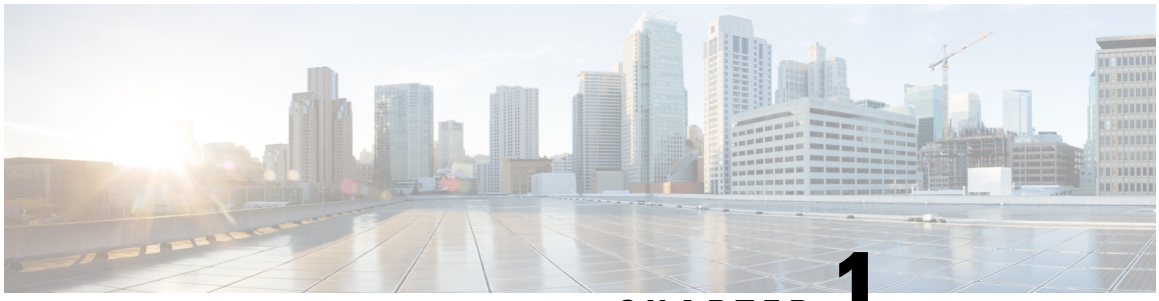
Cisco Network Insights for Resources Application for Cisco APIC User Guide, Release 2.1.x

First Published: 2019-12-13

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

CONTENTS



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

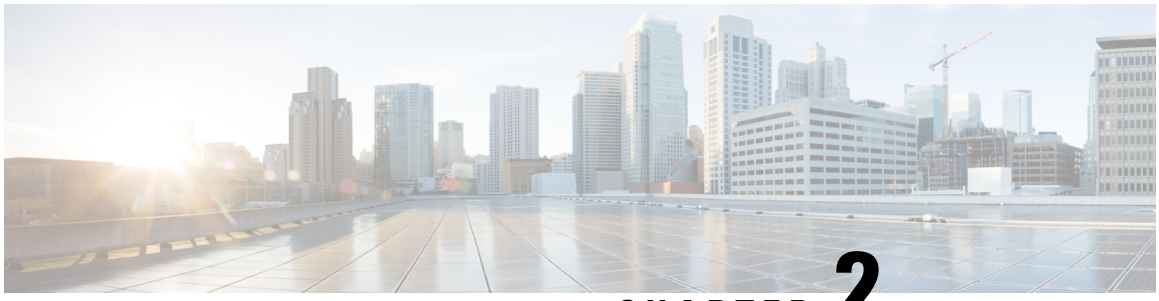
New and Changed Information

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 for Release 2.1.x

Feature	Description	Release
Endpoint Analytics (Beta)	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, and endpoints that do not get learnt back after a reboot. The Early Access Mode in the Network Insights Setup page lets the user enable beta Network Insights features and enhancements. Once the beta features are enabled they can not be disabled.	2.1.2
Anomaly Details enhancement	Support for Diagnostics, Recommendation, and Impact for Interface Anomalies.	2.1.2
UI enhancements	The UI enhancements in this release include cross launch navigation, the addition of top nodes in the dashboard, a fabric overview, and viewing of node details.	2.1.2
PC/vPC interface types	Support for PC/vPC interface types in the Interface Statistics tab.	2.1.2

Feature	Description	Release
BGP Statistics Telemetry	Support for BGP operational and statistical data in the Protocol Statistics tab.	2.1.2
Flow Telemetry enhancements	Support for Cisco Nexus FX, FX2, and EX switches.	2.1.2



CHAPTER 2

Cisco Network Insights for Resources Installation

This chapter contains the following sections:

About Cisco Network Insights for Resources

Cisco Network Insights for Resources (Cisco NIR) application consists of monitoring utilities that can be added to the Cisco Application Policy Infrastructure Controller (Cisco APIC). The application can also be added to the Cisco Application Services Engine with Cisco APIC.

Software Requirements

The following are software requirements for Cisco NIR on Cisco Application Services Engine with Cisco Application Policy Infrastructure Controller.

Table 2: Software Requirements for Cisco NIR on Cisco Application Services Engine with Cisco APIC

Software	Release
Cisco Application Policy Infrastructure Controller (Cisco APIC). Refer to Cisco APIC for details.	3.2(8) and 4.2(3)
Cisco Application Services Engine. Refer to Cisco Application Services Engine for details.	1.1.2i

Hardware Requirements

This section describes the Cisco ACI deployment requirements for Cisco NIR software telemetry.

The following are required for Cisco NIR application running on the Cisco Application Services Engine with Cisco APIC:

Table 3: Hardware Requirements for Cisco NIR on Cisco Application Services Engine with Cisco APIC

Feature	Hardware
Cisco Application Policy Infrastructure Controller (Cisco APIC)	Use existing Cisco APIC cluster M3 and L3
The Cisco Application Services Engine cluster	SE-CL-L3
Flow Telemetry	The following series switches and line cards are supported: • Cisco Nexus 9300-EX, -FX, -FX2, and 9500 platform switches • Cisco Nexus X9732C-EX line card

Downloading Cisco NIR Application from the Cisco App Center

This section contains the steps required to download Cisco NIR application in the Cisco APIC in preparation for installation.

Before you begin

You must have administrative credentials to download applications in the Cisco APIC.

Step 1 Log in to the Cisco APIC GUI with admin privileges.

- If you do not have admin privileges, log in to the Cisco App Center to download the application.

Step 2 Choose **Apps**.

Step 3 Click the **Download Applications** icon on the far-right side of the work pane.

A new browser tab or window opens to the Cisco App Center.

Step 4 Search for Cisco Network Insights for Resources application on the search bar.

Step 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.

Step 6 Review the license agreement and, if OK, click **Agree and download**.

The Cisco Network Insights for Resources application is downloaded to your local machine.

What to do next

Note the download location of the Cisco Network Insights for Resources file on your local machine. Make sure to move the downloaded Cisco Network Insights for Resources file to a http server, which can then be uploaded to Cisco Application Services Engine with Cisco APIC.

Installing Cisco NIR Application on Cisco APIC

This section contains the steps required to install Cisco NIR application on Cisco APIC. These steps are required for software telemetry.

Before you begin

You must have administrative credentials to install Cisco NIR application.

Step 1 Log in to the Cisco APIC GUI with admin privileges.

Step 2 Click the **Admin** > **Downloads** tab.

Step 3 Click the **Task** icon on the far-right side of the Downloads work pane and select **Add File to APIC**.
The **Add File to APIC** dialog appears.

Step 4 Enter the name of the download file in the **Download Name** field.

Step 5 In the **Protocol** field, choose **Secure Copy**.

Step 6 In the **URL** field, enter the path to the download file image location.

Step 7 Enter your name and password in the **Username** and **Password** fields.

Step 8 Enter **Submit**.

Step 9 Click the **Operational** tab and then click the **Refresh** icon to see the download status.

The application will automatically install once downloaded. This could take approximately five minutes to complete.

Step 10 After installing, click the **Operations** > **NIR** tab at the top of the GUI.

Once the application installation is completed, an application icon appears with the **Enable** button in green.

Step 11 Click **Enable** to open the application.
A Details dialog appears.

Step 12 Click **Enable**.

The application icon appears with a blue **Open** button.

Step 13 Click **Open**.

The application opens with a splash screen welcome dialog for Cisco NIR.

Step 14 Click **Begin First Time Setup** to setup the Cisco NIR application.

What to do next

Continue with the setup of the Cisco Network Insights for Resources application located in the Cisco NIR Initial Setup section.

Installing Cisco NIR on Cisco Application Services Engine with Cisco APIC

This section contains the steps required to install Cisco Network Insights for Resources application on the Cisco Application Services Engine with the Cisco APIC.

Before you begin

Before you begin installing a Cisco NIR application on the Cisco Application Services Engine with Cisco APIC, make sure the following requirements are met:

- You have installed and configured the Cisco Application Services Engine.
- You must have administrator credentials to install Cisco NIR application.

Step 1 Log in to the Cisco APIC GUI with admin privileges.

Step 2 Click **Admin** > **Downloads** tab on the top navigation bar.

Step 3 Click **Service Engine** from the tabs on the far-right side.

Step 4 Click the **Task** icon on the far-right side of the Downloads work pane and select **Add File to Service Engine**.

Step 5 In the **URL** enter the http address and click **Submit**.

Click **Refresh** icon on the far-right side of the Downloads work pane to check the upload status.

