit tcp 10.2.1.0/24 10.2.1.0/24
  65535 deny ip any any
exit

ipv6 access-list telemetryipv6acl
  43 permit udp 10:1:1:1::/64 10:1:1:1::/64
  45 permit tcp 10:2:1:1::/64 10:2:1:1::/64
```

See the REST API software_telemetry_config() and flow_telemetry_config() from Cisco NIR DCNM REST API Examples for details.

Cisco NIR Service Instance Status

To view Cisco NIR app service instance status, exit the Cisco NIR app and click the gear image in the lower left corner of the Cisco NIR app icon in the Cisco DCNM application work pane.



Running Instance Info

Container Name	Compute	East-West IP	Fabric IP
postprocessor_Cisco_afw.compute…	compute1-211.mutate.com	10.1.0.49	
postprocessor_Cisco_afw.compute…	compute2-211.mutate.com	10.1.0.50	
postprocessor_Cisco_afw.compute…	compute3-211.mutate.com	10.1.0.48	
nirhealth_Cisco_afw.1	compute3-211.mutate.com	10.1.0.54	
utrftcorr_Cisco_afw.compute3-211.…	compute3-211.mutate.com	10.1.0.57	
utrftcorr_Cisco_afw.compute1-211.…	compute1-211.mutate.com	10.1.0.58	
utrftcorr_Cisco_afw.compute2-211.…	compute2-211.mutate.com	10.1.0.56	
sensei_Cisco_afw.1	compute3-211.mutate.com	10.1.0.76	
eventcollector_Cisco_afw.compute…	compute2-211.mutate.com	10.1.0.78	
eventcollector_Cisco_afw.compute…	compute3-211.mutate.com	10.1.0.79	
eventcollector_Cisco_afw.compute…	compute1-211.mutate.com	10.1.0.80	
tmniragent_Cisco_afw.1	compute1-211.mutate.com	10.1.0.84	
utrftcoll_Cisco_afw.2	compute2-211.mutate.com	10.1.0.87	9.1.1.2
utrftcoll_Cisco_afw.3	compute3-211.mutate.com	10.1.0.88	9.1.1.4
utrftcoll_Cisco_afw.1	compute1-211.mutate.com	10.1.0.86	9.1.1.3
apiserver_Cisco_afw.compute1-21…	compute1-211.mutate.com	10.1.0.92	
apiserver_Cisco_afw.compute2-21…	compute2-211.mutate.com	10.1.0.90	
apiserver_Cisco_afw.compute3-21…	compute3-211.mutate.com	10.1.0.91	
utrctfilter_Cisco_afw.1	compute2-211.mutate.com	10.1.0.96	
thirdpartycoll_Cisco_afw.1	compute3-211.mutate.com	10.1.0.102	
flowsink_Cisco_afw.compute2-211.…	compute2-211.mutate.com	10.1.0.105	
flowsink_Cisco_afw.compute1-211.…	compute1-211.mutate.com	10.1.0.104	
flowsink_Cisco_afw.compute3-211.…	compute3-211.mutate.com	10.1.0.106	
genie_Cisco_afw.compute1-211.m…	compute1-211.mutate.com	10.1.0.110	
genie_Cisco_afw.compute3-211.m…	compute3-211.mutate.com	10.1.0.112	
genie_Cisco_afw.compute2-211.m…	compute2-211.mutate.com	10.1.0.111	
utr_Cisco_afw.1	compute2-211.mutate.com	10.1.0.116	9.1.1.6
utr_Cisco_afw.2	compute1-211.mutate.com	10.1.0.117	9.1.1.5
utr_Cisco_afw.3	compute3-211.mutate.com	10.1.0.118	9.1.1.7

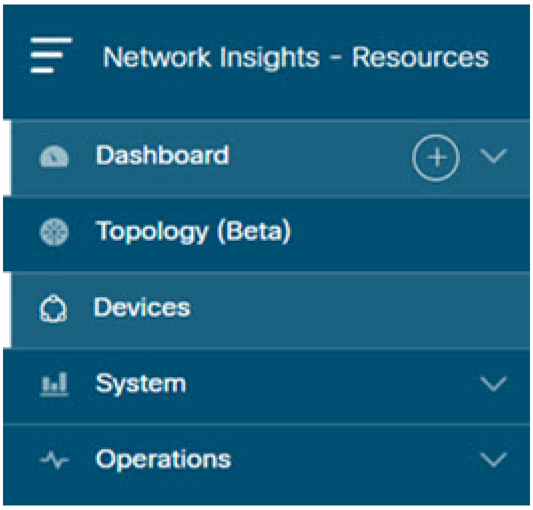
Cisco Network Insights for Resources Dashboard

Navigating Cisco NIR

The Cisco NIR app window is divided into two parts: the Navigation pane and the Work pane.

Navigation Pane

The Cisco NIR app navigation pane divides the collected data into four categories:



Dashboard: The main dashboard for the Cisco NIR app provides immediate access to site dashboard with anomalies.

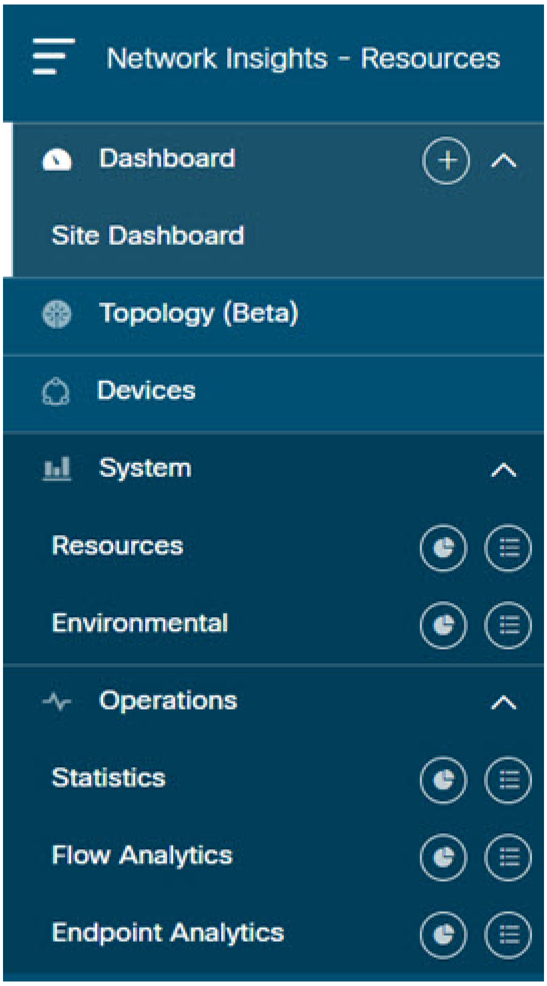
Topology: The topology view of the nodes connected to the Cisco DCNM site.

Devices: The detailed view of the nodes with a graphical representation of top nodes and top resources.

System: Resource and environmental utilization as well as software telemetry.

Operations: Statistics information for interfaces and protocols, flow analytics for viewing average latency, flow move indicator, and packet drops.

Expanding Dashboard, System, and Operations reveals additional functions:



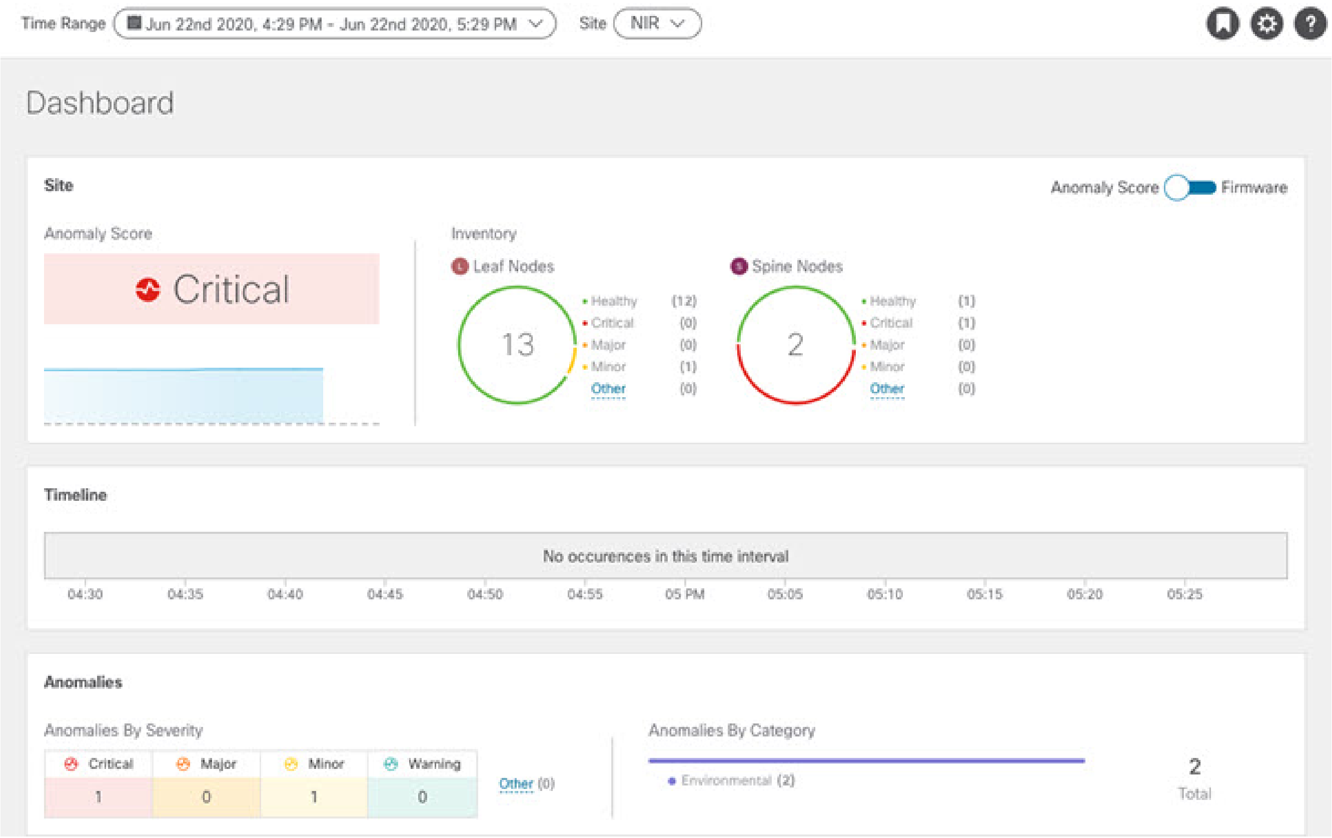
Dashboard View icon: Provides immediate access to top usage or issues for the selected telemetry type.

Browse View icon: Provides a detailed view of returned data for the selected telemetry type and allows for filtering to further isolate problem areas.

Work Pane

The work pane is the main viewing location in the Cisco NIR app. All information tiles, graphs, charts, and lists appear in the work pane.

Dashboard Work Pane

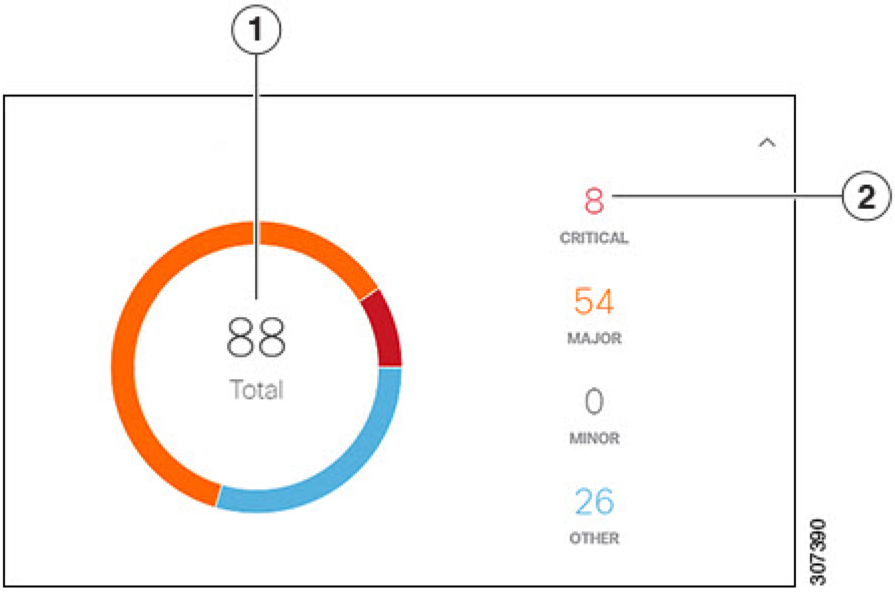


No occurences in this time interval

Critical	Major	Minor	Warning
1	0	1	0

Other (0)

In an information tile, you can usually click on a numeric value to switch to the Browse work pane:

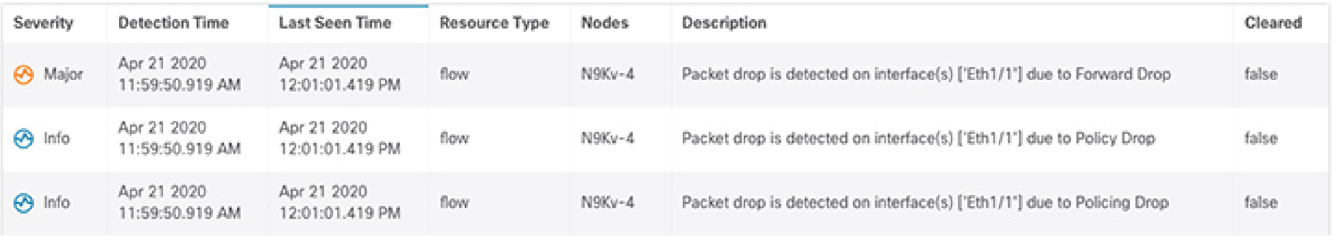


1 Launches the Browse work pane with all of the items displayed from the graph in the information tile.

2 Launches the Browse work pane with only the selected items displayed from the number in the information tile.

Browse Work Pane

The Browse work pane isolates the data for the parameter chosen on the Dashboard. The Browse work pane displays a top node lists, graphs over time, and lists all the nodes in an order defined by the anomaly score:



Severity	Detection Time	Last Seen Time	Resource Type	Nodes	Description	Cleared
Major	Apr 21 2020 11:59:50.919 AM	Apr 21 2020 12:01:01.419 PM	flow	N9Kv-4	Packet drop is detected on interface(s) ['Eth1/1'] due to Forward Drop	false
Info	Apr 21 2020 11:59:50.919 AM	Apr 21 2020 12:01:01.419 PM	flow	N9Kv-4	Packet drop is detected on interface(s) ['Eth1/1'] due to Policy Drop	false
Info	Apr 21 2020 11:59:50.919 AM	Apr 21 2020 12:01:01.419 PM	flow	N9Kv-4	Packet drop is detected on interface(s) ['Eth1/1'] due to Policing Drop	false

Clicking on one of the nodes in the list opens the Details work pane for that selection.

Details Work Pane

The Details work pane provides resource details about the item selected in the event list on the Browse work pane. The Details work pane consists of:

- General Information: Includes the anomaly score and the node name.
- Resource Trends: Includes operational resources, configuration resources, and hardware resources.
- Anomalies: Includes all anomalies for the node resource.

Top Navigation Pane

The Cisco NIR top navigation pane consists of the bookmark 🔖 icon. Any detailed view or page can be bookmarked and saved for later use. The bookmark saves the entire view, time range, nodes chosen, and creates a snapshot of the view. There is no limit for number of bookmarks added to the list.

Add a Bookmark

1. Click any detailed view from the left navigation pane, for example, Browse Resources, Browse Environmental, Browse Statistics, Dashboard view, or any specific view.
2. Click the bookmark icon on the top navigation pane.
3. The orange bookmark icon indicates that the selected detailed view is saved and added to the list of bookmarks. Bookmarks remember the original time range, start date and time, end date and time that the detailed view is created and saves the view or page to the list.

View a Bookmark

1. Click the bookmark icon on the top navigation pane.
2. Click any bookmark from the list to open the bookmarked page including the node view and selected time range. It helps you take a snapshot of detailed view pages for later use.

Delete a Bookmark

1. Click the bookmark icon on the top navigation pane.
2. Click the bookmarked page from the list to open the bookmarked page.
3. Unselect the bookmark icon.

Site Dashboard

Each node in the site streams telemetry data and events to a service in the Cisco NIR app. The Cisco NIR app analyzes the data and detects any anomalies. The Dashboards in the app provide relevant information to view.

The Cisco Network Insights for Resources (Cisco NIR) application main dashboard provides immediate access to anomalies occurring in the network. Anomalies are learned deviations from the last known "good" state of a switch and are displayed by type and severity. Anomalies include resource utilization, environmental, and interface-level errors, and are color coded based on severity:

- Critical: Red
- Major: Orange
- Minor: Yellow
- Warning: Turquoise
- Information: Blue
- Healthy: Green

In the Leaf Nodes and Spines blocks on the Dashboard, the large central number is the total count of those devices. The six colored icons at the bottom of the block are the six anomaly levels, and the small number below each icon is the count of devices at that anomaly level. The sum of these anomaly counters will be the same as the large total count.

Some factors that contribute to the presence of anomalies are exceeded thresholds and excessive rates of change.

Custom Dashboard

The custom dashboard lets you create a unique dashboard and add views on to the dashboard. This custom dashboard appears in the left navigation pane beneath the System Dashboard. In the work pane, the custom dashboard widget displays the top level information about each view pinned to the dashboard.

Create a Custom Dashboard

1. On the left navigation, click the + icon next to the **Dashboard** to create a custom dashboard.
2. Select a time range in the work pane.
3. Add a unique name in the text box. To edit the name, click the edit icon next to the name.

There is no limit for number of custom dashboards.

Add Views on to the Custom Dashboard

1. Click any detailed view from the left navigation pane, for example, resource detail, event detail, flow detail, dashboard view, or any specific view.

2. Click the pin icon on the right top navigation pane.
   - To pin to an existing custom dashboard, check the box for the existing dashboard.
   - Or, to create a new custom dashboard, click **Add**. Enter a unique name in the text box.
3. Click **Save**.

The custom dashboard appears on the left navigation beneath the **Site Dashboard**. There is no limit for number of views pinned to the dashboard.

View the Custom Dashboard

1. Click the custom dashboard from the left navigation pane.
2. Click any pinned view from the work pane.

Each view in the custom dashboard saves the entire snapshot of the page including the user selected time range for any specific node or nodes.

Delete Views from the Custom Dashboard

1. Click the custom dashboard from the left navigation pane. The custom dashboard widget displays the top level information about each view added.
2. Select any view in the work pane, click the pin icon for the selected view to delete or unpin the view from the custom dashboard.

Dashboard Inventory

Anomalies are raised when a certain parameter threshold exceeds, or a rate of change threshold exceeds. The main dashboard displays the following information.

Property	Description
Anomaly Score	Displays the health of the site through anomaly score.
Leaf	Displays the total number of leaf nodes in the site with anomalies.
Spine	Displays the total number of spine nodes in the site with anomalies.

- Toggle between **Anomaly Score** and **Firmware**. Each node type display anomaly breakdown based on the detected firmware versions instead of the breakdown by anomaly scores.
- Click **Anomaly Score** to view the details of the top nodes with anomaly score.
- Click **Spine** and **Leaf** to view the details of the individual nodes in the site from Browse Nodes work pane.

Site Dashboard Anomalies

The main dashboard displays the anomalies detected in the site nodes.

Property	Description
Anomalies by Category	Displays the number of Anomalies by their Category. Anomaly categories include: • Flows • Resources • Environmental • Statistics • Endpoints
Anomalies by Severity	Displays the number of Anomalies (internal site failures) and their severity level. Clicking on the area shows detail fault information, such as **Node** and **Anomaly Score**. • Critical • Major • Minor • Other

Click any number from Anomalies by Category and Anomalies by Severity to access the *Browse Anomalies* work pane.

Browse Anomalies

The Browse Anomalies pane displays the graph with top nodes by anomaly score based on Type and Severity. The page also displays the overview of the individual nodes in the site with severity, detection time, resource type, node name, cleared and other details.

- Double-click the anomaly for the anomaly details. The **Anomaly Details** page displays the general information of the anomaly, anomalies, list of paths, and related details.

On the **Anomaly Details** page for the selected node, click the ellipses ⋯ icon on the right top navigation pane for additional related information for the node such as, Flows, Statistics, Resources, Anomalies, and Environmental Resources.

From the ellipses menu click **Flows for the node** to open **Browse Flows** work pane, which filters the flows to view the top nodes by flow anomalies.

- Click **Statistics for the node** to open **Browse Statistics** pane, which filters the flows to view the top nodes by interface utilization.

Top Nodes by Anomalies

This section displays the overview of top nodes and their anomaly scores. The anomaly scores are based on the features that contribute to the anomaly. Click the node card headline for the *Node Details* page to display the general information, node overview, and a table of anomalies that apply to the nodes. The *Node Overview* section displays the features of the node such as Resource Utilization, Environmental, Statistics, Flow Analytics, and Event Analytics. Click each of these features to display specific information for the selected node.

Anomaly Score and Anomaly Precedence

The **Top Nodes by Anomalies** page summarizes anomalies based on the severity of the anomaly.

The following are examples of anomaly precedence for family of anomalies or individual anomalies based on the severity of the anomaly:

- A Leaf node has a critical anomaly and another Leaf node has nine major anomalies. In this case the Leaf node with nine major anomalies takes precedence over the Leaf node with a critical anomaly.
- A node has two critical and four major anomalies and another node has two critical and three major anomalies. It is almost always true that the node having less anomalies with high anomaly score gets precedence over node having more anomalies with less anomaly score.
- A node has one anomaly with score 91 and another node has nine anomalies with score 89 each. The node with nine anomalies that consumed 89 % is in worst case than the node with one anomaly that consumed 91%. In this case the node with nine anomalies gets the precedence.
- In case a Leaf node1 and a Leaf node2 have anomaly score more than a Leaf node4. The anomaly score for anomalies on Leaf node1 and Leaf node2 is 88, while both the anomalies on Leaf node4 have anomaly score 81, then the Leaf node with anomaly score 88 gets precedence.
    - Anomaly score for anomalies on Leaf node1 and Leaf node2 is 4^8.8 = 198668
    - Anomaly score for both the anomalies on Leaf node4 is 4^8.1 + 4^8.1 = 150562

Browse Anomaly Filters

The Cisco Network Insights for Resources, application dashboard provides immediate access to anomalies occurring in the network. View, sort, and filter anomalies through the Browse Anomalies work pane.

You can refine the displayed anomalies by the following filters:

- Detection Time - Display only anomalies with a specific detection time.
- Last Seen Time - Display only anomalies with a specific time.
- Description - Display only anomalies with a specified description.
- Cleared - Display only anomalies with cleared or uncleared status.
- Nodes - Display only anomalies for specific nodes.

- Category - Display only anomalies from a specific category.
- Resource Type - Display only anomalies of a specific resource type.
- Severity - Display only anomalies of a specific severity.

As a secondary filter refinement, use the following operators:

- `==` - 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.

Property	Description
Top Nodes by	Displays the top nodes by: • MAC (learned) • IPv4 (learned) • IPv6 (learned) • IPv4 Host Routes • IPv6 Host Routes • Multicast Routes • VLAN • VRF • Port Usage • Ingress Port Bandwidth • Egress Port Bandwidth • LPM

Property	Description
Operational Resources	Displays a list of operational resources based on resource utilization. List information includes: • Anomaly Score • Node • MAC (learned) • IPv4 (learned) • IPv6 (learned) • IPv4 Host Routes • IPv6 Host Routes • Multicast Routes
Configuration Resources	Displays a list of configuration resources based on resource utilization. List information includes: • Anomaly Score • Node • VRF • VTEP • VNI • VLAN
Hardware Resources	Displays a list of configuration resources based on resource utilization. List information includes: • Anomaly Score • Node • Port Usage • Port Bandwidth • LPM • Policy TCAM

Topology Dashboard

The Cisco Network Insights for Resources application dashboard provides access to the topology view of all the nodes with anomalies in the Cisco DCNM site.

Toggle Spine nodes, Leaf nodes, and Controllers to add or remove nodes from the topology view. Toggle each anomaly score to add or remove from the topology view.

View, sort, and filter anomalies through the topology work pane. You can refine the displayed nodes by the following filters:

- Name - Display only nodes with a specific name.
- VRF - Display only nodes from a specific VRF.
- IP - Display only nodes for a specific IP address.

Use the operators to filter the refinement.

The anomaly score is represented by the dot in the topology. The topology view helps find the nodes that are impacted by anomalies.

Click the node on the topology to view additional details for the node. The side panel displays general additional anomaly details for the node.

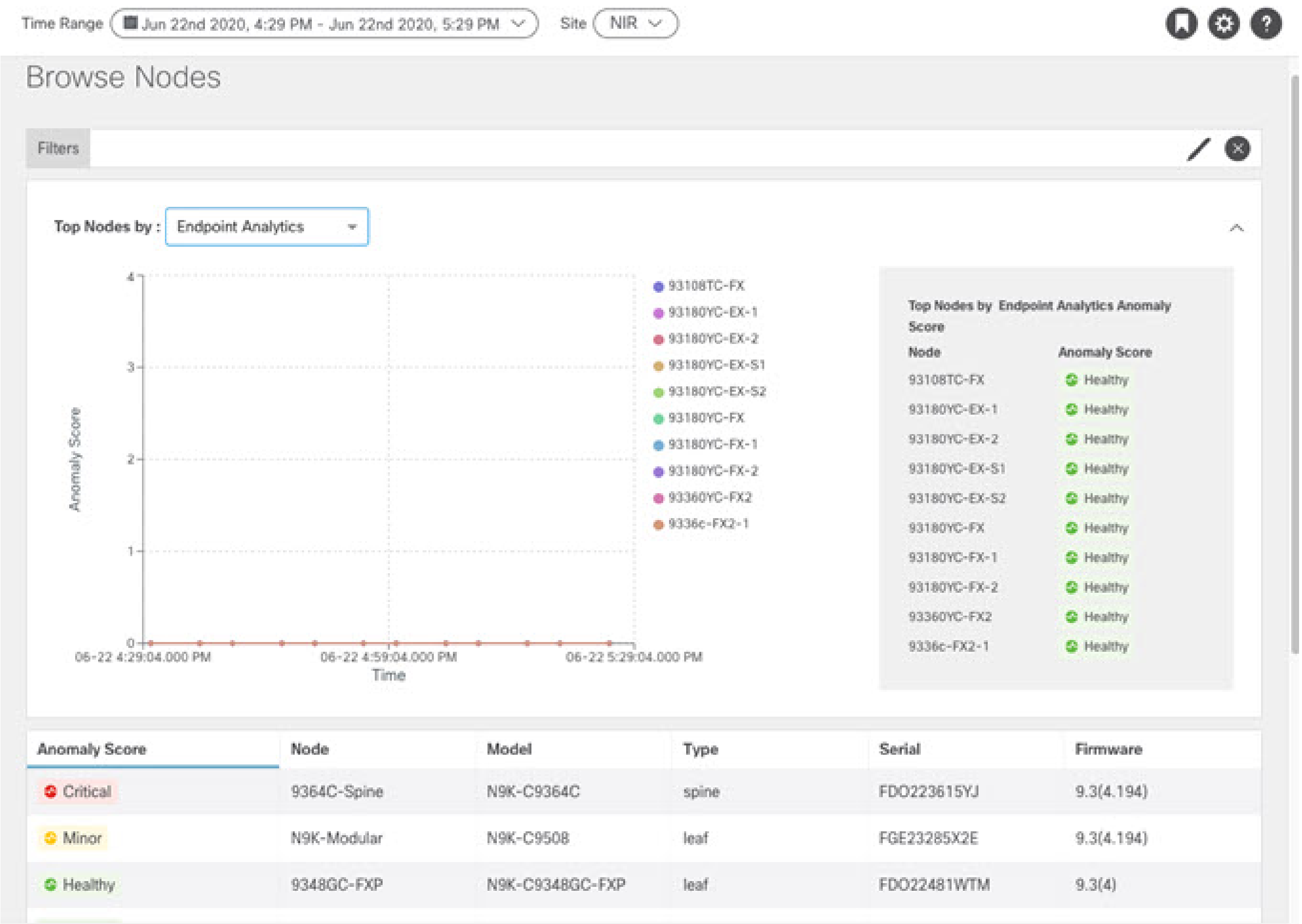
Topology Dashboard Limitations

- Topology view is available only for Spine and Leaf nodes.
- The topology view supports the nodes that are LLDP enabled.

Devices

Browse Nodes

The Browse Nodes pane displays the graph with top nodes based on Resource Utilization, Environmental, Statistics, End Point Analytics, and Flow Analytics, which are various ways of viewing the behavior of the nodes. The page also displays the overview of the individual nodes in the site with node name, switch models, node type and other details.



Time Range Jun 22nd 2020, 4:29 PM - Jun 22nd 2020, 5:29 PM Site NIR

Browse Nodes

Filters

Top Nodes by : Endpoint Analytics

Top Nodes by Endpoint Analytics Anomaly Score

Node	Anomaly Score
93108TC-FX	Healthy
93180YC-EX-1	Healthy
93180YC-EX-2	Healthy
93180YC-EX-S1	Healthy
93180YC-EX-S2	Healthy
93180YC-FX	Healthy
93180YC-FX-1	Healthy
93180YC-FX-2	Healthy
93360YC-FX2	Healthy
9336c-FX2-1	Healthy

Anomaly Score	Node	Model	Type	Serial	Firmware
Critical	9364C-Spine	N9K-C9364C	spine	FDO223615YJ	9.3(4.194)
Minor	N9K-Modular	N9K-C9508	leaf	FGE23285X2E	9.3(4.194)
Healthy	9348GC-FXP	N9K-C9348GC-FXP	leaf	FDO22481WTM	9.3(4)

