



Cisco Network Insights for Resources Application for Cisco APIC User Guide, Release 2.0.x

First Published: 2019-06-07

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	1
	New and Changed Information	1

CHAPTER 2	Cisco Network Insights for Resources Installation	3
	About Cisco Network Insights for Resources	3
	Software Requirements	3
	Hardware Requirements	3
	Downloading Cisco NIR Application from the Cisco App Center	4
	Installing Cisco NIR Application on Cisco APIC	4
	Installing Cisco NIR on Cisco Application Services Engine via Cisco APIC	5
	Upgrade Cisco NIR on Cisco Application Services Engine via Cisco APIC	6

CHAPTER 3	Using Cisco Network Insights for Resources	9
	Cisco NIR Components	9
	Cisco NIR Setup and Settings	10
	Guidelines and Limitations	11
	Navigating Cisco NIR	11
	Using the Cisco Network Insights for Resources Application	14
	Cisco NIR Dashboard	14
	Cisco NIR System	16
	Resources	16
	Environmental	19
	Cisco NIR Operations	20
	Statistics	21
	Flow Analytics	22
	Event Analytics	25

CHAPTER 4

Cisco NIR REST API Examples 29

- all_resources() 29
- anomalies_details() 30
- anomalies_summary() 31
- events_buckets() 31
- events_details() 32
- events_summary() 33
- get_fabrics_anomaly_summary() 34
- get_fabrics_list() 35
- get_nodes_list() 36
- get_protocols_details() 36
- get_protocols_resources() 38
- get_protocols_topentities() 38
- get_protocols_topnodes() 40
- health_diagnostics() 40
- service_health() 41
- utilization_node_details() 42
- utilization_top_nodes() 43

CHAPTER 5

Troubleshooting Cisco NIR Application 45

- Cisco NIR Application on Cisco APIC Troubleshooting Commands 45



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

- [New and Changed Information, on page 1](#)

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 2.0.x

Feature	Description	Release
Cisco NIR application on Cisco Application Services Engine	Cisco Network Insights for Resources app on Cisco Application Services Engine via Cisco APIC.	2.0.2
Flow Analytics	Flow analytics records let the user visualize the flows in the fabric and their characteristics across the entire ACI.	2.0.2
Cisco Network Insights for Resources Application	This guide was released to provide a description of Cisco Network Insights for Resources application.	2.0.1



CHAPTER 2

Cisco Network Insights for Resources Installation

This chapter contains the following sections:

- [About Cisco Network Insights for Resources, on page 3](#)
- [Downloading Cisco NIR Application from the Cisco App Center, on page 4](#)
- [Installing Cisco NIR Application on Cisco APIC , on page 4](#)
- [Installing Cisco NIR on Cisco Application Services Engine via Cisco APIC, on page 5](#)
- [Upgrade Cisco NIR on Cisco Application Services Engine via Cisco APIC, on page 6](#)

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 via Cisco APIC.

Software Requirements

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

- The Cisco NIR applications require Cisco Application Policy Infrastructure Controller (Cisco APIC), Release 4.1(2m). For details on Cisco Application Policy Infrastructure Controller, refer to the documentation [Cisco APIC](#).
- The Cisco NIR applications require Cisco Application Services Engine, Release 1.1.0a.

Hardware Requirements

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

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

- Use existing Cisco APIC cluster.
- The Cisco Application Services Engine cluster SE-NODE-G2.


- The Flow Telemetry is supported for Cisco Nexus 9300-FX and 9300-FX2 platform switches, Cisco Nexus 93180YC-FX and 93108TC-FX switches, and Cisco Nexus 9500 platform switches with line cards.

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, you can 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 via Cisco APIC.

Installing Cisco NIR Application on Cisco APIC


This section contains the steps required to install Cisco NIR application on Cisco APIC.

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 **Apps** tab at the top of the GUI and then click **Apps**.
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 welcome dialog for the first installation.
- Step 14** Once the application icon appears in the Catalog group, click the newly added icon to continue the installation. This part of the installation can take up to three minutes or more depending on the load on your servers.

What to do next

When the installation is complete, the application opens to the welcome dialog. Continue with the setup of the Cisco Network Insights for Resources application located in the Settings section of the next chapter.