Step 6 Once the **Status** is completed then click the **Apps** tab.

The Cisco NIR application installation progress dialog appears.

Step 7 After installing, click the **Apps** tab.

Once the application installation is completed, the NIR icon appears with the **Enable** button in green.

Step 8 Click **Enable** to open the application.

A Details dialog appears.

Step 9 Click **Enable**.

The application icon appears with a blue **Open** button.

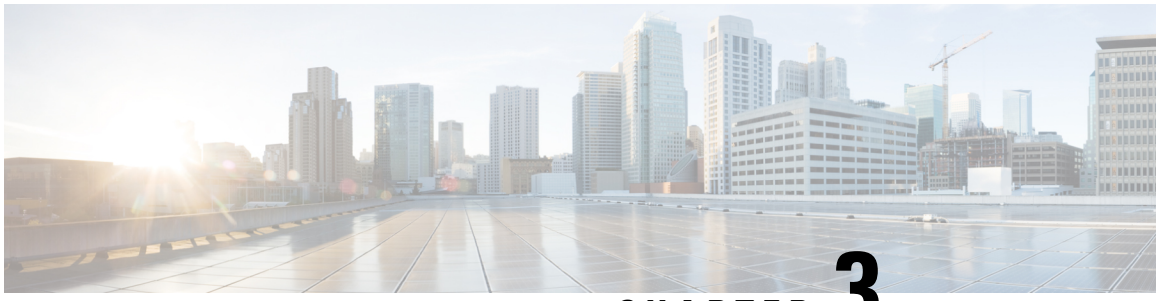
Step 10 Click **Open** from the Cisco NIR application dialog.

The application opens with a splash screen welcome dialog for Cisco NIR.

Step 11 Click **Begin First Time Setup** to setup the Cisco NIR application.

What to do next

Continue with the setup of the Cisco Network Insights for Resources application located in the Cisco NIR Initial Setup section of the next chapter.



CHAPTER 3

Cisco Network Insights for Resources Setup and Settings

This chapter contains the following sections:

Cisco Network Insights for Resources Components in Cisco APIC

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

The Cisco NIR application consists of the following components:

- **Data Collection**—The streaming of telemetry data is done by the Operating Systems on the fabric 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 a format that the analytics pipeline can understand and work upon.

  The following telemetry information collected from various nodes in the fabric to achieve the goal:

  - Resources Analytics—This includes monitoring software and hardware resources of fabric nodes on the Cisco APIC.
  - Environmental—This includes monitoring environmental statistics of hardware resources such as fan, CPU, memory, and power of the fabric nodes.
  - Statistics Analytics—This includes monitoring of nodes, interfaces, and protocols on the Cisco APIC and fabric nodes.

  - Flow Analytics—This includes monitoring of flows on the Cisco fabric nodes, detecting average latency, packet drop indication, and flow move indication across the entire Cisco ACI.
  - Endpoint Analytics—This includes monitoring endpoints on the Cisco fabric nodes for rapid endpoint moves, duplicate IP address, and endpoints that do not get learnt back after a reboot across the entire Cisco ACI.
  - Event Analytics—This includes monitoring of events, faults and configuration changes.

- **Resource Utilization and Environmental Statistics**—Resource analytics supports configuration, operational and hardware resources. Environmental covers CPU, memory, temperature, fan utilization, power, and storage related to the leaf nodes, spine nodes, and Cisco APIC. System analytics also covers anomalies, the trending information of each resource, and graphing of parameters, which help network operators debug nodes over periods of time.
- **Predictive Analytics and Correlation**—The value-add of this platform is predicting failures in the fabric and correlating internal fabric failures to the user-visible/interested failures.
- **Anomaly Detection**—Involves understanding the behavior of each component 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

- When fabric is upgraded and nodes are reloaded, disable and enable the Cisco NIR app for the application to load the latest data.

Cisco NIR Setup and Settings

Initial Setup

This section contains information required to set up the Cisco NIR application in the Cisco APIC.

Welcome to Network Insights

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

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

   The Network Insights Setup window appears.

2. Make sure the following fields are checked for the application. They are checked by default.
   - NTP and Time Zone Configuration
   - Inband IP Configuration

3. Toggle to disable or enable Flow Analytics.

4. 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.

1. Click **Get Started** to launch the application.

Settings

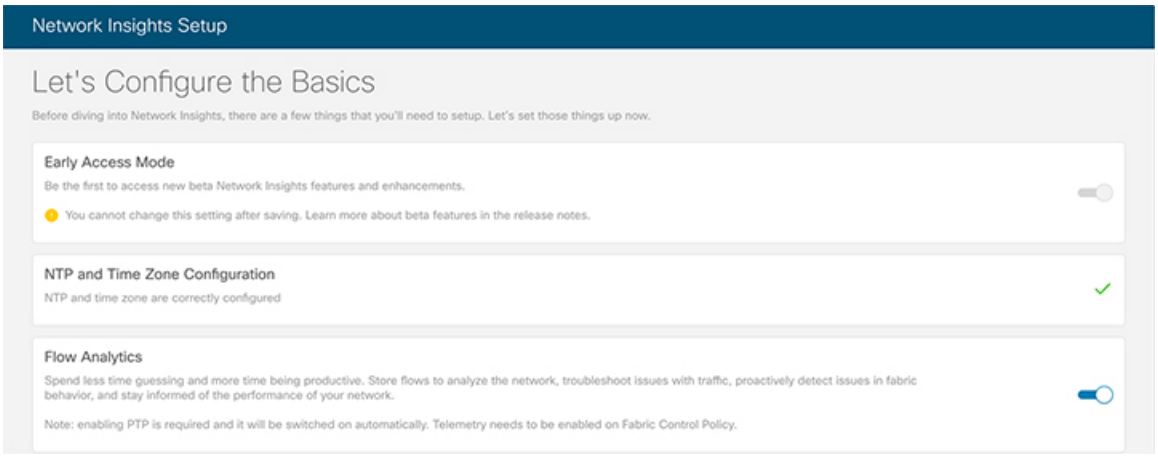
Once Cisco NIR is installed, if there are Faults present in the application, they will show on the **Faults** tab. To verify App functionality, click on the **Settings** icon and select **Service Status** . You should see green checks next to each service that is operating normally. In the **Settings** menu click **Collection Status**, you should see the green circles in the table indicating the nodes where information is being transmitted.

Property	Description
Time Range	Specify a time range and the tables below display the data that is collected during the specified interval.

Property	Description

	Clicking on this icon allows you to alter the following:
	• **Flow Collection Configuration**—Enable or disable flow collection and assign a previously configured inband management EPG. Create VRF and EPG collection rules per tenant:
	  • Click the **Plus** icon and enter the filter Name.
	  • Select a **Tenant**, and **VRF** from the drop-downs.
	  • Enter the subnet in the **Subnet** field and click **Add Subnet**.
	  • Click **Save**.
	Note To verify that **Flow Collection** has started, select **Collection Status**. On the **Collection Status** table, you should see the green circles indicating the nodes where the flows are being exported.
	• **System Status**—Displays service status of the flows, such as API Server, APIC Config Manager, Correlation Engine, Flow Manager, and Prediction Engine and Capacity Usage per node and Network Insights usage.
	• **Collection Status**—Displays if **Flow Collection** is functioning, you should see the green circles in the table indicating the nodes where the flows are being exported.
	• **Network Insights Setup**—Lets the user configure the Cisco NIR application setup and enable or disable Flow Analytics.
	• **Network Insights Setup**—Lets the user enable Early Access Mode and enable/disable Flow Analytics on **Network Insights Setup** page.
	The Early Access Mode lets the user enable beta Network Insights features and enhancements. Once the beta features are enabled, they can not be disabled.
	• **About Network Insights**—Displays the Cisco NIR application version.

The following is an example for **Network Insights Setup** configuration page.



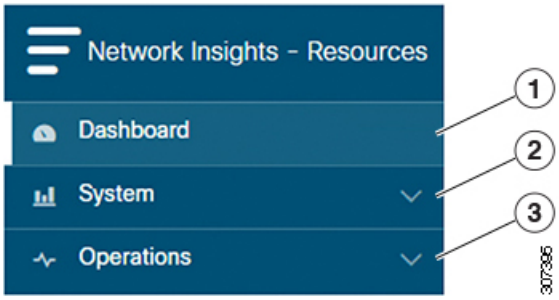
The Early Access Mode lets the user enable beta Network Insights features and enhancements. Once the beta features are enabled, they can not be disabled.