- Click the *Node* for the node detail view. The *Node Overview* section displays the top five resources in Network Insights Analytics-Resource Utilization, Environmental, Statistics, and Flow Analytics with the break down of the faults and events. The *Anomalies* section displays the anomalies that the system detects.

The Browse Nodes pane displays the graph with top resources based on Resource Utilization, Environmental, Statistics, and Flow Analytics, which are various ways of viewing the behavior of the nodes. The page also displays the overview of the individual nodes in the site with node name, switch models, node type and other details.

- Click the *Node* for the node summary pane to display all the gathered information for the selected node.
- Click the ↗ on the right top corner of the summary pane to show the *Node Details* page.

The Node Details page displays General Information, Node Overview, and Anomalies. The *Node Overview* section displays the top five resources in Network Insights Analytics-Resource Utilization, Environmental, Statistics, and Flow Analytics with the break down of the faults and events. The *Anomalies* section displays the anomalies that the system detects.

On the detail page for the selected node, click the ellipses ⋯ icon on the right top navigation pane for additional related information for the node such as, Flows, Statistics, Resources, Anomalies, Environmental Resources, and node details.

- From the ellipses menu click **Flows for the node** to open Browse Flow Records work pane, which filters the flows to view the top nodes by flow anomalies.
- Click **Statistics for the node** to open Browse Statistics work pane, which filters the flows to view the top nodes by interface utilization.

Cisco Network Insights for Resources System

Cisco NIR System

The System section of the NIR application contains two areas of data collection:

- **Resource Utilization** —Site component capacity information.
- **Environmental** —Hardware component capacity information.

System Resource Utilization

The System Resources of the Cisco NIR application contains two areas of data collection.

Resource Utilization Dashboard

The Resource Utilization dashboard displays utilization, rate of change, trends, and resource anomalies over time for operational, configuration and hardware resources. Top leaf nodes and spine nodes are displayed based on the factors that produced the high utilization.

Property	Description
Top Nodes by Capacity	The leaf node observations search can be more refined by filtering the information by the top leaf nodes.
Node Details	Displays the node trend observations by resource type: • Operational Resources • Configuration Resources • Hardware Resources

Guidelines and Limitations

- The Hardware Resources tab in System Resource Utilization Dashboard is not supported for Cisco Nexus 7000 series switches. The hardware resources do not have a direct mapping to the objects that show in Cisco NIR app. The command that shows hardware details does not provide the percentage of entries used and the maximum number of entries allocated for a particular feature. The Cisco NIR app raises the anomalies and details page for any resource in Hardware Resources tab for Cisco Nexus 7000 series switches.

Browse Resource Utilization

View, sort, and filter statistics through the Browse Resource Utilization work pane.

Resource Utilization Filters

You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

As a secondary filter refinement, use the following operators:

- `==` - 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.

Property	Description
Top Nodes by	Displays the top nodes by: • MAC • IPv4 Host Routes • IPv6 Host Routes • IPv4 Prefix Routes • IPv6 Prefix Routes • Multicast Routes • VLAN • VRF • Port Usage • Ingress Port Bandwidth • Egress Port Bandwidth • CoPP • LPM • HRT • L2 QoS TCAM • L3 QoS TCAM • VTEP • VNI L2 • VNI L3 • VLAN • Ingress VLAN ACL • Egress VLAN ACL • Ingress Port ACL • Ingress Routed ACL • Egress Routed ACL

Property	Description
Operational Resources	Displays a list of operational resources based on anomaly score. List information includes: • Anomaly Score • Node • MAC • IPv4 Host Routes • IPv6 Host Routes • IPv4 Prefix Routes • IPv6 Prefix Routes • Multicast Routes
Configuration Resources	Displays a list of configuration resources based on anomaly score. List information includes: • Anomaly Score • Node • VLAN • VTEP • VNI ◦ L2 ◦ L3 • VRF

Property	Description
Hardware Resources	Displays a list of configuration resources based on anomaly score. List information includes: • Anomaly Score • Node • Port Usage • Port Bandwidth • CoPP • LPM • HRT • QoS TCAM ◦ L2 ◦ L3 • VLAN ACL ◦ Ingress ◦ Egress • Port ACL ◦ Ingress • Routed ACL ◦ Ingress ◦ Egress

System Environmental

The System Environmental of the Cisco NIR application contains two areas of data collection.

Environmental Dashboard

The Environmental Dashboard displays utilization, rate of change, trends, and anomalies over time for switch environmental resources such as fans, power, CPU, and memory.

Property	Description
Top Nodes by Utilization	Displays the percentage utilized per component: • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage
Node Details	Displays the node trend observations by environmental resource type.

Browse Environmental Resources

View, sort, and filter statistics through the Browse Environmental Resources work pane.

Environmental Filters

You can refine the displayed statistics by the following filters:

- * Node - Display only nodes.

As a secondary filter refinement, use the following operators:

- `==` - 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.

Property	Description
Top Nodes by	Displays the top nodes by: • CPU (percent utilization) • Memory (percent utilization) • Temperature • Fan Utilization • Power Supply • Storage

Cisco Network Insights for Resources Operations

Cisco NIR Operations

The Operations section of the Cisco NIR application contains two areas of statistical and analytical information:

- **Statistics Analytics** —Switch nodes interface usage and protocol statistics.
- **Flow Analytics** —Telemetry information collected from various devices in the Cisco ACI site to the NX-OS sites.

Statistics Analytics

The Operations Statistics section of the Cisco NIR application contains interface and protocol statistical information for top switch nodes.

Statistics Dashboard

The Statistics Dashboard displays top switch nodes by interface errors or usage, and protocol statistics.

Property	Description
Top Nodes by Interface Utilization	Displays the top nodes based on the combined bandwidth utilization of it’s interfaces.
Top Nodes by Interfaces	Displays the top nodes and lists the transmit and receive bandwidth utilization of each of it’s interfaces.

In the **Top Nodes by Interfaces** click the node card to display the Interface Details page.

Interface Details

Click the node card in the **Top Nodes by Interfaces** to display the node interface details. The details include anomaly score, node, interface, type, operation status, summary of anomalies, trends, errors, configured protocols, DOM statistics, and microbursts.

The Anomalies section summarizes the anomaly detection details. The path summary section describes the source IP and destination IP address for the node with anomaly.

The trends section displays the network traffic trend over time for packets received, packets transmitted, bytes received, bytes transmitted, utilization rate, and errors. The charts in this section interprets network traffic behavior, peaks, and patterns over time.

The configured protocols section displays the interface protocols that are enabled and disabled with trends and errors.

The statistics section displays the DOM properties of the physical interface for the node.

The microbursts section displays the top microburst detected in the node by peak value and duration.

Browse Statistics Filters

Browse Statistics filters the interfaces to visualize the top interfaces by anomalies through the Browse Statistics work pane.

You can view, sort, and filter statistics through the Browse Statistics work pane. You can refine the displayed statistics by using the following filters:

- Node - Display only nodes.
- Interface - Display only interfaces.
- Interface Type - Display only specific interface types.
- Protocol - Display only protocols.
- Operational State - Display nodes with specific operational state.
- Admin State - Display nodes with specific admin status.

As a secondary filter refinement, use the following operators:

- `==` - 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.

Property	Description
Top 10 Interfaces by	Displays the top interfaces by: • Transmit Utilization • Receive Utilization • Error

Property	Description
Interface Statistics	Displays a list of interface statistics based on anomaly score. List information includes: • Anomaly Score • Interface • Interface Type • Node • Receive Utilization • Transmit Utilization • Errors
Protocol Statistics	Displays a list of protocol statistics based on anomaly score. List information includes: • Anomaly Score • Protocol • Node • Count • Errors

In order for the Cisco NIR app to receive data from the nodes, confirm that all the nodes in the site are synced with PTP Grand master for hardware telemetry and NTP clock for software telemetry.

Browse Statistics

The Browse Statistics dashboard displays interface statistics and protocol statistics for the top interfaces by anomalies for nodes.

Interface Statistics

The Browse Statistics dashboard displays interface statistics for the top interfaces by anomalies for nodes that are of type - physical, port channel, and virtual port channel (PC and vPC) interfaces.

The green dot next to the interface name represents the operational status that the interface is active. The red dot next to the interface name represents that the interface is down.

The interface type is physical, port channel, or virtual port channel (PC or vPC) interface.

- Double-click each row in the **Interface Statistics** page to display the interface detail page. This page summarizes node name, physical interface name, operational status, and admin state. The page also displays protocols, QoS, and DOM properties of the physical interface.

The port channel is an aggregate of physical interfaces and they can be statically channeled or can be dynamic using LACP protocols. The statistical data that is collected such as number of packets, bytes, and various errors are similar to that of physical interfaces. The *sourcename* differentiates the physical interface from port-channel (aggregated interfaces). The operational data is obtained by looking at additional set of objects that gives the admin-status, oper-status and list of member interfaces for both PC and vPC.

- Click a row in the **Interface Statistics** page for the side pane to display additional details of the node such as, node name, port channel name, operational status, and admin state. The page also displays the anomalies, traffic, and member interfaces associated in the port channel.

The vPC is a logical interface that spans across two physical switches for fault tolerance. Double-click each row in the **Interface Statistics** page, to display the interface detail page. This page summarizes node name, virtual port channel name, domain id, operational status, and admin state. The page also displays the anomalies, traffic, and the member interfaces associated in the nodes that are in the virtual port channel.

Micro-Burst Support for Interface Statistics

A burst of traffic impacts the output buffer of a physical interface port given the channel is already subscribed with line-rate flows.

These bursts are often hard to detect with just given queuing parameters, such as buffer cells used and buffer cells unused as there is a high variance of usage of these buffers.

The Cisco Nexus 9000 series switches provide a capability of detecting this by issuing an interrupt that is triggered when a queue occupancy rises above *x* bytes and falls below *y* bytes. This *x _& _y* bytes are configurable per queue per interface. You can configure up to 8 output queues per physical interface port.

When the UTR software collector receives a GRPC telemetry stream for the path `show queuing burst-detect detail`, according to the parser for the encoding path, data is formatted, and it's written to the telemetry output topic of Kafka.

Configuring and Monitoring Micro-Burst

See Micro-Burst Monitoring for details.

Supported Platforms

See Supported Platforms for details.

Micro-Burst Anomaly

Anomalies are raised in Cisco NIR app based on the number of micro-bursts at the interface level. Micro-burst anomaly jobs run every 5 minutes in a container environment, which checks for micro-burst records in micro-burst database. If the number of micro-bursts per interface is greater than `microburst count threshold` at any given point of time, then a minor anomaly is raised per interface in a node. At that point any anomaly record is written to Elasticsearch.

The Cisco NIR app raises these anomalies in the **Cisco NIR Operations** > **Interface Statistics** tab.

Protocol Statistics

The Browse Statistics dashboard displays protocol statistics for the top interfaces by anomalies for nodes that are of type CDP, LLDP, LACP, BGP. This page also displays node name and *Count* - the number of interfaces that the protocol is using or the number of sessions that the protocol is using for the node.

The BGP protocol data can be classified broadly into operational and statistical data. The operational data comprises of additional set of objects that gives the admin-status, oper-status and list of VRFs and VRF level information such as vrfName, vrfOperState, vrfRouteId, list of address family associated with each VRF, and list of peer and peer-entry information associated with each VRF. The statistical data comprises of peer-entry counters such as number of open's, updates, keepalives, route-refresh, capability, messages, notifications and bytes sent and received. It also includes peer-entry address family level the route count.

- Click a row on the Protocol Statistics summary page for the side pane to display additional details.
- Double-click a row with the protocol **BGP** for protocol details of the node such as, node name, protocol name, admin state, operational state and additional details. This page also displays the anomalies, neighbor nodes that are active, errors in the node, neighbor IP address, details about the established neighbors and not connected neighbors that the BGP protocol is using from the node family.
- Double-click a row with the protocol **CDP** , **LLDP** , or **LACP** for protocol details of the node such as, node name, protocol name, anomalies, interfaces that are active, errors in the node, and more details of the interface.

Multicast Protocol Statistics

The Browse Statistics dashboard displays protocol statistics for the top interfaces by anomalies for nodes that are of type PIM, IGMP, and IGMP Snoop protocol.

Internet Group Management Protocol

Use filters from browse statistics page to display the summary of a specific node for IGMP interface. The **General Information** section displays the anomaly score, node name, protocol, number of interfaces enabled for a specific node, and number of groups enabled on the interface. On Cisco DCNM the IGMP groups can be enabled on VLAN and can also be enabled on the interface.

The **Anomalies** section displays the anomalies that are generated on a node specific to IGMP.

The **Configured IGMP Interfaces** section displays the interfaces that are enabled with IGMP. It displays the interface name, VRF, IP address, IGMP querier, membership count, version, and errors.

The IGMP interfaces can be configured in 3 methods on the specific node. These are not configurable from Cisco NIR app.

- Enable PIM in the interface.
- Statistically bind the interface to a protocol.
- Enable link reports.
- Double-click a row for the side pane to display additional interface details. This includes groups enable status, statistical data about error counters, flags that are enabled on IGMP, and other properties that are specific to the node.

The **Multicast Groups** section displays the IGMP groups related details such as source, multicast group, VRF, version, last reporter, and outgoing interface specific to the IGMP group. It is possible to have multiple outgoing interfaces.

Internet Group Management Protocol Snoop

Use filters from browse statistics page to display the summary of a specific node for IGMP Snoop. In the VLAN the IGMP is enabled by default, where the IGMP snoops on VLAN for information. The **General Information** section displays the anomaly score, protocol, node name, number of groups, and number of instances where IGMP Snoop is enabled on the instances per VLAN.

The **Anomalies** section displays the anomalies that are present in the node specific to IGMP Snoop instance.

The **Trends** section displays the number of instances and break down of errors related to IGMP Snoop for a specific node. The number of instances are any number of bridge domains, where some are IGMP Snoop enabled and some are IGMP Snoop disabled. * The **Up** represents the instance count that are IGMP Snoop enabled. * The **Down** represents the instance count that are IGMP Snoop disabled.

The **IGMP Snoop Instances** section displays information per VLAN. This includes VLAN, admin state, querier address, querier version, multicast routing state (enabled or disabled), node querier state (enabled or disabled), and summary of errors.

- Double-click a row for the side pane to display other configured details specific to IGMP Snoop instance. This includes VLAN name, VLAN ID, properties that are enabled or disabled, statistical details and various error counters specific to the IGMP Snoop instance.

The **Multicast Group** section displays details such as source, multicast group, VLAN, version, last reporter, and outgoing interfaces for each IGMP Snoop group.

Protocol Independent Multicast

Double-click the protocol type **PIM** to display the summary of a specific node for PIM.

The **General Information** section displays the anomaly score, node name, protocol, number of domains, number of interfaces, and number of groups for the protocol.

The **Anomalies** section displays the anomalies that are generated on a node specific to the PIM.