Navigating Cisco NIR

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

Navigation Pane

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

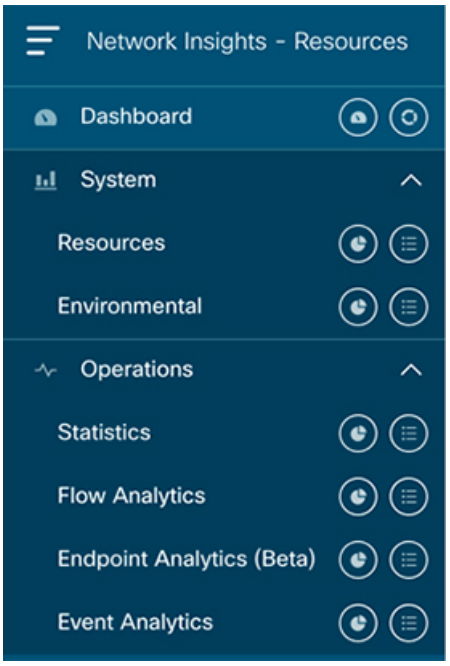


1 Dashboard: The main dashboard for the Cisco NIR application providing immediate access to anomalies.

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

3 Operations: Statistics information for interfaces and protocols, flow analytics for viewing average latency, flow move indicator, and packet drops, and event analytics for viewing audit logs, events and faults.

Expanding System and/or Operations reveals additional functions:



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

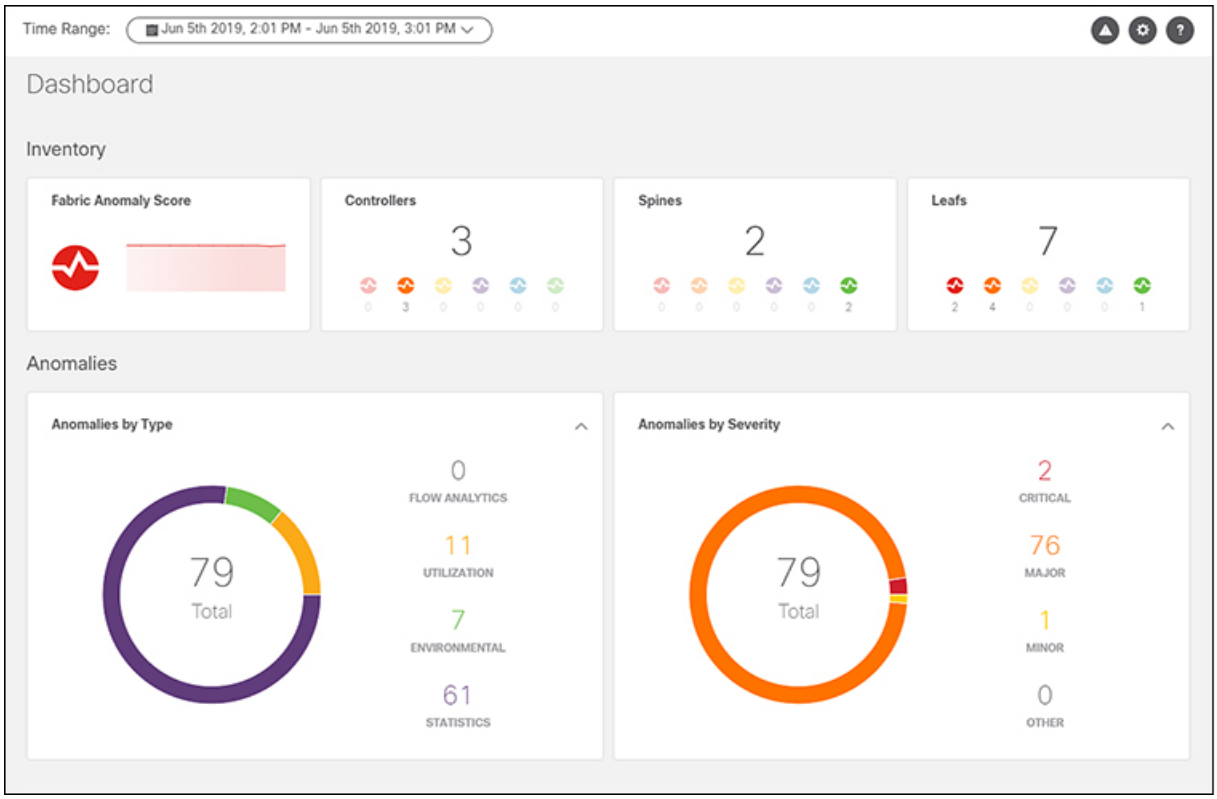
2 Browse View icon: Provides a detailed view of returned data for the selected telemetry type and allows for filtering to further isolate problem areas.

Work Pane

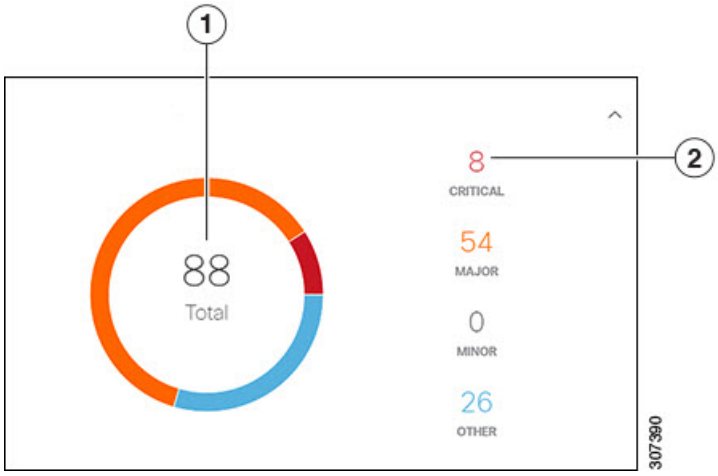
The work pane is the main viewing location in the Cisco NIR application. All information tiles, graphs, charts, and lists appear in the work pane.

Dashboard Work Pane

This is an example of the Cisco NIR Dashboard work pane:



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:

Start Time	End Time	Severity	Resource Type	Nodes	Description
May 16 2019 12:14:25pm	May 16 2019 07:54:37pm	Critical	config	N9Kv-2	Number of VRFs is above critical threshold (Usage : 991, Critical-Threshold : 900)
May 16 2019 12:14:53pm	May 16 2019 07:55:08pm	Critical	environmental	N9Kv-7	[Outlet Sensor] : Temperature is above critical threshold (Current Value : 75 C, Critical-Threshold : 72 C)
May 16 2019 12:14:17pm	May 16 2019 07:54:28pm	Critical	environmental	N9Kv-1	[Outlet Sensor] : Temperature is above critical threshold (Current Value : 75 C, Critical-Threshold : 72 C)

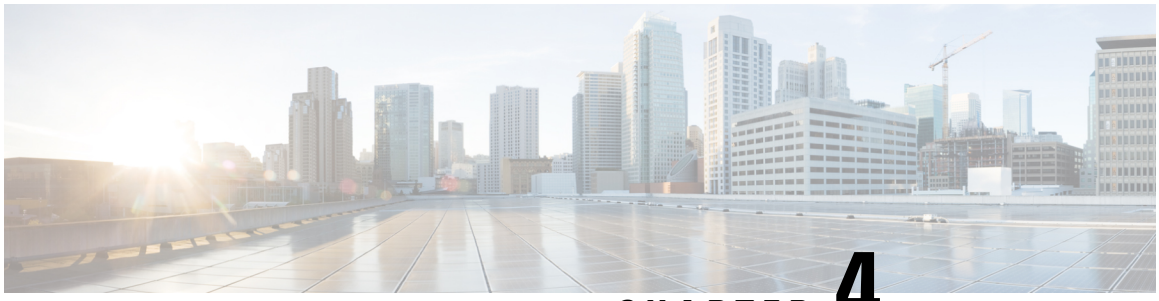
307391

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.



CHAPTER 4

Using Cisco Network Insights for Resources

This chapter contains the following sections:

Using the Cisco Network Insights for Resources Application

Each Cisco Application Centric Infrastructure (Cisco ACI) switch streams telemetry events from the fabric to the Cisco NIR app which then analyzes the events and proactively detects issues in the fabric behavior. Use the dashboards in the Cisco NIR application to view relevant information and select specific items to view details.

Cisco NIR Dashboard

The Cisco Network Insights for Resources (Cisco NIR) application 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, flow anomalies, and interface and protocol-level errors. Anomaly scores are color coded based on severity:

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

In the controllers/spines/leaves 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.

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
Fabric Anomaly Score	Displays the health of the fabric through the anomaly score.
Controllers	Displays the total number of Cisco APICs in the fabric.
Spines	Displays the total number of spine nodes in the fabric with anomalies.
Leafs	Displays the total number of leaf nodes in the fabric with anomalies.

Click Controllers, Spines, and Leafs to view the details of the individual nodes in the fabric from **Browse Nodes** work pane.

Browse Nodes

The Browse Nodes pane displays the graph with top nodes based on Resource Utilization, Environmental, Statistics, End Point Analytics, and Flow Anamoly, which are various ways of viewing the behavior of the nodes. The page also dispalys the overview of the individual nodes in the fabric with node name, switch models, node type and other details. Click **Node** for the node detail view. The **Node Overview** section dispalys the top five nodes based on Resource Utilization, Environmental, Flow analytics, and Endpoint 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 nodes based on Resource Utilization, Environmental, Statistics, and Flow Analytics, which are various ways of viewing the behavior of the nodes. The page also dispalys the overview of the individual nodes in the fabric with node name, switch models, node type and other details. Click the **Node** for the node summary pane to dispaly all the gathered information for the selected node.

Click the icon 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 dispalys the top five nodes based on Resource Utilization, Environmental, 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, Endpoint Analytics, Events, 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.

Dashboard Anomalies

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

Property	Description
Anomalies by Type	Displays the number of Anomalies by their type. Anomaly types include: • Flow Analytics • Utilization • Environmental • Statistics • Endpoints
Anomalies by Severity	Displays the number of Anomalies (internal Fabric 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 Type 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 dispalys the overview of the individual nodes in the fabric with severity, resource type, node name, description, cleared, acknowledged and other details. Double-click the anomaly for the anomaly details. The **Anomaly Details** page displays the description of the anomaly, recommendations to resolve the anamoly, and estimated impact with a report on the interfaces, and applications that were affected. Click **View Report** to see the details of the interfaces that were affected.

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, Endpoint Analytics, Events, 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.

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:

- Start Time - Display only anomalies with a specific start time.
- End Time - Display only anomalies with a specific end time.
- Description - Display only anomalies with a specified description.

- 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.
- Acknowledged - Do not display the selected anomaly when checked to **T** for 20 minutes.

For the 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.
- < - with the initial filter type, this operator, and a subsequent value, returns a match less than the value.
- <= - with the initial filter type, this operator, and a subsequent value, returns a match less than or equal to the value.
- > - with the initial filter type, this operator, and a subsequent value, returns a match greater than the value.
- >= - with the initial filter type, this operator, and a subsequent value, returns a match greater than or equal to the value.

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.

Browse Dashboard

The browse view icon on the Cisco NIR navigation pane for Dashboard dispalys an overview of the fabric, nodes in the fabric, and its connections. This page lets you show or hide Lines, Names, Spines, Leaf, Controller, and different types of nodes based on the anomaly score. Click the node to show the summary pane.

Cisco NIR System

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

- **Resources**—Fabric component capacity information.
- **Environmental**—Hardware component capacity information.

System Resources

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

Resources Dashboard

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

Property	Description
APIC Capacity	Displays operational capacity for Cisco APIC objects in the fabric.
Top Nodes by Utilization	Displays the top nodes based on anomaly score from resource utilization.

Browse Resources

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

Filters

You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

A 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.

Property	Description
Top Nodes by	Displays the top nodes by: • MAC (learned) • IPv4 (learned) • IPv6 (learned) • IPv4 Host Routes • IPv6 Host Routes • Multicast Routes • Endpoint Group • Bridge Domain • VLAN • VRF • Port Usage • Ingress Port Bandwidth • Egress Port Bandwidth • LPM • Policy TCAM
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 • IP v6 Host Routes • Multicast Routes

Property	Description
Configuration Resources	Displays a list of configuration resources based on resource utilization. List information includes: • Anomaly Score • Node • VRF • BD • EPG • 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

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: • Memory • Temperature • Storage • Fan Utilization • Power Supply • CPU

Browse Environmental Resources

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

Filters

You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

A 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.

Property	Description
Top Nodes by	Displays a graph of the top nodes by: • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage
Environmental Resources (table)	Displays a list of the top node by anomaly score. Table columns include: • Anomaly Score • Node • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage

Cisco NIR Operations

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

- **Statistics**—Switch nodes interface usage and protocol statistics.
- **Flow Analytics**—Telemetry information collected from various devices in the fabric.
- **Endpoint Analytics**—Displays endpoint anomalies for the nodes collected across the entire fabric.
- **Event Analytics**—Displays charts for event occurrences over time.

Statistics Analytics

The Statistics Analytics 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 Interface	Displays the top nodes and lists the transmit and receive bandwidth utilization for each of it's interfaces.

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 the following filters:

- Node - Display only nodes.
- Interface - Display only interfaces.
- Protocol - Display only protocols.
- Interface Type - Displays the interface type based on protocol.
- Operational State - Displays the interface active state.
- Admin State - Displays the interface enabled state.

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.

Property	Description
Top 10 Interfaces by	Displays the top interfaces by: • Transmit Utilization • Receive Utilization • Error
Interface Statistics	Displays a list of interface statistics that are sorted by anomaly score. List information includes: • Anomaly Score • Interface • Type • Node • Receive Utilization • Transmit Utilization • Errors
Protocol Statistics	Displays a list of protocol statistics that are sorted by anomaly score. List information includes: • Anomaly Score • Protocol • Type • Node • Number of Interfaces • Errors

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 **type > physical** for interface details of the node such as, 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 statistically chaneled or can be dynamic using LACP protocols. The statistical data that collects the counters for packets, bytes and various errors are similar to that of physical interface. 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 **type > pc** for interface 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 accross two physical switches for fault tolerance. Double-click **type > vpc** for interface details of the node such as, 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.

Protocol Statistics

The Browse Statistics dashboard displays protocol statistics for the top interfaces by anomalies for nodes that are of type CDP, LLDP, LACP, and BGP protocol. 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.

Double-click **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 **Neighbor** node for the **Neighbor Details** window to popup with more details.

Double-click **protocol > CDP**, **protocol > LLDP**, or **protocol > 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.

Browse Statistics Limitations

The following are Cisco NIR application limitations for Interface Statistics.

- Interface Statistics does not support *eqptIngrCrcErrPkts5min* counter.

Flow Analytics

The Flow Analytics section of the Cisco NIR application displays the telemetry information collected from various devices in the fabric.

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 Pre-requirements

The following are required for Cisco NIR application running on the Cisco Application Services Engine with Cisco APIC:

- The Flow Analytics for Cisco NIR application requires you to install Cisco Application Services Engine. Refer to Cisco Application Services Engine for details.
- For details on Flow Telemetry support for Cisco Nexus series switches and line cards, see Hardware Requirements, on page 3.

Flow Analytics Limitations

The following are Cisco NIR application limitations for Flow Analytics on **Cisco Nexus EX** switches. For details on Flow Telemetry hardware support, see Hardware Requirements, on page 3.

- Output port information for outgoing traffic from N9K-C93180YC-EX, N9K-C93108TC-EX, N9K-C93180LC-EX, and N9K-X9732C-EX line cards will not be displayed.
- The burst information for N9K-C93180YC-EX, N9K-C93108TC-EX, N9K-C93180LC-EX, and N9K-X9732C-EX line cards will not be displayed.
- The EPG names will reflect after few minutes of flow capture and after enabling the flow analytics. This information is fetched from the software and not from the EX ASIC.
- The L3out external EPG names, Buffer drop anomaly, Forwarding drop anomaly, and QoS (Policing) drop anomaly are not suported.

The following are Cisco NIR application limitations for Flow Analytics on **Cisco Nexus FX** switches.