The **Trends** section displays the errors and break down of errors related to PIM for a specific node.

The **Multicast PIM Domains** section displays the domain details for PIM specific to the node. It displays the basic information such as tenant, VRF, admin state where VRF is enabled or disabled, and rendezvous point addresses.

- Double-click a row for the side pane to display additional details about the specific multicast PIM domain. This includes VNI IDs, flags that are enabled, various errors and statistics information.
- Click on rendezvous point address, for example *1*, which displays a side pane with IP address details. This includes the group range the rendezvous point address refers to, lists the group range for a particular rendezvous address.

The **Multicast PIM Interfaces** section displays the summary table with interfaces that are enabled with PIM. It displays the VRF, IP address, designated router address, neighbor addresses, and errors for a specific PIM interface.

- Double-click a row for the side pane to display neighbor specific details. This includes statistics information for the neighbor, flags that are enabled with in the neighbor, and errors that are specific to the node.

The **Multicast PIM Groups** section summarizes the PIM group related details such as RPF source, RPF neighbors, VRF, group address, incoming interfaces, and flags that are enabled for the PIM group.

Multicast Protocol Statistics Analytics Limitations

- The PIM, IGMP, and IGMP Snoop multicast statistics protocols are supported only on Cisco Nexus 9000 series switches.
- The PIM, IGMP, and IGMP Snoop multicast statistics protocols are not supported for the following:
  - Cisco Nexus 7000 and 3000 series switches.
  - Cisco N9K-X9636C-R, N9K-X9636Q-R, N9K-X96136YC-R, and N3K-C3636C-R line cards.
- When Cisco NIR app programs these devices in Managed mode it avoids enabling the NXAPI export for the unsupported devices. When the fabric is in Monitored mode, the generated configuration avoids the NXAPI commands for the unsupported devices. If you configure these exports manually using direct switch configuration and if the data for these features comes from the unsupported devices, the multicast statistical data may be shown in the Cisco NIR app UI.
- The total multicast routes (S, G, and *G together) supported per device is 8000 and per fabric is 64000.

Protocol Statistics Analytics Limitations

- The CDP protocol statistics is not supported for Cisco Nexus 7000 series switches.
- Cisco NIR app does not support BGP `PrefixSaved` statistics on the following:
  - Cisco Nexus 3000, 7000, and 9000 series switches.

    - Cisco N9K-X96136YC-R, N9K-X9636C-R, N9K-X9636Q-R, and N3K-C3636C-R line cards.

Flow Analytics

The Flow Analytics section of the Cisco NIR application displays the anomalies detected in the flow such as average latency, packet drop indication, and flow move indication collected from various nodes in the site.

Flow Analytics Overview

Flow Analytics provides deep insights at a flow level giving details such as average latency, packet drop indicator and flow move indicator. It also raises anomalies when the latency of the flows increase or when packets get dropped because of congestion or forwarding errors.

Each flow has a packet counter representing the number of packets entering the ASIC for that flow over a period of time. This period of time is called aggregation interval. There are several points where flow statistics for a given flow can be aggregated. Aggregation can happen in the ASIC, switch software, and server software.

Flow Analytics Hardware Requirements

For details on Flow Telemetry support for Cisco Nexus platform switches, see Cisco NIR Release Notes Compatibility Information section.

Flow Analytics Limitations

The following are limitations for Flow Analytics for Cisco NIR application on Cisco Nexus EX line cards. For details on Flow Telemetry hardware support, see Cisco NIR Release Notes Compatibility Information section.

- Output port information for outgoing traffic from N9K-C93180YC-EX, N9K-C93108TC-EX, and N9K-C93180LC-EX line cards will not be displayed.
- Flow analytics does not support multicast traffic. The access list must be provisioned to exclude the multicast traffic flows.
- The number of anomalies in the **Site Dashboard** will not match the number of anomalies in the flow browse page. The Site Dashboard contains the total anomaly count for the time range you selected. The flow records are not aggregated in the flow browse view, where multiple flow records can point to the same anomaly entry.
- The L3-VNI flows show as L2-VNI flows when the VXLAN flow is dropped in the ingress node. When VXLAN packets are dropped in the first-hop, the exported VXLAN flow telemetry records will indicate the drop. However, they don’t carry the VNI information in it. The Ingress interface from the flow telemetry export along with the VRF associated with the interface, does not deduce if the flow is L2-VNI or L3-VNI. In this case Cisco NIR app associates the L2-VNI for the flow.
- When there are 29 million anomalies in the indices, flow database writes are too slow, which

causes KAFKA lag on 350 nodes supported for software telemetry and flow telemetry. The KAFKA lag results in partial data in Cisco NIR app user interface.

- Flow Analytics information is retained for 7 days or until flow database reaches 80%, which ever happens first, then older flow analytics information is deleted from the database.

Flow Analytics Dashboard

The Flow Analytics Dashboard displays telemetry information collected from various devices in the site. The flow analytics records let the user visualize the flows in the site and their characteristics across the entire Cisco DCNM site.

Property	Description
Top Nodes by	The flow analytics engine also runs machine-learning algorithms on the behavior of the flows to raise anomalies in the behavior, such as Average Latency, Packet Drop Indicator, and Flow Move Indicator. The graph represents the anomalies in the behavior over a period of time.
Top Nodes by Flow Anomalies	Flow telemetry and analytics gives in-depth visibility of the data plane. The flow analytics engine collects the flow records streamed from the nodes and converts to understandable flow records. Top nodes by flow anomalies displays the nodes in the network with the most anomalies.

In the **Top Nodes by Flow Anomalies** click the node card to display the Flow Records page.

Flow Record Details

Click the node card in the **Top Nodes by Flow Anomalies** to display the flow record details. The details include anomaly score, record time, flow type, aggregated flow information, summary of anomalies, path summary, and charts for flow properties.

The aggregated flow section displays in-depth analysis of flow anomalies including source, destination, Ingress, and Egress details.

The Anomalies section summarizes the anomaly detection details. The path summary section describes the source IP and destination IP address for the node with anomaly.

The related details section displays anomaly analysis with the comparison charts for each flow property against time.

Browse Flow Records

The Browse Flow Records page displays the active nodes, ingress nodes, egress nodes, and flow collection filters, which display the anomalies in the site nodes.

The Browse Flow Records page displays Site flows by Anomaly Score, Packet Drop Indicator, Average Latency, and Flow Move Indicator.

Property	Description
Nodes	Shows all the nodes where the flows are reported.
Filters	Display the node flow observations sorted by the following filters: • Record Time • Nodes • Flow Type • Protocol • Source Address • Source Port • Destination Address • Destination Port • Ingress Node • Ingress VRF • Source VNI • Egress Node • Egress VRF • Destination VNI
Site Flows by	A time series plot for flow analytics properties such as anomaly score, average latency, packet drop indicator, and flow move indicator that are recorded in the entire site for the time interval you selected. The node flows recorded for **Top Sources** and **Top Destinations** are also shown.

Property	Description
Top Flows	Lists the top flows in the entire site that scored highest in the following: • **Anomaly Score**—The score is based on the number of detected anomalies logged in the database. • **Record Time**—The node flows are captured at individual record times between the start and end time that you selected. Flow analytics records multiple entries for a flow that are captured at individual record times. • **Packet Drop Indicator**—The flow records are analyzed for drops. The primary method of detecting drops is to check for discrepancies in the ingress and egress packet counts. • **Latency**—The time taken by a packet to traverse from source to destination in the site. A prerequisite for site latency measurement is that all the nodes shall be synchronized with uniform time. • **Flow Move Indicator**—The number of times a Flow moves from one leaf node to another. The first ARP/RARP or regular packet sent by that endpoint appears as a flow entering the site through the new leaf node.

Double click the flow for additional details. The **Flow Details** page displays the general information of the flow, anomalies, path summary, charts, and related details.

Endpoint Analytics

The Endpoint Analytics section of the Cisco NIR application contains endpoint information, charts, and history for the nodes with endpoint anomalies collected across the entire Cisco DCNM site.

Endpoint Analytics Overview

Endpoint Analytics provides detailed analytics of endpoints learnt in the site with the following information:

- The endpoints present on the leaf switches - browse endpoint analytics using filter options, such as IP address, MAC address, node, entity name and so on.
- The endpoints in the site at a particular time - view the endpoint history.

- The endpoint information for compute administrator - view the endpoint placement information and correlation to virtual machine and hypervisor.
- The policies applied on an endpoint - view the discover configuration and operational information of the endpoint.

The following anomalies are detected as part of endpoint analytics:

- The rapid endpoint moves across nodes, interface, and endpoint groups.
- Detect endpoints that have duplicate IP address.

Endpoint Analytics Dashboard

The Endpoint Analytics Dashboard displays time series information for the top nodes with number of endpoints that are varying. The Endpoint Analytics provides detailed analytics of endpoints learnt in the site.

Property	Description
Top Nodes by Number of Endpoints	Displays the top nodes based on the number of active endpoints.
Top Nodes by Endpoint Anomalies	Displays the nodes in the network with the most endpoint anomalies.

In the **Top Nodes by Endpoint Anomalies** click the node card to display the *Endpoint Details* page.

Browse Endpoint Analytics

Browse Endpoint Analytics displays the graph with top 5 endpoints by anomaly score over a period of time.

You can view, sort, and filter endpoints through the work pane. You can refine the displayed endpoints by the following filters:

- VRF - Displays nodes with IP address.
- BD - Displays nodes with domain id.
- MAC Address - Display nodes with MAC address.
- Nodes - Display only nodes.
- Interface - Display only interfaces.
- IP address - Display nodes with IP address.
- Encap - Displays nodes with specific encapsulation.
- Status - Display nodes with the status.
- Time - Display endpoints that had the last update happened at this time.

The filter refinement lets you select the filter, operator, and value. You can use the following operators:

`==` - with the initial filter type, this operator, and a subsequent value, returns an exact match.

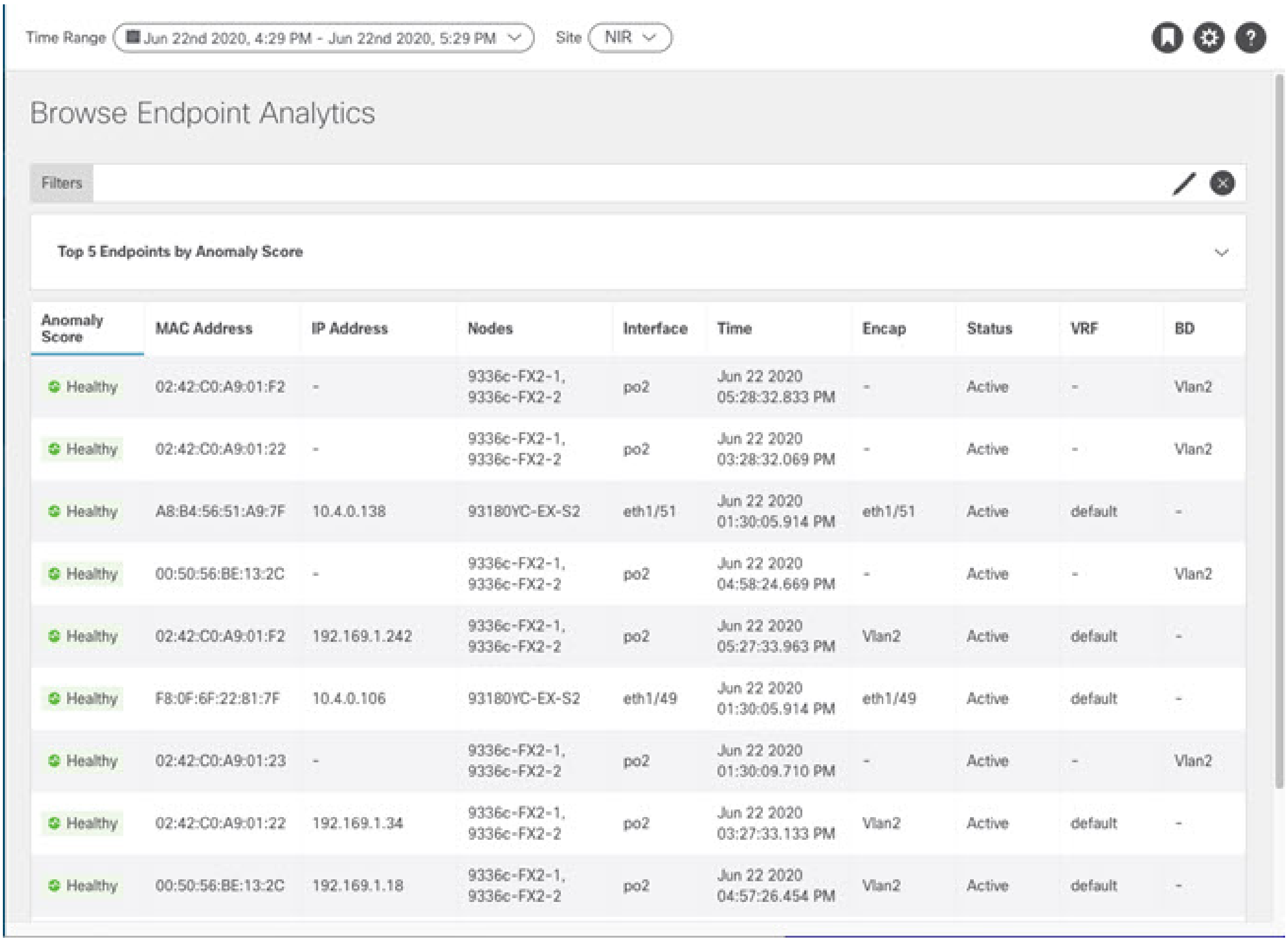
`!=` - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.

`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.

Endpoint Analytics Summary

The Browse Endpoint Analytics page summarizes the endpoints that are sorted by anomaly score.



Time Range: Jun 22nd 2020, 4:29 PM - Jun 22nd 2020, 5:29 PM
Site: NIR

Browse Endpoint Analytics

Filters

Top 5 Endpoints by Anomaly Score

Anomaly Score	MAC Address	IP Address	Nodes	Interface	Time	Encap	Status	VRF	BD
Healthy	02:42:C0:A9:01:F2	-	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 05:28:32.833 PM	-	Active	-	Vlan2
Healthy	02:42:C0:A9:01:22	-	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 03:28:32.069 PM	-	Active	-	Vlan2
Healthy	A8:B4:56:51:A9:7F	10.4.0.138	93180YC-EX-S2	eth1/51	Jun 22 2020 01:30:05.914 PM	eth1/51	Active	default	-
Healthy	00:50:56:BE:13:2C	-	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 04:58:24.669 PM	-	Active	-	Vlan2
Healthy	02:42:C0:A9:01:F2	192.169.1.242	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 05:27:33.963 PM	Vlan2	Active	default	-
Healthy	F8:0F:6F:22:81:7F	10.4.0.106	93180YC-EX-S2	eth1/49	Jun 22 2020 01:30:05.914 PM	eth1/49	Active	default	-
Healthy	02:42:C0:A9:01:23	-	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 01:30:09.710 PM	-	Active	-	Vlan2
Healthy	02:42:C0:A9:01:22	192.169.1.34	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 03:27:33.133 PM	Vlan2	Active	default	-
Healthy	00:50:56:BE:13:2C	192.169.1.18	9336c-FX2-1, 9336c-FX2-2	po2	Jun 22 2020 04:57:26.454 PM	Vlan2	Active	default	-

Click an endpoint in the summary table for the side pane to display configuration, operational, endpoint status, and additional details about the anomaly.

Click the ☐ icon on the right top corner of the side pane to display the *Endpoint Details* page.

Double-click the endpoint anomaly in the table to display the *Endpoint Details* page. The *Endpoint Details* page describes general information about the endpoint based on configuration and operation of the endpoint. The configuration section displays the MAC address, BD, VRF, and Encap details for the selected endpoint. The operational section displays the Node name, Interface, VM id, hypervisor id, and other details.

The following anomalies are detected as part of endpoint analytics:

- The rapid endpoint moves across nodes, interface, and endpoint groups.
- Detect endpoints that have duplicate IP address.

This page also lists the *Anomalies*, *Endpoint History*, *Duplicate Endpoints*. The *Anomalies* section displays the anomalies for the selected endpoint.

The *Endpoint History* lists in decrease order of when the endpoint was updated. It lists the endpoints moving over a period of time between interfaces and across the nodes. Hovering over the highlighted value shows the change for that value. Hovering over Changes column shows all changes.

The L2 endpoints have VLAN information while L3 endpoints have VRF information.

The *Duplicates* section lists duplicate IP addresses attached to the endpoint. Duplicate IP address occurs when two different nodes with the same IP address are attached to an endpoint in certain period of time.

Supporting Third-Party Nodes for Cisco NIR Application

About Third-Party Nodes Support for Cisco NIR Application

The Cisco Network Insights for Resources app in Cisco DCNM provides a way to gather data from third-party nodes through Cisco NIR application. The data is acquired through the third-party collector service using REST based EAPI method calls provided by the collector service.

The following telemetry information is collected from third-party nodes in the site:

- Environmental Statistics—This includes monitoring environmental statistics such as CPU, memory, fan, temperature, and power usage, and storage details of the site nodes.
- Interface Statistics—This includes monitoring of nodes, interfaces, and protocol statistics on Cisco DCNM and site nodes using LLDP and LACP.
- Resource Statistics—This includes monitoring software and hardware resources of site nodes on Cisco DCNM using IPv4 unicast, IPv4 multicast, and MAC.

Third-Party Hardware Support for Cisco DCNM

The Cisco NIR app in Cisco DCNM supports Arista 7050SX and 7280SR platform switches.

Third-Party Nodes Limitations for Cisco NIR Application

The following are limitations for third-party nodes for Cisco NIR application.

- The Interface Statistics for LLDP and LACP do not support *Flap Count*, *Entries Aged Count*, and *PDU Timeout Count*.
- The Interface Statistics for MAC do not support local and static endpoints.
- Third-party nodes are discovered in a separate fabric.
- Third-party nodes are supported only on Monitored mode.
- Third-party nodes are accessible in non-privileged mode for data to be streamed.

Enabling Third-Party Nodes for Data Collection

Adding or removing the third-party nodes from the site will generate a control message, which triggers the third-party collector service present in the UTR pipeline to start or stop collecting data from the specific node.

To discover and enable third-party nodes to Cisco DCNM site:

- Create an external site to discover the third-party nodes, refer to Creating an External Fabric for details.
- To discover the third-party nodes, refer to Discovering New Switches for details.
- Add the third-party nodes to the external site, see Adding non-Nexus Devices to External Fabrics for details.

Configuring Third-Party Nodes in Cisco DCNM

Before you begin adding the third-party nodes to the site on Cisco DCNM, make sure the following requirement is met:

- You must have administrator credentials for doing the third-party node discovery.

Most of the Interface Statistics data is obtained with out any specific configuration for the third-party nodes. The following configuration is required for collecting port channel and storage statistics.

1. Setup the port channel for LACP. See Port Channel Configuration Procedures for details.
2. Execute the `aaa authorization exec default local` CLI command to collect storage statistics.

Cisco NIR DCNM REST API Examples

all_resources()

Get all the resources.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/utilization/resources.json
Parameters :
   None
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/utilization/resources.json'
Response   :
   {
       "totalResultsCount": 5,
       "totalItemsCount":5,
       "entries": [
           {
               "categoryName": "",
               "resourceName": "EndPoints",
           }
           <-- SNIP LIST OF ALL OTHER RESOURCES -->
           {
           }
       ]
   }
```