- The Cisco NIR application supports all IP sizes, but shows it different from actual IP size. For example, for 1000 bytes of IP packet size:
  - For ipv4 inter-leaf traffic (with spine), the Cisco NIR app shows Ingress IP size of 1050 bytes and Egress IP size of 1108 bytes. For ipv4 intra-leaf traffic the Cisco NIR app shows both Ingress and Egress IP size of 1050 bytes.
  - For ipv6 inter-leaf traffic (with spine), the Cisco NIR app shows Ingress IP size of 1070 bytes and Egress IP size of 1128 bytes. For ipv4 intra-leaf traffic the Cisco NIR app shows both Ingress and Egress IP size of 1070 bytes.
- The Cisco NIR app captures the maximum anomaly score for a particular flow, for the entire cycle of the user specified time range.

Flow Analytics Dashboard

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

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 ASIC hardware and converts the 5-tuples to user-understandable EPG-based flow records. Top nodes by flow anomalies displays the nodes in the network with the most anamolies. The details include, type of alarm, source destination, packet drops and latency.

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

Browse Flows

The Browse Flows page dispalys the active nodes, ingress nodes, egress nodes, and flow collection filters, which display the anomalies in the behavior of fabric nodes.

Property	Description
Nodes	Active nodes are leaf nodes and spines that show the anomaly score for the top nodes by flow anomalies.
Ingress Nodes	Dispalys the Ingress node name and tenant that show the top nodes by flow anomalies.
Egress Nodes	Dispalys the Egress node name and tenant that show the top nodes by flow anomalies.
Filters	Display the node flow observations sorted by the following filters: • Timestamp • Ingress Nodes • Egress Nodes • Source EPG • Source Address • Source Port • Destination EPG • Destination Address • Destination Port • Address Type • Protocol

Property	Description
Top 10 flows by	Lists the top 10 flows that scored highest in the following: • **Anomaly Score**—The score is based on the number of detected anomalies logged in the database. • **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 fabric. **Note** A prerequisite for fabric 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 Cisco ACI leaf node to another. The first ARP/RARP or regular packet sent by that endpoint appears as a flow entering the fabric through the new Cisco ACI leaf node.

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

Endpoint Analytics

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

Endpoint Analytics Overview

Endpoint Analytics provides detailed analytics of endpoints learnt in the fabric 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 fabric 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 missing endpoints that fail to get learnt after a node reboot.
- 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 fabric.

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 health of each node with endpoint anomalies.

Browse Endpoint Analytics

Browse Endpoint Analytics displays the list of endpoints that are sorted by anomaly score.

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

- Tenant - Displays nodes with tenant name.
- VRF - Displays nodes with IP address.
- BD - Displays nodes with domain id.
- EPG/l3 out - Displays nodes with entity type - L3out or EPG (L2 endpoint).
- MAC Address - Display nodes with MAC address.
- Nodes - Display only nodes.
- Interface - Display only interfaces.
- IP address - Display nodes with IP address.
- 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.

Browse Endpoints	Description
Top 10 Endpoints by Anomaly Score	Displays the top endpoints based on the time series information collected for number of endpoints. Dispalys the following: • Endpoint • Anomaly Score
Table of Endpoints	Displays a list of endpoints that are sorted by anomaly score. List information includes: • Anomaly Score • Tenant • VRF • BD • EPG/l3 out • MAC Address • IP Address • Nodes • Interface • Status • Time

Endpoint Details

Double-click the endpoint in the table to open a **Endpoint Details** page. The **Endpoint Details** page displays general information about the endpoint based on configuration and operation of the endpoint. The configuration section displays the Tenant, EPG, BD, VRF, and Encap details for the selected endpoint. The operational section displays the Node name, Interface, VM name and id, hypervisor id, Rogue (endpoints that move often) and other details.

This page also lists the **Anomalies**, **Endpoint History**, and **Duplicates** sections. The endpoints in the fabric may move to many places. The **Endpoint History** lists in decrease order of when the endpoint was updated. It also lists the endpoint movement in the fabric for an IP address at a particular time. **Duplicates** section lists the MAC address of the node that was part of duplicate IP address.

Event Analytics

The Operations Event Analytics section of the Cisco NIR application displays charts for event occurrences information for top switch nodes.

Event Analytics Dashboard

The Event Analytics Dashboard displays charts for event occurrences over time, audit logs by action, and events/faults by severity.

Property	Description
Event Analytics by time	Displays all audit logs, events, and faults over a timeline chart. To modify the timeline, go to Time Range at the top of the work pane.
Audit Logs by Actions	Displays all audit logs based on the action performed. The audit log records actions performed by users, including direct and indirect actions. Each entry in the audit log represents a single, non-persistent action. For example, if a user logs in, logs out, or creates, modifies, or deletes an object such as a service profile, the switch manager adds an entry to the audit log for that action.
Events by Severity	Displays all events by severity. An event is an immutable object that is managed by the switch manager. Each event represents a non-persistent condition in the instance. After the event is created and logged, the event does not change. For example, if you power on a server, the switch manager creates and logs an event for the beginning and the end of that request.
Faults by Severity	Displays all faults by severity. A fault is represented as mutable, stateful, and persistent Managed Object (MO). When a failure occurs or an alarm is raised, the system creates a fault MO as a child object to the MO that is primarily associated with the fault. For a fault object class, the fault conditions are defined by the fault rules of the parent object class. Each fault includes information about the operational state of the affected object at the time the fault was raised. If the fault is transitional and the failure is resolved, then the object transitions to a functional state.

Browse Audit Logs, Events & Faults

View, sort, and filter audit logs, events, and faults through the Browse Audit Logs, Events & Faults work pane.

Filters

You can refine the displayed statistics by the following filters:

- Creation Time - Display only logs, events, and failures for a specific date.
- Type - Display only logs, events, and failures for the specified type.
- Severity - Display only logs, events, and failures for the specified severity.
- Action - Display only logs, events, and failures for the specified action type. This filter applies to audit logs.
- Node - Display only logs, events, and failures for the specified node name.
- Affected Object - Display only logs, events, and failures for the specified managed object.
- Description - Display only logs, events, and failures for the specified description.
- Record ID - Display only logs, events, and failures for the specified record ID.

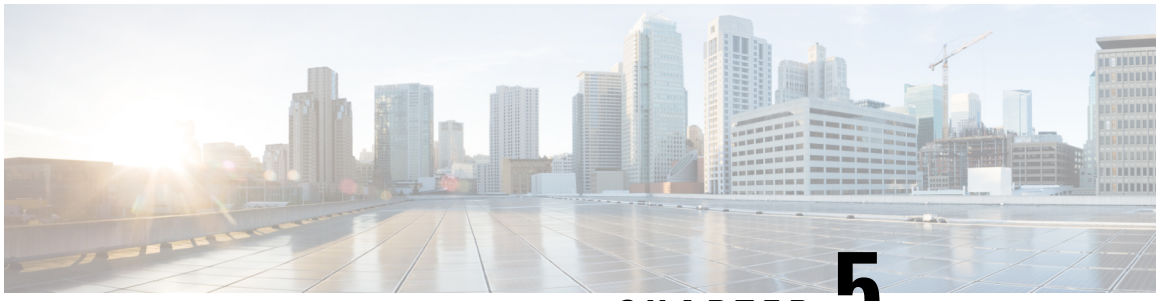
As a filter refinement, use the following operators:

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

- Audit Log (Type) - Display only audit logs.
- Event (Type) - Display only events.
- Fault (Type) - Display only faults.
- Cleared (Severity) - Display only cleared events and faults.
- Info (Severity) - Display only informational events and faults.
- Warning (Severity) - Display only warning events and faults.
- Minor (Severity) - Display only minor events and faults.
- Major (Severity) - Display only major events and faults.
- Critical (Severity) - Display only critical events and faults.
- Creation (Action) - Display only created audit logs.
- Deletion (Action) - Display only deleted audit logs.
- Modification (Action) - Display only modified audit logs.

Property	Description
Audit Logs by Action	Displays audit logs by: • Deletion • Creation • Modification
Events by Severity	Displays all events based on severity: • Critical • Major • Minor • Other

Property	Description
Faults by Severity	Displays all faults based on severity: • Critical • Major • Minor • Other



CHAPTER 5

Upgrade Cisco Network Insights for Resources

This chapter contains the following sections:

Upgrade Cisco NIR on Cisco Application Services Engine with Cisco APIC

This section contains the steps required to upgrade Cisco Network Insights for Resources application on the Cisco Application Services Engine with the Cisco APIC.

Before you begin

Before you begin upgrading a Cisco NIR application on the Cisco Application Services Engine with Cisco APIC, make sure the following requirements are met:

- You must have administrator credentials to upgrade Cisco NIR application.
- You **do not** remove the current Cisco NIR application on the Cisco Application Services Engine.

Step 1 Follow steps 1 to 5 from Installing Cisco NIR on Cisco Application Services Engine with Cisco APIC, on page 6.

Step 2 Once the **Status** is completed then click the **Apps** tab.

The Cisco NIR application upgrading progress dialog appears.

Step 3 Click **Open** from the Cisco NIR application dialog.

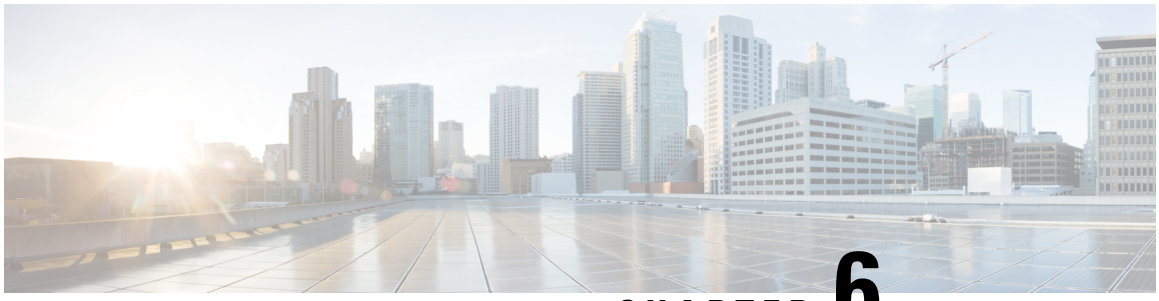
This upgrade procedure preserves the user data from the previous installation.

Upgrade Paths for Cisco NIR Application

The following table lists the supported upgrade paths for Cisco NIR application.

Table 4: Supported Upgrade Paths for Cisco Network Insights for Resources Application

From	To
Cisco NIR on Cisco Application Services Engine via Cisco APIC 2.1.1	Cisco NIR on Cisco Application Services Engine via Cisco APIC 2.1.2



CHAPTER 6

Cisco NIR REST API Examples

This chapter contains the following sections:

all_resources()

```
Get all resources  .
REST URL   :
   GET /api/telemetry/utilization/resources.json
Parameters :
   None
Example    :
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/utilization/resources.json'
Cisco NIR app installed on Cisco Application Services Engine:
```

```
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 /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 :
Cisco NIR app installed on Cisco APIC:
    curl -ksb -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/anomalies/details.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 /api/telemetry/anomalies/summary.json
Parameters :
   startTs  (optional) => Start timestamp, default:now-1h
   endTs    (optional) => End timestamp, default:current-time
Example :

Cisco NIR app installed on Cisco APIC:
    curl -ksb -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/anomalies/summary.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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
            }
        ]
    }
```

events_buckets()

```
Get the Events, Audit Logs and Faults count
REST URL   :
    GET /api/telemetry/events/buckets.json
Parameters :
    startTs (mandatory) => Start timestamp
    endTs               => End timestamp, default:current-time
    granularity         => Granularity, default:1 sec
Example    :
```

```
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/events/buckets.json'
Cisco NIR app installed on Cisco Application Services Engine:
    curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/api/api/telemetry/events/buckets.json'
Response   :
    {
        "totalItemsCount": 3,
        "totalResultsCount": 3,
        "entries": [
            {
                "eventType": "auditLog",
                "entries": [
                    {
                        "startTs": "2018-08-10T17:52:16.000Z",
                        "endTs": "2018-08-10T17:52:16.999Z",
                        "ts": "2018-08-10T17:52:16.499Z",
                        "recordId": null,
                        "recordCount": 3
                    },
                    {
                        "startTs": "2018-08-10T17:52:40.000Z",
                        "endTs": "2018-08-10T17:52:40.999Z",
                        "ts": "2018-08-10T17:52:40.499Z",
                        "recordId": null,
                        "recordCount": 29
                    }
                ],
                "recordCount": 32
            },
            {
                "eventType": "event",
                "entries": [
                    {
                        "startTs": "2018-08-10T17:52:14.000Z",
                        "endTs": "2018-08-10T17:52:14.999Z",
                        "ts": "2018-08-10T17:52:14.499Z",
                        "recordId": "bld1",
                        "recordCount": 1
                    }
                ]
                "recordCount": 1
            }
    }
```

events_details()

```
Get the Events, Audit Logs and Faults detailed info
REST URL   :
   GET /api/telemetry/events/details.json
Parameters :
    startTs (mandatory) => Start timestamp
    endTs               => End timestamp, default:current-time
    filter              => Lucene format filter, default:null
    offset              => Time offset, default:0
Example    :
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/events/details.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/api/api/telemetry/events/details.json'
```

```
Response   :
    {
         "totalItemsCount": 233971,
         "totalResultsCount": 233971,
         "offset": 0,
         "entries": [
            {
                "ack": false,
                "rule": "tca-l2-ingr-bytes5min-drop-rate",
                "lifecycle": "raised",
                "code": "F110176",
                "digest": "l3EncRtdIfF110176",
                "faultType": "operational",
                "highestSeverity": "warning",
                "occurrences": 1,
                "recordId": "bld115",
                "cause": "threshold-crossed",
                "changeSet": [
                    {
                        "oldValue": "",
                        "propertyName": "dropRate",
                        "newValue": "52039"
                    }
                ],
                "subject": "counter",
                "severity": "warning",
                "eventType": "fault",
                "severityId": 2,
                "prevSeverity": "warning",
                "contextClass": "l3EncRtdIf",
                "contextDn": "sys/inst-overlay-1/encrtd-[eth11/7.231]",
                "eventId": 0,
                "origSeverity": "warning",
                "domain": "infra",
                "nodeType": "switch",
                "delegatedFrom": "",
                "modType": "modification",
                "nodeName": "spine1",
                "displayNodeName": "spine1",
               "description": "TCA: ingress drop bytes rate(l2IngrBytes5min:dropRate) value
 52039 raised above threshold 10000",
                "createTime": "2018-08-10T17:55:13Z",
                "isDelegated": false
            }
     ]
}
```

events_summary()

```
Get the Events, Audit Logs and Faults summary
REST URL   :
   GET /api/telemetry/events/summary.json
Parameters :
    startTs (mandatory) => Start timestamp
    endTs               => End timestamp, default:current-time
    filter              => Lucene format filter, default:null
Example    :
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/events/summary.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/api/api/telemetry/events/summary.json'
```

```
Response   :
    {
        "totalItemsCount": 3,
        "totalResultsCount": 3,
        "entries": [
            {
                "eventType": "fault",
                "totalCount": 145516,
                "entries": [
                    {
                        "severity": "warning",
                        "count": 83190
                    },
                    {
                        "severity": "cleared",
                        "count": 57196
                    },
                    {
                        "severity": "critical",
                        "count": 4710
                    },
                    {
                        "severity": "major",
                        "count": 420
                    }
                ]
            },
            {
                "eventType": "event",
                "totalCount": 4,
                "entries": [
                    {
                        "severity": "info",
                        "count": 4
                    }
                ]
            },
            {
                "eventType": "auditLog",
                "totalCount": 2,
                "entries": [
                    {
                        "action": "creation",
                        "count": 2
                    }
                ]
            }
        ]
    }
```

flows_details()

```
Get detailed flows
REST URL   :
   GET /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:
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/flows/details.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 flows.
REST URL   :
   GET /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:

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/flows/summary.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 flows top flows.
REST URL   :
   GET /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:

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/flows/topFlows.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 flows top nodes.
REST URL   :
   GET /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:

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/flows/topNodes.json'

Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 fabric anomaly summary.
REST URL   :
    GET /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    :

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/fabricsSummary.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 fabrics list.
REST URL   :
    GET /api/telemetry/fabrics.json
Parameters :
    filter              => Lucene format filter, default:null
Example    :
Cisco NIR app installed on Cisco APIC:
    curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/fabrics.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET 'https://<ip:port>/sedgeapi/v1/cisco-nir/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 nodes list.
REST URL   :
    GET /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    :

Cisco NIR app installed on Cisco APIC:
    curl -k -i -XGET 'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/nodes.json
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET 'https://<ip:port>/sedgeapi/v1/cisco-nir/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 Stats details.
REST URL   :
   GET /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    :

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
```

```
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/protocols/details.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 Stats resources.
REST URL   :
   GET /api/telemetry/protocols/resources.json
Parameters :
   filter              => Lucene format filter, default:null
   fabricName          => limit the records pertaining to this fabricName
Example    :
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/protocols/resources.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 Stats topEntities.
REST URL   :
   GET /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    :
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/protocols/topEntities.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 Stats topNodes.
REST URL   :
   GET /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    :

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/protocols/topNodes.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 health dianostics.
REST URL   :
```

```
   GET /api/telemetry/health/collectionStats.json
Parameters :
   None
Example    :

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/health/collectionStats.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 /api/telemetry/health/serviceHealth.json
Parameters :
   None
Example    :

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/health/serviceHealth.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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-->
```

```
        ]
    }
```

utilization_node_details()