anomalies_details()

Get the anomalies in the system.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/anomalies/details.json
Parameters :
   startTs  (optional) => Start timestamp, default:now-1h
   endTs    (optional) => End timestamp, default:current-time
   count    (optional) => Num.of nodes in response, default:10
   orderBy  (optional) => Sort per the given field
Example :
    curl -ksb -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/anomalies/details.json'
Response :
    {
        "totalItemsCount": 90,
        "totalResultsCount": 90,
        "offset": 0,
        "entries": [
            {
                "anomalyId": "QUE000000000018",
                "category": "System Resource",
                "startTs": "2018-09-19T16:45:05.679Z",
                "endTs": "2018-09-19T16:58:05.778Z",
                "entityName": "svc_ifc_policyelem",
                "severity": "critical",
                "anomalyType": "build-up",
                "nodeNames": [
                    "leaf2"
                ],
                "resourceType": "queue",
                "resourceName": "recvQ",
                "anomalyStr": "[svc_ifc_policyelem] : Unexpected build-up of 7487
message[s] in recvQ",
                "anomalyScore": 83
            },
            {
                "anomalyId": "QUE000000000007",
                "category": "System Resource",
                "startTs": "2018-09-19T15:16:10.420Z",
                "endTs": "2018-09-19T16:49:01.289Z",
                "entityName": "svc_ifc_policyelem",
                "severity": "critical",
                "anomalyType": "build-up",
                "nodeNames": [
                "leaf1"
                ],
                "resourceType": "queue",
                "resourceName": "recvQ",
                "anomalyStr": "[svc_ifc_policyelem] : Unexpected build-up of 7502
message[s] in recvQ",
                "anomalyScore": 83
            }
        ]
    }
```

anomalies_summary()

Get summary of the anomalies in the system.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/anomalies/summary.json
Parameters :
   startTs  (optional) => Start timestamp, default:now-1h
   endTs    (optional) => End timestamp, default:current-time
Example :
    curl -ksb -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/anomalies/summary.json'
Response :
    {
        "totalAnomalyCount": 2,
        "totalAnomalyScore": 120.0,
        "entries": [
            {
                "severity": "warning",
                "anomalyCount": 1,
                "anomalyScore": 40.0
            },
            {
                "severity": "major",
                "anomalyCount": 1,
                "anomalyScore": 80.0
            }
        ]
    }
```

flow_telemetry_config()

Get the hardware flow telemetry configuration for the given switch.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/ftExpectedConfig.json?switch=<serialnum>
Parameters :
   serialnum  (required) => path: string type
Example :
    curl -ksb -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/ftExpectedConfig.json?switch=<serialnum>'
Response :
    {
      configure terminal
      nip access-list telemetryipv4acl
        30 permit udp 23.0.0.0/8 eq 60 29.0.0.0/8 eq 60
        31 permit udp 29.0.0.0/8 eq 60 23.0.0.0/8 eq 60
      65535 deny ip any
        nipv6 access-list telemetryipv6acl
      65535 deny ipv6 any
```

```
         feature analytics
         flow exporter telemetry
       destination 152.22.254.2 use-vrf default
         transport udp 30000
         source loopback0
         dscp 44
         flow exporter telemetryExp_1
       destination 152.22.254.4 use-vrf default
         transport udp 30000
         source loopback0
         dscp 44
         flow exporter telemetryExp_2
       destination 152.22.254.3 use-vrf default
         transport udp 30000
         source loopback0
         dscp 44
       flow record telemetryRec
         match ip source address
         match ip destination address
         match ip protocol
         match transport source-port
         match transport destination-port
         collect counter bytes
         collect counter packets
       flow monitor telemetryMon
         record telemetryRec
         exporter-bucket-id 1 0 1365
         exporter telemetryExp_0
         exporter-bucket-id 2 1366 2730
         exporter telemetryExp_1
         exporter-bucket-id 3 2731 4095
         exporter telemetryExp_2
       flow profile telemetryProf
         collect interval 1000
         source port 787
       flow filter telemetryFP
         ipv4 telemetryipv4acl
         ipv6 telemetryipv6acl
       flow system config
         exporter-id 80
         monitor telemetryMon input
         profile telemetryProf
         filter telemetryFP"

  }
```

flows_details()

Get detailed flows.

```
```

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/details.json
Parameters :
   startTs  (mandatory) => Start timestamp,
   endTs    (mandatory) => End timestamp, default:current-time
   filter   (optional) => Lucene format filter
{srcIp,srcPort,dstIp,dstPort,ProtocolName,ingressVrf,egressVrf}, default:null
   statName (optional) => Stat name {flow:latency, flow:epmove, flow:pktdrop,
flow:ingressburstmax, flow:egressburstmax, flow:ingressPktCount, flow:egressPktCount}
   granularity (optional) => Granularity of time period
   fabricName (optional) => limit the records pertaining to this fabricName

Example:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/details.json'
Response:
    {
        "nodeName": null,
        "description": "",
        "statName": null,
        "entries": [
            {
                "flowId": "44.3.3.26:0",
                "srcIp": "44.3.3.26",
                "dstIp": "42.2.2.22",
                "srcPort": "0",
                "dstPort": "0",
                "protocol": "61",
                "protocolName": "ANY-HOST",
                "ingressVrf": "ctx4_1",
                "egressVrf": "ctx4_1",
                "flowType": "IPV4",
                "ingressTenant": "tele4",
                "egressTenant": "tele4",
                "stats": [
                    {
                        "ingressPktCount": 6875,
                        "ingressByteCount": 8250000,
                        "egressPktCount": 0,
                        "egressByteCount": 0,
                        "ingressBurst": 0,
                        "ingressBurstMax": 4800,
                        "egressBurst": 0,
                        "egressBurstMax": 0,
                        "hashCollision": 0,
                        "latency": 0,
                        "srcMoveCount": 0,
                        "dstMoveCount": 0,
                        "moveCount": 0,
                        "dropPktCount": 0,
                        "dropNodes": [
                            "telemetry-hw-spine1"
                        ],
                        "paths": [
                            [
                                {
                                    "node": "telemetry-hw-leaf3",
                                    "nodeType": "Leaf",
                                    "ingressVifs": [
                                        "eth1/1"
                                    ],
                                    "egressVifs": [
                                        "eth1/49"
                                    ]
                                },
                                {
                                    "node": "telemetry-hw-spine1",
                                    "nodeType": "Spine",
                                    "asicDropCode": 128,
                                    "dropReason": "",
                                    "dropType": "info",
                                    "ingressVifs": [
                                        "eth2/2"
                                    ],
                                    "egressVifs": [
                                        ""
                                    ]
                                }
                            ]
                        ],
                        "nodeNames": [
                            "telemetry-hw-leaf3",
                            "telemetry-hw-spine1"
                        ],
                        "ingressNodes": [
                            "telemetry-hw-leaf3"
                        ],
                        "egressNodes": [],
                        "anomalyScore": 1,
                        "dropReasons": [],
                        "srcEpg": "testl3out",
                        "dstEpg": "",
                        "ts": "2019-02-01T19:18:56.458Z",
                        "originTs": "2019-02-01T19:18:38.445Z",
                        "terminalTs": "2019-02-01T19:20:42.419Z"
                    }
                ],
                "srcEpg": "testl3out",
                "dstEpg": ""
            }
        ]
```

```
    }
```

flows_summary()

Browse the flows.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/summary.json
Parameters :
   startTs  (optional) => Start timestamp, default:now-1h
   endTs    (optional) => End timestamp, default:current-time
   filter              => Lucene format filter, default:null
   fabricName (optional) => limit the records pertaining to this fabricName
Example:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/summary.json'
Response:
    {
        "nodeName": null,
        "description": "",
        "statName": null,
        "entries": [
            {
                "flowId": "44.3.3.26:0",
                "srcIp": "44.3.3.26",
                "dstIp": "42.2.2.22",
                "srcPort": "0",
                "dstPort": "0",
                "protocol": "61",
                "protocolName": "ANY-HOST",
                "ingressVrf": "ctx4_1",
                "egressVrf": "ctx4_1",
                "flowType": "IPV4",
                "ingressTenant": "tele4",
                "egressTenant": "tele4",
                "stats": [
                    {
                        "ingressPktCount": 6875,
                        "ingressByteCount": 8250000,
                        "egressPktCount": 0,
                        "egressByteCount": 0,
                        "ingressBurst": 0,
                        "ingressBurstMax": 4800,
                        "egressBurst": 0,
                        "egressBurstMax": 0,
                        "hashCollision": 0,
                        "latency": 0,
                        "srcMoveCount": 0,
                        "dstMoveCount": 0,
                        "moveCount": 0,
                        "dropPktCount": 0,
                        "dropNodes": [
                            "telemetry-hw-spine1"
                        ],
                        "paths": [
                            [
                                {
                                    "node": "telemetry-hw-leaf3",
                                    "nodeType": "Leaf",
                                    "ingressVifs": [
                                        "eth1/1"
                                    ],
                                    "egressVifs": [
                                        "eth1/49"
                                    ]
                                },
                                {
                                    "node": "telemetry-hw-spine1",
                                    "nodeType": "Spine",
                                    "asicDropCode": 128,
                                    "dropReason": "",
                                    "dropType": "info",
                                    "ingressVifs": [
                                        "eth2/2"
                                    ],
                                    "egressVifs": [
                                        ""
                                    ]
                                }
                            ]
                        ],
                        "nodeNames": [
                            "telemetry-hw-leaf3",
                            "telemetry-hw-spine1"
                        ],
                        "ingressNodes": [
                            "telemetry-hw-leaf3"
                        ],
                        "egressNodes": [],
                        "anomalyScore": 1,
                        "dropReasons": [],
                        "srcEpg": "testl3out",
                        "dstEpg": "",
                        "ts": "2019-02-01T19:18:56.458Z",
                        "originTs": "2019-02-01T19:18:38.445Z",
                        "terminalTs": "2019-02-01T19:20:42.419Z"
                    }
                ],
                "srcEpg": "testl3out",
                "dstEpg": ""
```

```
            }
        ]
    }
```

flows_top_flows()

Get the flows top flows.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/topFlows.json
Parameters :
   startTs  (optional) => Start timestamp, default:now-1h
   endTs    (optional) => End timestamp, default:current-time
   granularity (optional) => Granularity of time period
   statName (optional) => Stat name {flow:latency, flow:epmove, flow:pktdrop}
   fabricName (optional) => limit the records pertaining to this fabricName
Example:
    curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/topFlows.json'
Response:
    {
        "nodeName": null,
        "description": "",
        "statName": null,
        "entries": [
            {
                "flowId": "44.3.3.26:0",
                "srcIp": "44.3.3.26",
                "dstIp": "42.2.2.22",
                "srcPort": "0",
                "dstPort": "0",
                "protocol": "61",
                "protocolName": "ANY-HOST",
                "ingressVrf": "ctx4_1",
                "egressVrf": "ctx4_1",
                "flowType": "IPV4",
                "ingressTenant": "tele4",
                "egressTenant": "tele4",
                "stats": [
                    {
                        "ingressPktCount": 6875,
                        "ingressByteCount": 8250000,
                        "egressPktCount": 0,
                        "egressByteCount": 0,
                        "ingressBurst": 0,
                        "ingressBurstMax": 4800,
                        "egressBurst": 0,
                        "egressBurstMax": 0,
                        "hashCollision": 0,
                        "latency": 0,
                        "srcMoveCount": 0,
                        "dstMoveCount": 0,
                        "moveCount": 0,
                        "dropPktCount": 0,
                        "dropNodes": [
                            "telemetry-hw-spine1"
                        ],
                        "paths": [
                            [
                                {
                                    "node": "telemetry-hw-leaf3",
                                    "nodeType": "Leaf",
                                    "ingressVifs": [
                                        "eth1/1"
                                    ],
                                    "egressVifs": [
                                        "eth1/49"
                                    ]
                                },
                                {
                                    "node": "telemetry-hw-spine1",
                                    "nodeType": "Spine",
                                    "asicDropCode": 128,
                                    "dropReason": "",
                                    "dropType": "info",
                                    "ingressVifs": [
                                        "eth2/2"
                                    ],
                                    "egressVifs": [
                                        ""
                                    ]
                                }
                            ]
                        ],
                        "nodeNames": [
                            "telemetry-hw-leaf3",
                            "telemetry-hw-spine1"
                        ],
                        "ingressNodes": [
                            "telemetry-hw-leaf3"
                        ],
                        "egressNodes": [],
                        "anomalyScore": 1,
                        "dropReasons": [],
                        "srcEpg": "testl3out",
                        "dstEpg": "",
                        "ts": "2019-02-01T19:18:56.458Z",
                        "originTs": "2019-02-01T19:18:38.445Z",
                        "terminalTs": "2019-02-01T19:20:42.419Z"
                    }
```

```
                ],
                "srcEpg": "testl3out",
                "dstEpg": ""
            }
        ]
    }
```

flows_top_nodes()

Get the flows top nodes.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/topNodes.json
Parameters :
   startTs  (optional) => Start timestamp, default:now-1h
   endTs    (optional) => End timestamp, default:current-time
   granularity (optional) => Granularity of time period
   statName (optional) => Stat name {flow:latency, flow:epmove, flow:pktdrop},
default:flow-latency
   fabricName (optional) => limit the records pertaining to this fabricName
Example:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/flows/topNodes.json'
Response:
    {
        "entries": [
            {
                "nodeName": "telemetry-hw-spine1",
                "description": "",
                "stats": [
                    {
                        "ts": "2019-02-01T19:16:32.002Z",
                        "latency": 6
                    }
                ]
            },
            {
                "nodeName": "telemetry-hv-leaf1",
                "description": "",
                "stats": [
                    {
                        "ts": "2019-02-01T19:16:32.002Z",
                        "latency": 5
                    }
                ]
            }
        ]
    }
```

get_fabrics_anomaly_summary()

Get the fabric anomaly summary.

```
REST URL   :
    GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/fabricsSummary.json
Parameters :
    fabricName (mandatory) => Name of the Fabric
    startTs                => Start timestamp, default:current-time - 1 hour
    endTs                  => End timestamp, default:current-time
    include="anomalyScore" => Requires the Latest Maximum anomalyscores of the fabric,
default:'no'
    history                => Requires the timeseries data of sum(anomaly scores,
default:'no'
    granularity            => applicable if history = "yes" , granulairy of the
timeseries data, default=5m
Example    :
    curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/fabricsSummary.json'
Response   :
    {
        "anomalyScore" : "X"
        "entries": [
                 {
                     totalAnomalyScore ;  X
                     ts : now
                 }
                 .........
                 {
                     totalAnomalyScore ;  X
                     ts : now
                 }
        ],
        "totalResultsCount": N,
        "totalItemsCount": N
    }
```

get_fabrics_list()

Get the fabrics list.

```
REST URL   :
    GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-api/api/telemetry/fabrics.json
Parameters :
    filter              => Lucene format filter, default:null
Example    :
    curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/fabrics.json'
Response   :
    {
        "entries": [
            {
                "fabricName": "FABRIC1",
                "fabricId": "1",
                "vendor": "CISCO_N9K_STANDALONE",
                "fabricType": "VXLAN",
                "configStatus": "ENABLED",
                "switchCount": 2,
                "controllerCount": 0
            },
            {
                "fabricName": "FABRIC2",
                "fabricId": "2",
                "vendor": "CISCO_ACI",
                "fabricType": "VXLAN",
                "configStatus": "ENABLED",
                "switchCount": 4,
                "controllerCount": 3
            },
            <--snip-->
        ],
        "totalResultsCount": 11,
        "totalItemsCount": 11
    }
```

get_nodes_list()

Get the nodes list.