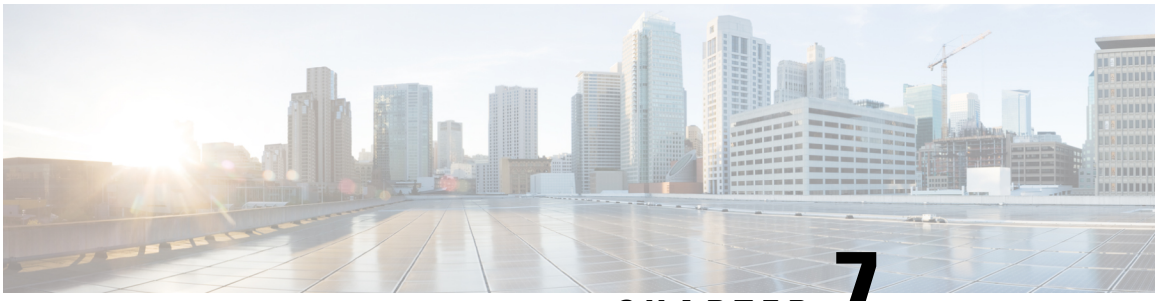
```
Get node details .
REST URL   :
   GET /api/telemetry/utilization/nodeDetails.json
Parameters :
   None
Example    :

Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/utilizationnodeDetails.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 /api/telemetry/utilization/topNodes.json
Parameters :
   None
Example    :
Cisco NIR app installed on Cisco APIC:
   curl -k -i -XGET
'https://<ip:port>/appcenter/Cisco/NIR/api/telemetry/utilization/topNodes.json'
Cisco NIR app installed on Cisco Application Services Engine:
   curl -k -i -XGET
'https://<ip:port>/sedgeapi/v1/cisco-nir/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 -->
        }
    ]
}
```



CHAPTER 7

Troubleshooting Cisco NIR Application

This chapter contains the following sections:

Troubleshooting Cisco NIR Common GUI Issues

The following are troubleshooting tips for GUI issues on Cisco NIR app in Cisco DCNM .

- 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. The 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 a spinner then this means almost none of the APIs are responding.
- If the Cisco NIR GUI page is taking a while to load fabrics then this means the `fabrics.json` API is not responding or not returning any fabrics.
- If the fabric anomaly score does not agree with reported anomalies, or the node counts are incorrect, then check the `fabricsSummary.json` response for the fabric `anomalyScore` value, and check the `nodes.json` response for the types and counts of nodes reported.

- If the expected fabrics are not shown in the fabric 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 fabrics. Make sure the appropriate fabrics 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 fabric 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 > fabric > 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.

Total Audit Logs, Events, and Faults

Faults

If faults occur within the application, they can be viewed from the Warning icon at the top-right of Application GUI screen next to the Settings icon.

Table 5: Total Audit Logs, Events, and Faults

Property	Description
Creation Time	The day and time of when the audit log, event, or fault instance occurred.

Property	Description
Severity	The current severity level of the event. The levels are: • **Critical**—A service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service and its capability must be restored. • **Major**—Serious problems exist with one or more components. These issues should be researched and fixed immediately. • **Minor**—Problems exist with one or more components that might adversely affect system performance. These issues should be researched and fixed as soon as possible before they become a critical problem. • **Warning**—Potential problems exist with one or more components that might adversely affect system performance if they are allowed to continue. These issues should be researched and fixed as soon as possible before they become a critical problem. • **Info**—A basic notification or informational message, possibly independently insignificant. • **Cleared**—A notification that the condition that caused the fault has been resolved, and the fault has been cleared.
Code	The code that helps to categorize and identify different types of fault instance objects.
Last Transition	The day and time on which the severity last changed. If the severity has not changed, this field displays the original creation date.
Description	Additional descriptive information on the audit log, event or fault.