```
REST URL   :
    GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-api/api/telemetry/nodes.json
Parameters :
    startTs (mandatory) => Start timestamp
    endTs               => End timestamp, default:current-time
    count               => Num.of nodes in response, default:1000
    filter              => Lucene format filter, default:null
Example    :
    curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/nodes.json'
Response   :
    {
        "entries": [
            {
                "nodeRole": "leaf",
                "nodeId": "302",
                "nodeName": "rleaf-scrimshaw2",
                "nodeMgmtpIp": "1.2.3.4"
            },
            {
                "nodeRole": "spine",
                "nodeId": "205",
                "nodeName": "swmp14-dopplebock",
                "nodeMgmtpIp": "1.2.3.4"
            },
            <--snip-->
        ],
        "totalResultsCount": 11,
        "offset": 0,
        "totalItemsCount": 11
    }
```

get_protocols_details()

Get Telemetry Protocol Statistics details.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/details.json
Parameters :
   startTs  (mandatory) => Start timestamp
   endTs                => End timestamp, default:current-time
   fabricName           => limit the records pertaining to this fabricName
   nodeName             => Name of node
   statName             => <protocol[:counter[:qualifier]],
protocol[:counter[:qualifier]]...>
   history              => '1' or '0', default is '0', indicates time-series request
   granularity          => Granularity of time period, default:5m
   orderBy              => One statName of the format <protocol[:counter[:qualifier]]>
   filter               => Lucene format filter to query for specific nodeName or
sourceName, default:null
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/details.json'
Response   :
   {
       "totalResultsCount": 6,
       "totalItemsCount": 6,
       "offset": 0,
       "description": "Protocol statistical counters",
       "entries": [
           {
               "nodeName": "leaf-103",
               "entries": [
                   {
                       "sourceName": "phys-[eth1/14]",
                       "entries": [
                           {
                               "counterName": "InterfaceUtilisationIngress",
                               "value": 60.625,
                               "trending": "up",
                               "stats": [
                                   {
                                       "ts": "2018-10-24T05:05:00.000Z",
                                       "value": 60.625
                                   },
                                   {
                                       "ts": "2018-10-24T05:00:00.000Z",
                                       "value": 59.827586206896555
                                   },
                                   {
                                       "ts": "2018-10-24T04:55:00.000Z",
                                       "value": 59.57142857142857
                                   }
                               ]
                           }
                       ]
                   },
   <--snip-->
                   {
                       "sourceName": "phys-[eth1/11]",
                       "entries": [
                           {
                               "counterName": "LldpPktsEgress",
                               "value": 111.0,
                               "trending": "up",
                               "stats": [
                                   {
                                       "ts": "2018-10-24T05:05:00.000Z",
                                       "value": 111.0
                                   },
                                   {
                                       "ts": "2018-10-24T05:00:00.000Z",
                                       "value": 110.10344827586206
                                   },
                                   {
                                       "ts": "2018-10-24T04:55:00.000Z",
                                       "value": 109.61904761904762
                                   }
                               ]
                           }
                       ]
                   }
               ]
           }
       ]
   }
```

get_protocols_resources()

Get Telemetry Protocol Statistics resources.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/resources.json
Parameters :
   filter               => Lucene format filter, default:null
   fabricName           => limit the records pertaining to this fabricName
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/resources.json'
Response   :
   [
       {
           "protocol": "interface",
           "counter": "utilisation",
           "qualifiers": [
               "ingress",
               "egress"
           ]
       },
       {
           "protocol": "interface",
           "counter": "bytes",
           "qualifiers": [
               "ingress",
               "egress"
           ]
       },
   <--snip-->
       {
           "protocol": "lldp",
           "counter": "pkts",
           "qualifiers": [
               "ingress",
               "egress"
           ]
       },
       {
           "protocol": "lldp",
           "counter": "errors"
       }
   ]
```

get_protocols_topentities()

Get Telemetry Protocol Statistics.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
```

```
api/api/telemetry/protocols/topEntities.json
Parameters :
   startTs  (mandatory) => Start timestamp
   endTs                => End timestamp, default:current-time
   fabricName           => limit the records pertaining to this fabricName
   statName             => parameter to find topEntities
protocol[:counter[:qualifier]]
   granularity          => Granularity of time period, default:5m
   filter               => Lucene format filter to query for specific nodeName or
sourceName, default:null
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/topEntities.json'
Response   :
   {
       "totalResultsCount": 6,
       "totalItemsCount": 6,
       "offset": 0,
       "description": "Protocol statistical counters",
       "entries": [
           {
               "nodeName": "leaf-103",
               "entries": [
                   {
                       "sourceName": "phys-[eth1/4]",
                       "entries": [
                           {
                               "counterName": "InterfaceUtilisationIngress",
                               "value": 65.53333333333333,
                               "trending": "down",
                               "stats": [
                                   {
                                       "ts": "2018-10-24T05:20:00.000Z",
                                       "value": 65.53333333333333
                                   },
                                   {
                                       "ts": "2018-10-24T05:15:00.000Z",
                                       "value": 65.78571428571429
                                   }
                               ]
                           }
                       ]
                   },
                   {
                       "sourceName": "phys-[eth1/14]",
                       "entries": [
                           {
                               "counterName": "InterfaceUtilisationIngress",
                               "value": 59.666666666666664,
                               "trending": "up",
                               "stats": [
                                   {
                                       "ts": "2018-10-24T05:20:00.000Z",
                                       "value": 59.666666666666664
                                   },
                                   {
                                       "ts": "2018-10-24T05:15:00.000Z",
                                       "value": 59.5
                                   }
                               ]
                           }
                       ]
                   },
   <--snip-->
               ]
           }
       ]
   }
```

get_protocols_topnodes()

Get Telemetry Protocol Statistics.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/topNodes.json
Parameters :
   startTs  (mandatory) => Start timestamp
   endTs                => End timestamp, default:current-time
   fabricName           => limit the records pertaining to this fabricName
   nodeName             => Name of node
   statName             => interface:utilization
   summarize            => '1' or '0', default is '0', summarizes across protocols
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/protocols/topNodes.json'
Response   :
    {
        "totalResultsCount": 6,
        "totalItemsCount": 6,
        "offset": 0,
        "description": "Protocol top nodes by score",
        "entries": [
            {
                "nodeName": "leaf-103",
                "entries": [
                    {
                        "counterName": "protocol|utilization",
                        "stats": [
                            {
                                "ts": "2019-02-08T13:50:00.000Z",
                                "value": 62.333333333333336
                            },
                            {
                                "ts": "2019-02-08T13:45:00.000Z",
                                "value": 62.833333333333336
                            }
                        ],
                        "value": 62.333333333333336,
                        "trending": "down"
                    }
                ]
            },
    ....
    }
```

health_diagnostics()

Get the health diagnostics.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/health/collectionStats.json
Parameters :
   None
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/health/collectionStats.json'
Response   :
   {
       "totalItemsCount": 11,
       "entries": [
           {
               "nodeName": "pod20-leaf3",
               "stats": [
                   {
                       "resource": "sysStats",
                       "totalItemsCount": 9600,
                       "lastUpdatedTs": "2018-06-13T10:25:52.468Z",
                       "state": "HEALTHY"
                   }
               ]
           },
           <--snip-->
       ]
   }
```

service_health()

Get the health of the services.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/health/serviceHealth.json
Parameters :
   None
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/health/serviceHealth.json'
Response   :
   {
       "entries": [
           {
               "serviceType": "THIRD_PARTY_SERVICE",
               "serviceName": "elastic",
               "state": "HEALTHY",
               "displayName": "Data Store"
           },
           {
               "serviceType": "CISCO_SERVICE",
               "serviceName": "correlator",
               "state": "HEALTHY",
               "displayName": "Correlator"
           },
           <--snip-->
       ]
   }
```

software_telemetry_config()

Get the software telemetry configuration for the given switch.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/swExpectedConfig.json?switch=<serialnum>
Parameters :
   serialNumber  (required) => path: string type
Example :
    curl -ksb -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/swExpectedConfig.json?switch=<serialnum>'
Response :
    {

    feature ntp
    ntp server <IP address> prefer use-vrf management

    feature lldp
    feature icam
    feature telemetry
```

```
  telemetry
  destination-profile
        use-vrf management
  destination-group 500
        ip address <IP address of> port 57500 protocol gRPC encoding GPB
        use-chunking size 4096
  destination-group 501
    ip address <IP address of> port 57500 protocol gRPC encoding GPB-compact
    use-chunking size 4096
  sensor-group 506
    data-source NX-API
    path "show system routing mode" depth unbounded
  sensor-group 511
    data-source DME
    path sys/intf depth unbounded filter-condition
or(and(updated(ethpmAggrIf.operSt),eq(ethpmAggrIf.operSt,"down")),and(updated(ethpmAgg
rIf.operSt),eq(ethpmAggrIf.operSt,"up")))
  sensor-group 500
    data-source NX-API
    path "show icam scale" depth unbounded
    path "show environment temperature" depth unbounded
    path "show spanning-tree summary" depth unbounded
    path "show processes cpu" depth unbounded
    path "show processes memory physical" depth unbounded
    path "show system resources" depth unbounded
    path "show module" depth unbounded
    path "show processes log" depth unbounded
  sensor-group 502
    data-source DME
    path sys/intf depth 0 query-condition query-target=subtree&target-subtree-
class=ethpmPhysIf,rmonEtherStats,rmonIfIn,rmonIfOut,ethpmAggrIf,l1PhysIf,pcAggrIf,ethp
mPortCap
  sensor-group 503
    data-source DME
    path sys/intf depth 0 query-condition query-target=subtree&target-subtree-
class=eqptFcotLane,eqptFcotSensor
  sensor-group 504
    data-source NX-API
    path "show routing ip summary cached vrf all" depth unbounded
    path "show routing ipv6 summary cached vrf all" depth unbounded
    path "show ip mroute summary vrf all" depth unbounded
    path "show ipv6 mroute summary vrf all" depth unbounded
    path "show vpc" depth unbounded
    path "show vrf all" depth unbounded
    path "show mac address-table count" depth unbounded
    path "show nve vni" depth unbounded
    path "show nve peers detail" depth unbounded
    path "show vlan summary" depth unbounded
    path "show system internal icam app hardware internal forwarding table
utilization" depth unbounded query-condition show-output-format=json
```

```
    path "show system internal icam app system internal access-list resource
utilization" depth unbounded query-condition show-output-format=json
  sensor-group 505
    data-source NX-API
    path "show environment power" depth unbounded
    path "show system internal flash" depth unbounded
    path "show clock" depth unbounded
    path "show feature" depth unbounded
    path "show environment fan detail" depth unbounded
  sensor-group 501
    data-source NX-API
    path "show lacp counters detail" depth unbounded
    path "show lacp interface" depth unbounded
    path "show port-channel summary" depth unbounded
    path "show lldp traffic interface all" depth unbounded
  sensor-group 507
    data-source DME
    path sys/cdp depth 1 query-condition query-target=subtree&target-subtree-
class=cdpIf,cdpAdjEp,cdpIfStats
    path sys/bgp depth 1 query-condition query-target=subtree&target-subtree-
class=bgpEntity,bgpInst,bgpDom,bgpDomAf,bgpPeer,bgpPeerEntry,bgpPeerEntryStats,bgpPeer
Events,bgpPeerAfEntry
    path sys/lldp depth 1 query-condition query-target=subtree&target-subtree-
class=lldpIf,lldpAdjEp,lldpIfStats
  sensor-group 508
    data-source DME
    path sys/intf depth 1 query-condition query-target=subtree&target-subtree-
class=pcAggrIf&query-target-filter=deleted()
  sensor-group 509
    data-source NX-API
    path "show ip igmp interface vrf all" depth unbounded
    path "show ip igmp groups vrf all" depth unbounded
    path "show ip igmp snooping statistics" depth unbounded
    path "show ip igmp snooping" depth unbounded
    path "show ip igmp snooping groups" depth unbounded
    path "show ip igmp snooping groups summary" depth unbounded
    path "show ip igmp snooping groups detail" depth unbounded
    path "show ip pim statistics vrf all" depth unbounded
    path "show ip pim interface vrf all" depth unbounded
    path "show ip pim neighbor vrf all" depth unbounded
    path "show ip pim rp vrf all" depth unbounded
    path "show ip pim route vrf all" depth unbounded
    path "show queuing burst-detect detail" depth unbounded
  sensor-group 510
    data-source NATIVE
    path adjacency
    path mac-all
  subscription 500
    dst-grp 500
    snsr-grp 506 sample-interval 3600000
    snsr-grp 511 sample-interval 0
    snsr-grp 500 sample-interval 59000
    snsr-grp 502 sample-interval 60000
    snsr-grp 503 sample-interval 62000
    snsr-grp 504 sample-interval 61000
    snsr-grp 505 sample-interval 300000
    snsr-grp 501 sample-interval 60000
    snsr-grp 507 sample-interval 65000
    snsr-grp 508 sample-interval 0
    snsr-grp 509 sample-interval 63000
  subscription 501
    dst-grp 501
    snsr-grp 510 sample-interval 0
end
    }
```

utilization_node_details()

Get the node details.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/utilization/nodeDetails.json
Parameters :
   None
Example    :
  curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/utilizationnodeDetails.json'
Response   :
    {
       "totalResultsCount": 157,
       "totalItemsCount":157,
       "entries": [
           {
               "nodeName": "node-1",
               "entries": [
                   {
                       "resourceName":"cpu",
                       "latestValue":"85",
                       "maxValue":"100",
                       "resourceCategory":"",
                       "trending":"down",
                       "values":[
                           { "value":"85", "ts":"2018-02-21T20:21:03.109Z" },
                           {},
                           <--snip-->
                           {}
                       ]
                   },
                   {
                       "resourceName":"memory",
                       "latestValue":"84",
                       "maxValue":"100",
                       "resourceCategory":"",
                       "trending":"up",
                       "values":[
                           { "value":"84", "ts":"2018-02-21T20:21:03.109Z" },
                           {},
                           <--snip-->
                           {}
                       ]
                   },
                   <-- snip , LIST OF ALL OTHER RESOURCES -->
                   {
                       "resourceName":"ports",
                       "latestValue":"83",
                       "maxValue":"100",
                       "resourceCategory":"",
                       "trending":"up",
                       "values":[
                           { "value":"83", "ts":"2018-02-21T20:21:03.109Z" },
                           {},
                           <--snip-->
                           {}
                       ]
                   }
               ]
          },
          {
              "nodeName": "node-2"
              <-- same as in node-1 -->
          }
          <----snip LIST OF ALL OTHER NODES --->
          {
              "nodeName": "node-10"
              <-- same as in node-1 -->
          }
      ]
   }
```

utilization_top_nodes()

Get top nodes by utilization.

```
REST URL   :
   GET https://<ip:port>/appcenter/Cisco/NIR/apiserver-
api/api/telemetry/utilization/topNodes.json
Parameters :
   None
Example    :
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/apiserver-
```

```
api/api/telemetry/utilization/topNodes.json'
Response   :
   {
       "totalResultsCount": 10,
       "totalItemsCount":10,
       "entries": [
           {
               "nodeName": "node-1",
               "entries": [
                   {
                       "resourceName":"cpu",
                       "latestValue":"85",
                       "maxValue":"100",
                       "resourceCategory":"",
                       "trending":"down",
                       "values":[
                           { "value":"85", "ts":"2018-02-21T20:21:03.109Z" },
                           {},
                           <--snip-->
                           {}
                       ]
                   },
                   {
                       "resourceName":"memory",
                       "latestValue":"84",
                       "maxValue":"100",
                       "resourceCategory":"",
                       "trending":"up",
                       "values":[
                           { "value":"84", "ts":"2018-02-21T20:21:03.109Z" },
                           {},
                           <--snip-->
                           {}
                       ]
                   },
                   {
                       "resourceName":"ports",
                       "latestValue":"83",
                       "maxValue":"100",
                       "resourceCategory":"",
                       "trending":"up",
                       "values":[
                           { "value":"83", "ts":"2018-02-21T20:21:03.109Z" },
                           {},
                           <--snip-->
                           {}
                       ]
                   }
               ]
          },
          {
              "nodeName": "node-2"
              <-- same as in node-1 -->
          }
          <----snip--->
          {
              "nodeName": "node-10"
              <-- same as in node-1 -->
          }
      ]
   }
```

Troubleshooting Cisco NIR Application on Cisco DCNM

Troubleshooting Cisco NIR Common GUI Issues

- The Cisco NIR app has the ability to display historical data. The specific time duration can be selected from the available calendar to see data within that particular time range.
- The majority of issues will be due to receiving data from the APIs other than what was expected. Opening the **Developer Tools Network** tab and repeating the last action will show the API data received. If the issue is with the APIs, then troubleshooting will need to continue on the backend.
- If the API requests and responses are accurate then check the **Developer Tools Console** tab for any errors.
- After initial installation the application needs time to start. During this time, the GUI may exhibit incomplete or unstable behavior. It is recommended to wait several minutes before starting to use the application.
- Take screenshots just before and just after reproducing an issue. Screenshots along with a full network capture saved as HAR with contents can be used to issue reports. If an issue report has a HAR recording attached then there is a significantly higher chance that the root cause can be identified and resolved quickly.
- If the Cisco NIR GUI page loads to a skeleton template with spinner then this means almost none of the APIs are responding.
- If the Cisco NIR GUI page is taking a while to load sites then this means the `fabrics.json` API is not responding or not returning any sites.
- If the site anomaly score does not agree with reported anomalies, or the node counts are incorrect, then check the `fabricsSummary.json` response for the site `anomalyScore` value, and check the `nodes.json` response for the types and counts of nodes reported.
- If the expected sites are not shown in the site selection dropdown, first verify that they are not included in the `fabrics.json` response entries, then rerun setup and edit the data collection setup configuration to view the state of the configured sites. Make sure the appropriate sites are enabled and that no errors are reported. This data comes from the `get_nir_fabrics` request.
- For Flow Analytics issues make sure the following requirements are met:
  - The `capability.json` request is made when the GUI loads and returns true. If it returns false, it means the site does not support this feature.
  - Navigate to **Application Settings** tab and make sure **Flow Collection** has been enabled, the Management In-Band EPG has been selected, and verify the flow collection filters have been correctly configured.
  - To verify the MOs are using `visore`, navigate to **uni** > **site** > **flowcol** to check the configuration and check the classes `telemetrySelector`, `telemetrySubnetFltGrp`, and `telemetrySubnetFilter`.
  - Navigate to **Collection Status** tab and check if the nodes are returning flow telemetry.

Troubleshooting at Cisco NIR App Level

- To view running service instances, navigate to **DCNM** > **Application** > **NIR** and right-click the settings icon.
- To view capacity usage, navigate to **NIR**, right-click the settings icon and choose **System Status**.
- If there is no data shown in Cisco NIR dashboard, check the *Setup* page. Navigate to **NIR**, right-click the settings icon and choose **Rerun Setup**.
    - If no site is enabled, try to enable a site from available sites.
    - If no site is available, check if Cisco DCNM site is setup properly.
- To view telemetry data collection status, navigate to **NIR**, right-click the settings icon and choose **Collection Status**. Any red dot indicates that the telemetry data is not streamed. Possibilities for red dot are:
    - Switch is in monitor mode and telemetry configuration may not be available.
    - Switch telemetry configuration CLI may be missing or causing error.

Troubleshooting at Switch Level

- To check the telemetry connection status:
    - Login to the switch using SSH.
    - Execute the following command and verify status of telemetry connection.

    ```
    switch# show telemetry transport
    ```

- To check the telemetry data collector details:
    - Login to the switch using SSH.
    - Execute the following command.

    ```
    switch# show telemetry data collector details
    ```

- To check for any time sync issues from the switches:
    - Login to Cisco DCNM compute node using SSH.
    - Execute the following commands:

    ```
    node# docker ps|grep debug
    node# docker exec -it <debugcontainerid> sh
    node# show ntp-time-sync
    ```

    Check if the telemetry data is not synced with NTP server.

Troubleshooting at Services Level

- To check the basic services are running:

  1. To check for the required telemetry services are up and running:

     - Login to the master node and execute the following command.

       ```
       node# docker service Is
       ```

     - Verify the services `elasticsearch_Cisco_afw`, `elasticservice_Cisco_afw`, `elasticsix_Cisco_afw`, `elasticsixhwtm_Cisco_afw`, `kafka_Cisco_afw`, `zookeeper_Cisco_afw`, `apiserver_Cisco_afw`, `eventcollector_Cisco_afw`, `flowsink_Cisco_afw`, `genie_Cisco_afw`, `nirhealth_Cisco_afw`, `sensei_Cisco_afw`, `thirdpartycoll_Cisco_afw`, `tmniragent_Cisco_afw`, `utr_Cisco_afw`, `postprocessor_Cisco_afw`, `utrctfilter_Cisco_afw`, `utrftcoll_Cisco_afw`, and `utrftcorr_Cisco_afw` are available and running.

  2. To check all the topics are pre-created and are in place:

     - Login to the compute node and execute the following command.

       ```
       node# docker ps|grep debugtools
       ```

     - Get the container ID and execute the following command to debug the container.

       ```
       node# docker exec -it <debugcontainerid> sh
       ```

     - Execute the following command in shell prompt.

       ```
       sh# show kafka topics
       ```

     - Verify the topics `cisco_nir-aggFlows`, `cisco_nir-anomalies`, `cisco_nir-anomalyFlows`, `cisco_nir-anomalydir`, `cisco_nir-anomalywriter`, `cisco_nir-config`, `cisco_nir-ct_debug`, `cisco_nir-debug`, `cisco_nir-distributedcache`, `cisco_nir-eprecords`, `cisco_nir-eprecords-in`, `cisco_nir-events`, `cisco_nir-fabricsdata`, `cisco_nir-flows`, `cisco_nir-internalAggFlows`, `cisco_nir-operational`, `cisco_nir-rest-dial-in`, `cisco_nir-stats-json`, `cisco_nir-sw-telemetry-utr-out`, `cisco_nir-swTrackrNotif`, `cisco_nir-systemanomalies`, `cisco_nir-systemtasks`, `cisco_nir-tasks`, and `cisco_nir-telemetryEvents` are available.

  3. To check all the indicies are present:

     - Login to the compute node and execute the following command.

       ```
       node# docker ps|grep debugtools
       ```

     - Get the container ID and execute the following command to debug the container.

       ```
       node# docker exec -it <debugcontainerid> sh
       ```

     - Execute the following command in shell prompt.

       ```
       sh# show elastic indices
       ```

     - Verify the indicies `cisco_nir-anomalydb`, `cisco_nir-anomalydirdb`, `cisco_nir-fabricsdb`, `cisco_nir-geniemetricsdb`, `cisco_nir-heartbeatdb`, `cisco_nir-integrationsdb`, `cisco_nir-mcastoperdb`, `cisco_nir-onboardingdb`, `cisco_nir-operdb`, `cisco_nir-policydb`, `cisco_nir-

    `registerdb`, `cisco_nir-registeriddb`, `cisco_nir-svcstatsdb`, `cisco_nir-systemanomalydb`, `cisco_nir-systemprefsdb`, `cisco_nir-trendstatsdb`, `cisco_nir-userprefsdb`, `cisco_nir-collectorstatsdb`, `cisco_nir-enrich_interfacedb`, `cisco_nir-enrich_l2db`, `cisco_nir-enrich_l3db`, `cisco_nir-enrich_summarydb`, `cisco_nir-eprecordsdb`, `cisco_nir-eventsdb`, `cisco_nir-fabricnodesdb`, `cisco_nir-interfacedb`, `cisco_nir-l2db`, `cisco_nir-l3db`, `cisco_nir-l3outdb`, `cisco_nir-microburstdb`, `cisco_nir-resourcecollectdb`, `cisco_nir-routesdb`, `cisco_nir-statsdb`, `telemetry_cfg-book_cfg_2_2_2`, `telemetry_cfg-fabric_cfg_2_2_2`, `telemetry_cfg-hwft_cfg_2_2_2`, `telemetry_cfg-hwft_fabric_cfg_2_2_2`, `telemetry_cfg-hwft_switch_cfg_2_2_2`, `telemetry_cfg-rcv_cfg_hw_ft_2_2_2`, `telemetry_cfg-rcv_cfg_sw_2_2_2`, `telemetry_cfg-switch_cfg_2_2_2`, `telemetry_netvrf-netvrf_2_2_2`, `telemetry_nir_fabrictype`, `telemetry_nir_ft_fabric_cfg`, and `telemetry_nir_ft_filter_cfg` are available.

4. Other useful docker commands to check the basic services are running:
   - Login to the compute node and execute the following command.

     `node# docker ps`

   - To get the memory and CPU statistics of containers running in compute node:

     `node# docker estats`

   - Get the container ID to view the instant logs of any running container:

     `node# docker logs <containerid> -f`

   - To view the logs of any running service in the master mode:

     `node# docker service logs <servicecontainerid> -f`

- To check for the individual services:
  - Telemetry receiver stage.
  - Postprocessor stage.
  - Event collector, Predictor and correlator stage.

Troubleshooting at UTR Telemetry Receiver Level

1. Make sure the Debug Tools app is available and running to debug a service.
   - Login to the compute node and execute the following command.

     ```
     node# docker ps|grep debug
     ```

   - Get the container ID and execute the following command to debug container.

     ```
     node# docker exec -it <debugcontainerid> sh
     ```

2. Execute the following command to verify that the data is flowing through UTR service.

```
sh-4.2# show kafka data-utr-out --help
Usage: show kafka data-utr-out [OPTIONS]

Options:
-n, --node-name TEXT
-o, --offset [latest|earliest]
--help
Show this message and exit.
```

3. Other useful commands to check UTR telemetry receiver data.

```
sh# show kafka data-utr-out -n leaf0 -o latest</userinput>
sh# show kafka data-utr-out -n leaf0 -o latest | grep -i "show vlan summary"
```

Troubleshooting at Post-Processor Level

- Make sure the Dubug Tools app is running to debug a service.
  - Login to the compute node and execute the following command.

    ```
    node# docker ps|grep debug
    ```

  - Get the container ID and execute the following command to debug the container.

    ```
    node# docker exec -it <debugcontainerid> sh
    ```

- Execute the following commands to verify that the data is flowing through post-processor service.

```
sh-4.2# show kafka data-processed --help
Usage: show kafka data-processed [OPTIONS]

Options:
-r, --stat-type [hardware|protocol|environmental|config|operational|interface|To be
removed]
-n, --node-name TEXT
-f, --fabric-name TEXT
-o, --offset [latest|earliest]
--help Show this message and exit.
```

- Execute the following command to verify that the site node is flowing through post-processor service.

```
sh-4.2# show kafka data-fabricnodes --help
Usage: show kafka data-fabricnodes [OPTIONS]

Options:
-n, --node-name TEXT
-f, --fabric-name TEXT
-o, --offset [latest|earliest]
--help Show this message and exit.
```

- Other useful commands to troubleshoot post-processor:

```
sh# show kafka data-processed -r environmental -n leaf0 -o earliest VXLAN-1
sh# show kafka data-processed -r environmental -n leaf0 -o earliest VXLAN-1 | grep -l
"powerDrawn"
```

Troubleshooting at Event Collector, Predictor, and Correlator Services Level

- Execute the following command to verify the processed data is available in time series database.

```
sh-4.2#  show nir es stats
Usage: show nir es stats [OPTIONS] COMMAND [ARGS]...

Options:
  --help Show this message and exit.

Commands:
aggregated
anomaly
raw

sh-4.2#  show nir es stats raw --help
Usage: show nir es stats raw [OPTIONS]

Options:
-r, --stat-type [utilization|l2_protocol|interface]
-n, --node-name TEXT
-f, --fabric-name TEXT
-s, --start-time [now-15m|now-1h|now-6h|now-1d|now-1w|now-1M]
-p, --pretty
--help Show this message and exit.
```

- Other useful commands to troubleshoot collector, predictor, and correlator services.
  - Execute the following commands to check for the available fabrics.

```
# show nir es fabrics
# show nir es fabrics -f Simulation
```

- Execute the following commands to check for the available fabrics nodes.

```
# show nir es fabrics-nodes -f Simulation
# show nir es fabrics-nodes -f Simulation -n N9Kv-2
```

- Execute the following command to verify the Statistics data.

```
# show nir es stats raw -f Simulation -n N9Kv-1 -r utilization
```

- Execute the following command to verify the Aggregated data.

```
# show nir es stats aggregated -f Simulation -n N9Kv-2 -r config
```

- Execute the following command to verify the Anomaly data.

```
# show nir es stats anomaly -f Simulation -n N9Kv-1 -r config
```

Debugging Cisco NIR App on Cisco DCNM

- To fetch the software telemetry logs from the devices streaming the data execute the following command:

  ```
  N9k-ToR2# show tech-support telemetry > ts_telemetry.log
  ```

- To fetch the logs for single node Cisco DCNM server execute the following command:

  ```
  # appmgr afw fetch-logs Cisco:NIR
  ```

- To fetch the logs for Cisco DCNM server with HA (active-standby):
  - Login to the active Cisco DCNM server.
  - Execute the following command:

    ```
    # appmgr afw fetch-logs Cisco:NIR:2.0 [password]
    ```

- To collect the logs for applications such as Kafka and Elastic execute the following command:

  ```
  # appmgr afw fetch-logs Cisco:Kafka
  ```

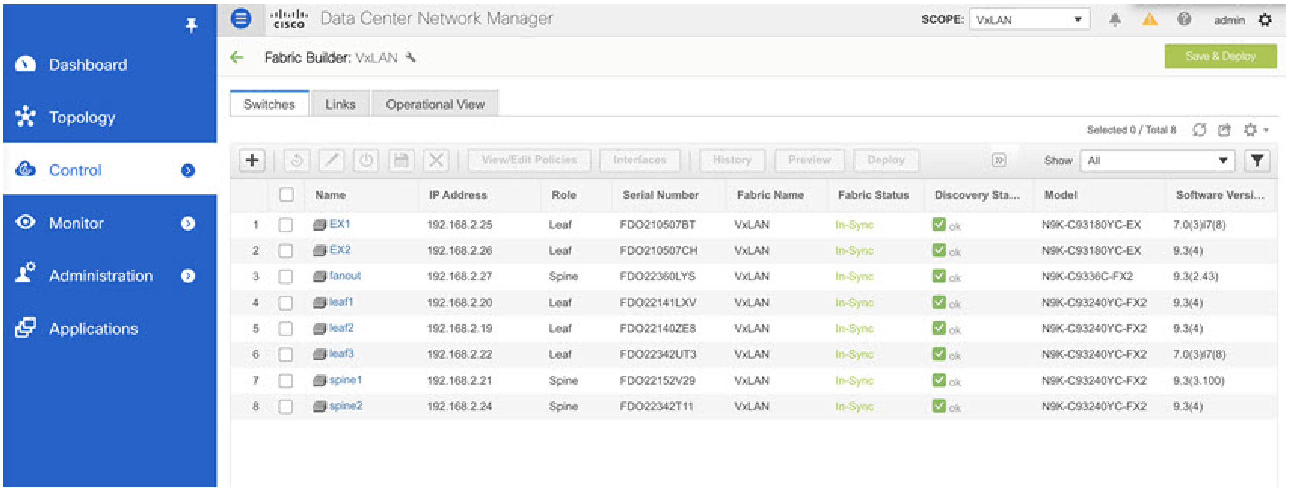
- To collect the logs for all applications execute the following command:

  ```
  # appmgr techsupport
  ```

Configure Telemetry on Cisco DCNM Site in Managed Mode

The following steps configure and enable telemetry on Cisco DCNM site in managed mode.

1. Ensure the switches on Cisco DCNM site display *In-Sync* status as shown in the following illustration. Click **Save & Deploy**, if the switches on Cisco DCNM site display *Out-of-Sync* status.



Fabric Builder: VxLAN

Selected 0 / Total 8

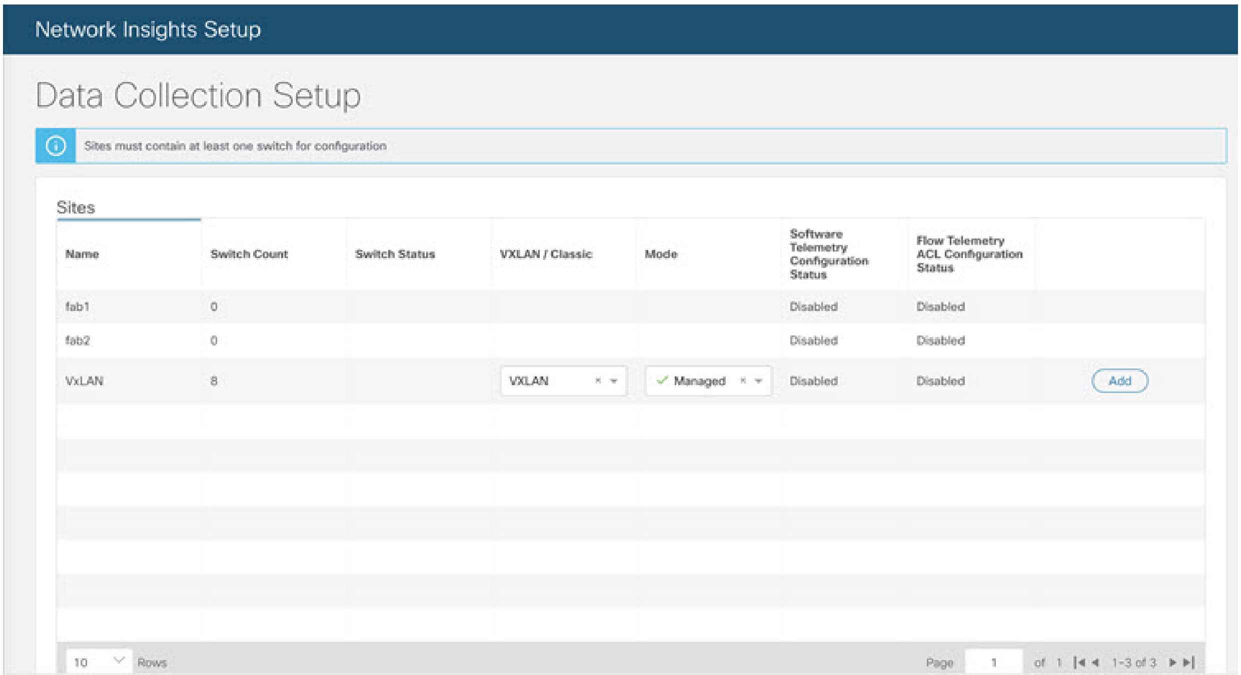
		Name	IP Address	Role	Serial Number	Fabric Name	Fabric Status	Discovery Sta...	Model	Software Versi...
1	□	EX1	192.168.2.25	Leaf	FDO210507BT	VxLAN	In-Sync	✓ ok	N9K-C93180YC-EX	7.0(3)I7(8)
2	□	EX2	192.168.2.26	Leaf	FDO210507CH	VxLAN	In-Sync	✓ ok	N9K-C93180YC-EX	9.3(4)
3	□	fanout	192.168.2.27	Spine	FDO22360LYS	VxLAN	In-Sync	✓ ok	N9K-C9336C-FX2	9.3(2.43)
4	□	leaf1	192.168.2.20	Leaf	FDO22141LXV	VxLAN	In-Sync	✓ ok	N9K-C93240YC-FX2	9.3(4)
5	□	leaf2	192.168.2.19	Leaf	FDO22140ZE8	VxLAN	In-Sync	✓ ok	N9K-C93240YC-FX2	9.3(4)
6	□	leaf3	192.168.2.22	Leaf	FDO22342UT3	VxLAN	In-Sync	✓ ok	N9K-C93240YC-FX2	7.0(3)I7(8)
7	□	spine1	192.168.2.21	Spine	FDO22152V29	VxLAN	In-Sync	✓ ok	N9K-C93240YC-FX2	9.3(3.100)
8	□	spine2	192.168.2.24	Spine	FDO22342T11	VxLAN	In-Sync	✓ ok	N9K-C93240YC-FX2	9.3(4)

2. Click **Settings** > **Network Insights Setup** > **Edit Configuration** on the right top of Cisco NIR app.

   a. Select VxLAN or Classic site type.

   b. Select the Managed Mode site mode.

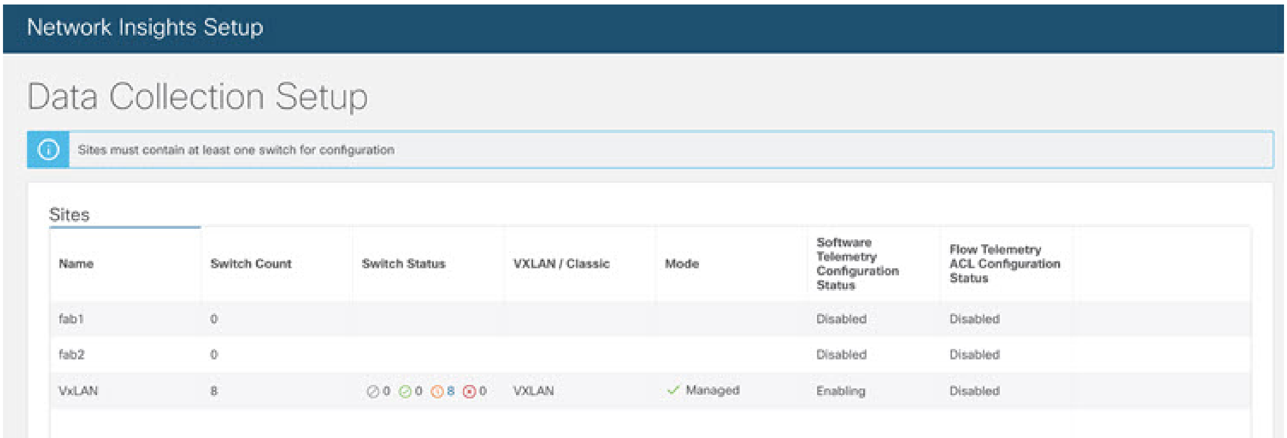
   c. Click **Add** and then **Apply**.



Sites must contain at least one switch for configuration

Name	Switch Count	Switch Status	VXLAN / Classic	Mode	Software Telemetry Configuration Status	Flow Telemetry ACL Configuration Status	
fab1	0				Disabled	Disabled	
fab2	0				Disabled	Disabled	
VxLAN	8		VXLAN	✓ Managed	Disabled	Disabled	Add

3. The **Software Telemetry Configuration Status** shows *Enabling* and then *Enabled* or *Enable Failed* status.



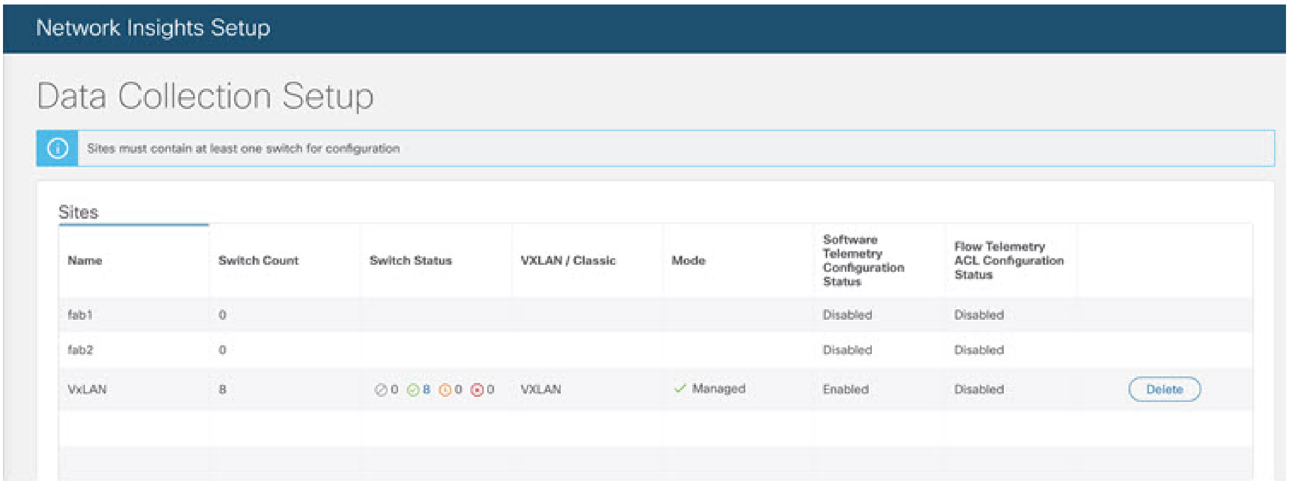
Network Insights Setup

Data Collection Setup

ⓘ Sites must contain at least one switch for configuration

Sites

Name	Switch Count	Switch Status	VXLAN / Classic	Mode	Software Telemetry Configuration Status	Flow Telemetry ACL Configuration Status
fab1	0				Disabled	Disabled
fab2	0				Disabled	Disabled
VxLAN	8	⊘ 0 ⊘ 0 ⊙ 8 ⊗ 0	VXLAN	✓ Managed	Enabling	Disabled



Network Insights Setup

Data Collection Setup

ⓘ Sites must contain at least one switch for configuration

Sites

Name	Switch Count	Switch Status	VXLAN / Classic	Mode	Software Telemetry Configuration Status	Flow Telemetry ACL Configuration Status	
fab1	0				Disabled	Disabled	
fab2	0				Disabled	Disabled	
VxLAN	8	⊘ 0 ⊘ 8 ⊙ 0 ⊗ 0	VXLAN	✓ Managed	Enabled	Disabled	Delete

4. Once the status shows *Enabled* or *Enable Failed*, navigate to Fabric Builder UI screen.

    a. Verify that all switches display *In-Sync* status.

    b. Click **Save & Deploy**, if the switches display *Out-of-Sync* status.

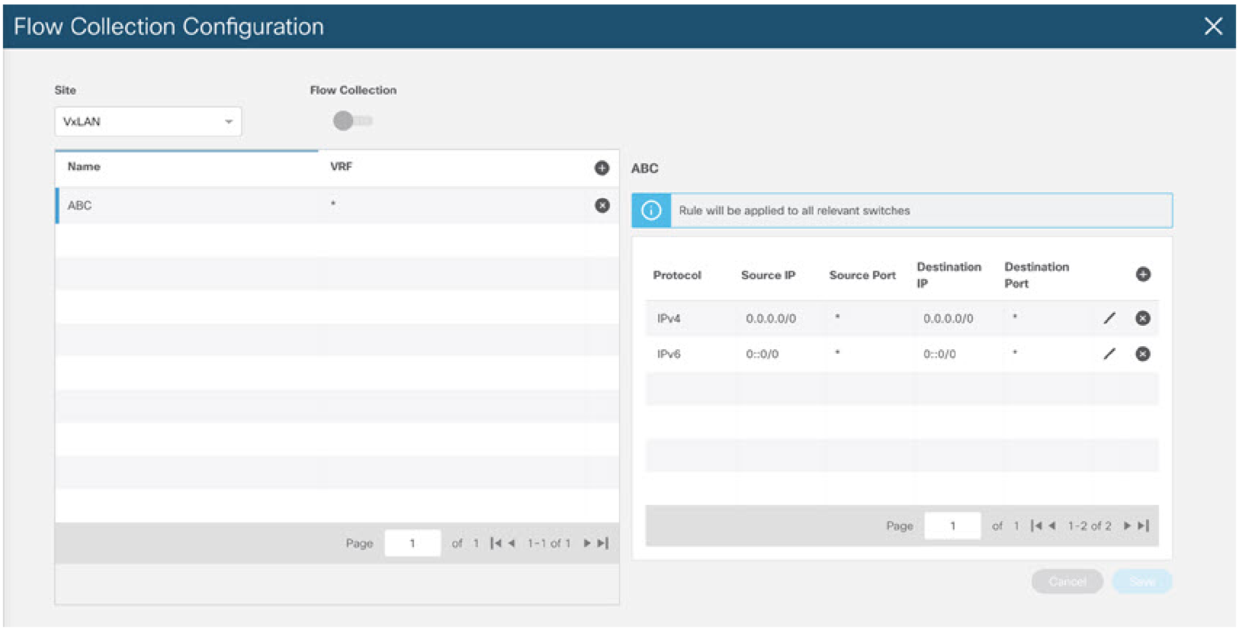
5. Click **Settings** > **Flow Collection Configuration** on the right top of Cisco NIR app.

    a. Choose the site from the drop-down menu.

    b. Select the switch to create a flow collection rule.

    c. Click **Save**.

    d. Toggle **Flow Collection** to enable flow telemetry on the switches.



Flow Collection Configuration

Site: VxLAN

Flow Collection

Name	VRF
ABC	*

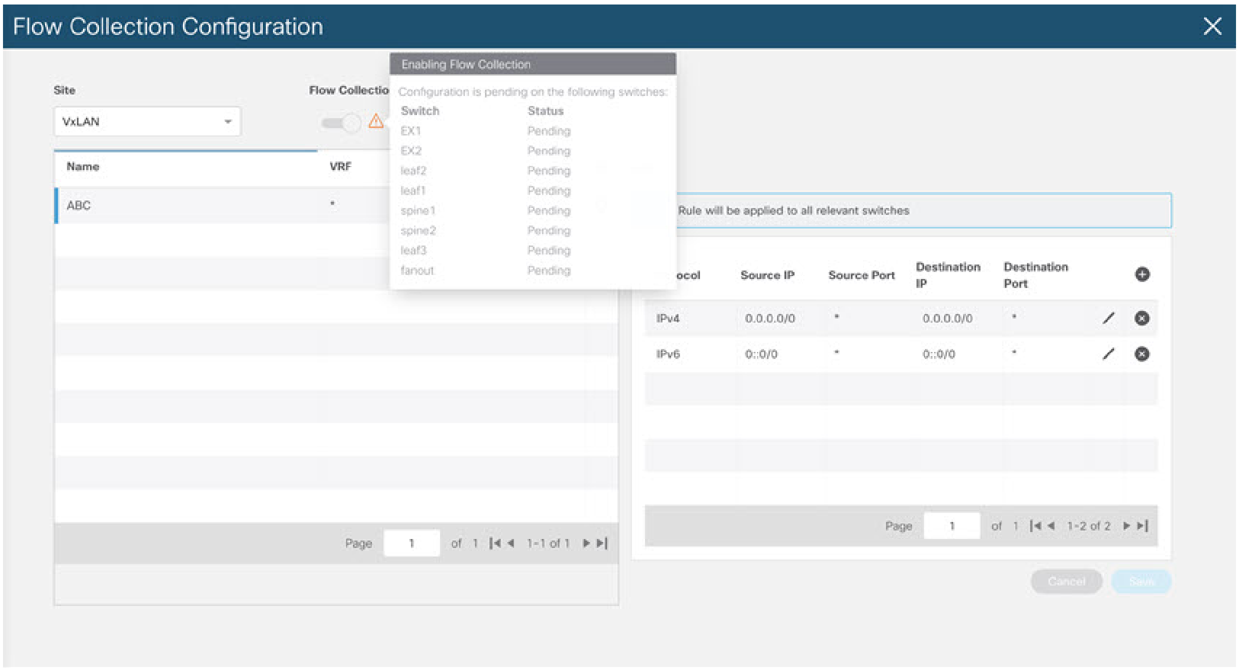
Page 1 of 1 1-1 of 1

ABC

Rule will be applied to all relevant switches

Protocol	Source IP	Source Port	Destination IP	Destination Port
IPv4	0.0.0.0/0	*	0.0.0.0/0	*
IPv6	0::0/0	*	0::0/0	*

Page 1 of 1 1-2 of 2



Flow Collection Configuration

Site: VxLAN

Flow Collectio

Enabling Flow Collection

Configuration is pending on the following switches:

Switch	Status
EX1	Pending
EX2	Pending
leaf2	Pending
leaf1	Pending
spine1	Pending
spine2	Pending
leaf3	Pending
fanout	Pending

Name	VRF
ABC	*

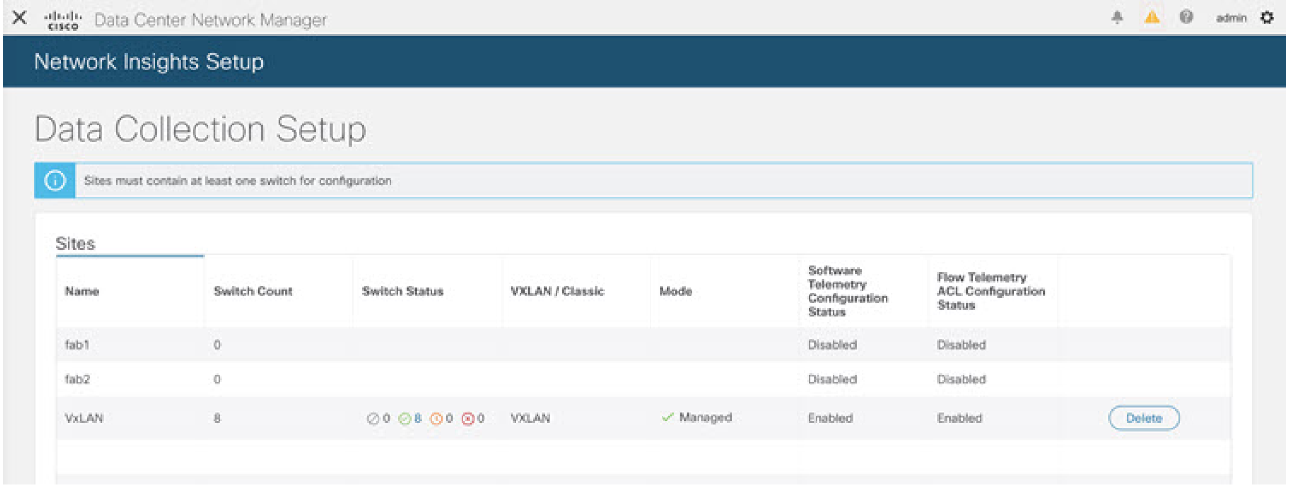
Page 1 of 1 1-1 of 1

Rule will be applied to all relevant switches

ocol	Source IP	Source Port	Destination IP	Destination Port
IPv4	0.0.0.0/0	*	0.0.0.0/0	*
IPv6	0::0/0	*	0::0/0	*

Page 1 of 1 1-2 of 2

6. Click **Settings** > **Network Insights Setup** > **Edit Configuration**. Once the status shows *Enabled* or *Enable Failed*, repeat Steps 4a and 4b.



Network Insights Setup

Data Collection Setup

Sites must contain at least one switch for configuration

Sites

Name	Switch Count	Switch Status	VXLAN / Classic	Mode	Software Telemetry Configuration Status	Flow Telemetry ACL Configuration Status	
fab1	0				Disabled	Disabled	
fab2	0				Disabled	Disabled	
VxLAN	8	⊘ 0 ✓ 8 ◷ 0 ⊗ 0	VXLAN	✓ Managed	Enabled	Enabled	Delete

Disable Telemetry on Cisco DCNM Site in Managed Mode

The following steps disable telemetry configuration on Cisco DCNM site in managed mode.

1. Click **Settings** > **Network Insights Setup** > **Edit Configuration** on the right top of Cisco NIR app.
2. Click **Delete** > **Apply** for the switch you want to disable telemetry. It disables software telemetry and flow telemetry for the switch.
3. The **Software Telemetry Configuration Status** shows *Disabling*, *Disabled*, or *Disable Failed* status.
4. Navigate to Fabric Builder UI screen.
   a. Verify that all switches display *In-Sync* status.
   b. Click **Save & Deploy**, if the switches display *Out-of-Sync* status.