Basic Debugging Commands

```
apic-ifc1# acidiag scheduler status
Scheduler status:
 [True]    APIC-01
 [True]    APIC-02
 [True]    APIC-03

apic-ifc1# acidiag scheduler members

 ID            Name    Status        Address      OOBAddress    Type       Serial  NodeFqdn
--------------------------------------------------------------------------------------------

  1*     apic-ifc1    active        10.0.0.1   172.1.2.3    Apic  FCH1748V24D
apic-ifc1.node.ifav22.apic.local
  2      apic-ifc2    active        10.0.0.2    172.4.5.6    Apic  FCH1809V18S
apic-ifc2.node.ifav22.apic.local
  3      apic-ifc3    active        10.0.0.3    172.7.8.9    Apic  FCH1809V191
apic-ifc3.node.ifav22.apic.local

apic-ifc1#
apic-ifc1# acidiag scheduler appstatus
```

```
Job                                 Type         Status
-----------------------------------------------------
Cisco_NIR
 `-Cisco_NIR-ClusterService         service      running
 `-Cisco_NIR-SystemService          system       running
bird_kafka
 `-bird_kafka-kafka                 system       running
bird_kafkax
 `-bird_kafkax-kafka                system       running
bird_zk
 `-bird_zk-zk                       service      running
elastic
 `-elastic-systemjob                system       running
elasticx
 `-elasticx-systemjob               system       running

apic-ifc1# acidiag scheduler appstatus bird_kafka

Container            Group                                  Node             Status
  Modified             Image
-------------------------------------------------------------------------------------------------

kafka                bird_kafka-kafka.kafka                 apic-ifc3      running
0d 19h 37m 16s       apic-system/kafka:0.1.0
kafka                bird_kafka-kafka.kafka                 apic-ifc1      running
0d 19h 37m 16s       apic-system/kafka:0.1.0
kafka                bird_kafka-kafka.kafka                 apic-ifc2      running
0d 19h 37m 16s       apic-system/kafka:0.1.0

apic-ifc1# acidiag scheduler appstatus elastic

Container            Group                                  Node             Status
  Modified             Image
-------------------------------------------------------------------------------------------------

es                   elastic-systemjob.db                   apic-ifc1      running
0d 19h 41m  8s       apic-system/elastic:v1
es                   elastic-systemjob.db                   apic-ifc3      running
1d 13h  2m 52s       apic-system/elastic:v1
es                   elastic-systemjob.db                   apic-ifc2      running
1d 13h 13m 15s       apic-system/elastic:v1

apic-ifc1# acidiag scheduler appstatus Cisco_NIR

Container            Group                                  Node             Status
  Modified             Image
-------------------------------------------------------------------------------------------------

app-brain            Cisco_NIR-ClusterService.brain         apic-ifc2      running
0d 18h 58m 53s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/brain:v1-0-1-827
app-scheduler        Cisco_NIR-ClusterService.scheduler     apic-ifc1      running
0d 18h 58m 54s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/scheduler:v1-0-1-827
app-correlator       Cisco_NIR-ClusterService.correlator    apic-ifc3      running
0d 18h 58m 53s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/correlator:v1-0-1-827
app-predictor        Cisco_NIR-ClusterService.predictor     apic-ifc3      running
0d 18h 58m 53s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/predictor:v1-0-1-827
app-apicagent        Cisco_NIR-ClusterService.apicagent     apic-ifc2      running
0d 18h 58m 54s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/apicagent:v1-0-1-827
```

```
app-logstash         Cisco_NIR-SystemService.logstash         apic-ifc1      running
0d 18h 59m  4s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/logstash:v1-0-1-827
app-eventcollector   Cisco_NIR-SystemService.eventcollector   apic-ifc3      running
0d 18h 59m  5s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/eventcollector:v1-0-1-827
app-eventcollector   Cisco_NIR-SystemService.eventcollector   apic-ifc1      running
0d 18h 59m  4s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/eventcollector:v1-0-1-827
app-logstash         Cisco_NIR-SystemService.logstash         apic-ifc2      running
0d 18h 59m  5s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/logstash:v1-0-1-827
app-apiserver        Cisco_NIR-SystemService.apiserver        apic-ifc2      running
0d 18h 59m  4s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/apiserver:v1-0-1-827
app-apiserver        Cisco_NIR-SystemService.apiserver        apic-ifc1      running
0d 18h 59m  5s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/apiserver:v1-0-1-827
app-logstash         Cisco_NIR-SystemService.logstash         apic-ifc3      running
0d 18h 59m  4s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/logstash:v1-0-1-827
app-apiserver        Cisco_NIR-SystemService.apiserver        apic-ifc3      running
0d 18h 59m  4s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/apiserver:v1-0-1-827
app-eventcollector   Cisco_NIR-SystemService.eventcollector   apic-ifc2      running
0d 18h 59m  4s
local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/eventcollector:v1-0-1-827

apic-ifc1#
apic-ifc1# acidiag scheduler elastic members
ip       heap.percent ram.percent cpu load_1m load_5m load_15m node.role master name
10.0.0.3           26          99  20    4.88    4.40     3.49 mdi       -      apic-ifc3
10.0.0.1           26          91  19    3.04    3.75     3.56 mdi       -      apic-ifc1
10.0.0.2           26          88  19    0.97    1.77     2.05 mdi       *      apic-ifc2

apic-ifc1# acidiag scheduler elastic health
{
  "cluster_name" : "elasticsearch",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 120,
  "active_shards" : 360,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}

apic-ifc1# acidiag scheduler elastic indices
health status index                                    uuid                   pri rep
docs.count docs.deleted store.size pri.store.size
green  open   cisco_nir-fabricnodesdb                  B8X8lktsSnWzCckzms8JfQ   1   2
   16            0    182.7kb           61kb
green  open   cisco_nir-aggflowdb-2019.01.31.18.00.00 RnIB3S7fTBikO07xPhquFw   9   2
    0            0      6.1kb            2kb
green  open   cisco_nir-sysmetrics-2019.01.31         HBP_iJgsRQyGTyOa-Horvg   7   2
1807463           0    747.1mb        249.1mb
green  open   cisco_nir-statsdb-000003                Sgh1bZ7CQ_et4j__AQ56Ww   5   2
```

```
9517896            0      2.9gb        998.8mb
green  open   cisco_nir-eventsdb                     tJTC02wpSmy_9Fa8p33WDg   5   2
22940              0     25.4mb          8.4mb
green  open   searchguard                            9nSh8NeqSYKYF7w4W0eHkQ   1   2
    5              2     65.1kb         21.7kb
green  open   cisco_nir-statsdb-000002               Zv9P247tSfyK_6o37NGkjg   5   2
9494058            0      2.9gb        999.5mb
green  open   cisco_nir-fault_historydb              mUY-NT2lQqmP54flD44xzg   5   2
 2405              0      4.3mb          1.4mb
green  open   cisco_nir-collectorstatsdb             6RrCkrhxT6OWz-M8eIfjrw   5   2
    0              0      3.4kb          1.1kb
green  open   cisco_nir-sysmetrics-2019.01.30        wz3Jif_8SMOhc4Or8MEXNg   7   2
41870              0     19.2mb          6.4mb
green  open   cisco_nir-fabric_issuesdb              tj-Y0cP4SF2OdfMkumqcqQ   2   2
    0              0      1.3kb           466b
green  open   cisco_nir-anomalytsdb                  rzGukbWCTk276i2FQpRCJQ   3   2
    1              0     24.9kb          8.3kb
green  open   cisco_nir-aggflowdb-2019.01.31.12.00.00 hVUmPx5JQJi9gtiEB4no_A   9   2
    0              0      6.1kb            2kb
green  open   cisco_nir-resourcecollectdb            kDTBYxq0RtSp0tzXkFgVWw   3   2
168380             0     38.1mb         12.7mb
green  open   cisco_nir-resourcescoresdb             ApM3S1QEQ3m9co-UeX-tvQ   3   2
38120              0     29.4mb          9.8mb
green  open   cisco_nir-aggflowdb-2019.01.31.16.00.00 fdaRZvNVS2eVqEF1uRFKcg   9   2
    0              0      6.1kb            2kb
green  open   cisco_nir-eprecordsdb                  JIzHooPPQwShJeFCa11GyA   5   2
    0              0      3.4kb          1.1kb
green  open   cisco_nir-statsdb-000004               pqhaqo3OTv6E6y1zBwfwYg   5   2
1539566            0    507.6mb        170.8mb
green  open   cisco_nir-aggflowdb-2019.01.31.14.00.00 G6yngLSoQzyn1odMCDLIaQ   9   2
    0              0      6.1kb            2kb
green  open   cisco_nir-licensedb                    87XBQmQHRfap024AAXnEXg   1   2
    1              0     10.2kb          3.4kb
green  open   cisco_nir-aggflowdb-2019.01.31.20.00.00 ZQdMl2yxSaaNCdGXW-4YOg   9   2
    0              0      6.1kb            2kb
green  open   cisco_nir-aggflowdb-2019.01.31.10.00.00 btO1x9A0Teakv2AdK_6n-A   9   2
    0              0      6.1kb            2kb
green  open   cisco_nir-anomalydb                    QrHtrk2LSZ-LNsS37E0btQ   3   2
    1              0     23.5kb          7.8kb

apic-ifc1# acidiag scheduler elastic shards
index                                 shard prirep state      docs   store ip        node
cisco_nir-sysmetrics-2019.01.30         4     r      STARTED    5914 924.5kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         4     p      STARTED    5914 928.9kb 10.0.0.2
ifav22-ifc2
cisco_nir-sysmetrics-2019.01.30         4     r      STARTED    5914 899.8kb 10.0.0.1
ifav22-ifc1
cisco_nir-sysmetrics-2019.01.30         1     r      STARTED    6033 920.7kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         1     p      STARTED    6033 954.1kb 10.0.0.2
ifav22-ifc2
cisco_nir-sysmetrics-2019.01.30         1     r      STARTED    6033 982.7kb 10.0.0.1
ifav22-ifc1
cisco_nir-sysmetrics-2019.01.30         2     r      STARTED    6070 944.1kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         2     r      STARTED    6070 914.2kb 10.0.0.2
ifav22-ifc2
cisco_nir-sysmetrics-2019.01.30         2     p      STARTED    6070 951.1kb 10.0.0.1
ifav22-ifc1
cisco_nir-sysmetrics-2019.01.30         6     p      STARTED    5923 961.2kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         6     r      STARTED    5923 944.4kb 10.0.0.2
ifav22-ifc2
```

```
cisco_nir-sysmetrics-2019.01.30         6     r      STARTED    5923 958.8kb 10.0.0.1
ifav22-ifc1
cisco_nir-sysmetrics-2019.01.30         3     p      STARTED    5962 954.4kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         3     r      STARTED    5962 911.1kb 10.0.0.2
ifav22-ifc2
cisco_nir-sysmetrics-2019.01.30         3     r      STARTED    5962 926.3kb 10.0.0.1
ifav22-ifc1
cisco_nir-sysmetrics-2019.01.30         5     r      STARTED    6003 937.9kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         5     r      STARTED    6003 931.6kb 10.0.0.2
ifav22-ifc2
cisco_nir-sysmetrics-2019.01.30         5     p      STARTED    6003   912kb 10.0.0.1
ifav22-ifc1
cisco_nir-sysmetrics-2019.01.30         0     p      STARTED    5965 947.9kb 10.0.0.3
ifav22-ifc3
cisco_nir-sysmetrics-2019.01.30         0     r      STARTED    5965 909.2kb 10.0.0.2
ifav22-ifc2
cisco_nir-sysmetrics-2019.01.30         0     r      STARTED    5965 966.8kb 10.0.0.1
ifav22-ifc1

<-- SNIP LIST OF ALL OTHER RESOURCES -->
apic-ifc1#
```