Installing Cisco NIR on Cisco Application Services Engine via Cisco APIC

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

Before you begin

Before you begin installing a Cisco NIR application on the Cisco Application Services Engine via 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**.
- You can 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 at the top of the GUI and then click **Apps**.
- Once the application installation is completed, an application 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 **Welcome to Network Insights Setup** dialog appears the first time after installation.
-

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.

Upgrade Cisco NIR on Cisco Application Services Engine via Cisco APIC

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

Before you begin

Before you begin upgrading a Cisco NIR application on the Cisco Application Services Engine via 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 via Cisco APIC](#), on page 5.
- 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.
-



CHAPTER 3

Using Cisco Network Insights for Resources

This chapter contains the following sections:

- [Cisco NIR Components, on page 9](#)
- [Cisco NIR Setup and Settings, on page 10](#)
- [Guidelines and Limitations, on page 11](#)
- [Navigating Cisco NIR, on page 11](#)
- [Using the Cisco Network Insights for Resources Application, on page 14](#)

Cisco NIR Components



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 switches. 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 devices 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 devices in the fabric to achieve the goal:

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

- **Flow Analytics**—This includes the anomalies in the behavior of fabric switches such as average latency, packet drop indicator, and flow move indicator across the entire ACI.
- **Resource and Environmental Utilization**—Resource analytics supports configuration, operational and hardware resources. Environmental covers CPU, memory, temperature, fan utilization, power, and storage related to the leaf switches, spine switches, and Cisco APIC. System analytics also covers anomalies, the trending information of each resource, and graphing of parameters, which help network operators debug devices 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 well 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 a anomaly database.

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 Set Up**.

The Set Up window appears.

2. Make sure the following are checked for the application. They are checked by default.


- NTP and Time Zone Configuration
- Flow Analytics
- Inband IP Configuration

3. Click **Done**.

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
	<p>Clicking on this settings menu allows you to display or alter the following:</p> <ul style="list-style-type: none"> • Application Settings—Displays if Flow Collection is turned on and Management In-Band EPG is set to default. • Flow Collection Filters—Displays the available VRF based filters. You can also add a new filter rule that will be applied to all relevant switches. • Service Status—Displays the health information of critical services packaged as part of the APP NIR. • Collection Status—Displays data collection of System Metrics, and Events information per node. • Rerun Set Up—Allows you to go back to the Data Collection Set Up check list. • About Network Insights—Displays the application version number.

Guidelines and Limitations

The following are guidelines and limitations for Cisco NIR on Cisco APIC.

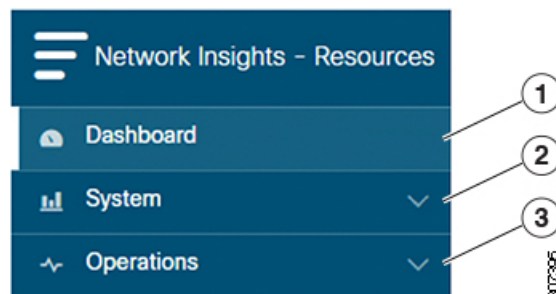
- When fabric is upgraded and nodes are reloaded, disable and enable the Cisco NIR app for the application to load the latest data.

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:

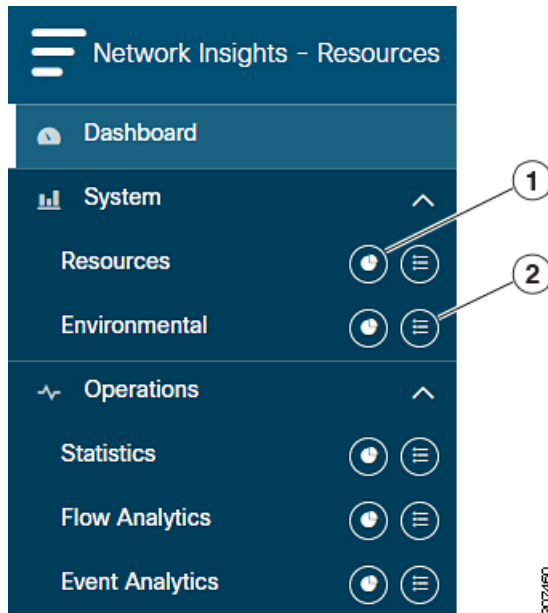


1 Dashboard: The main dashboard for the Cisco NIR application providing immediate access to anomalies.

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.

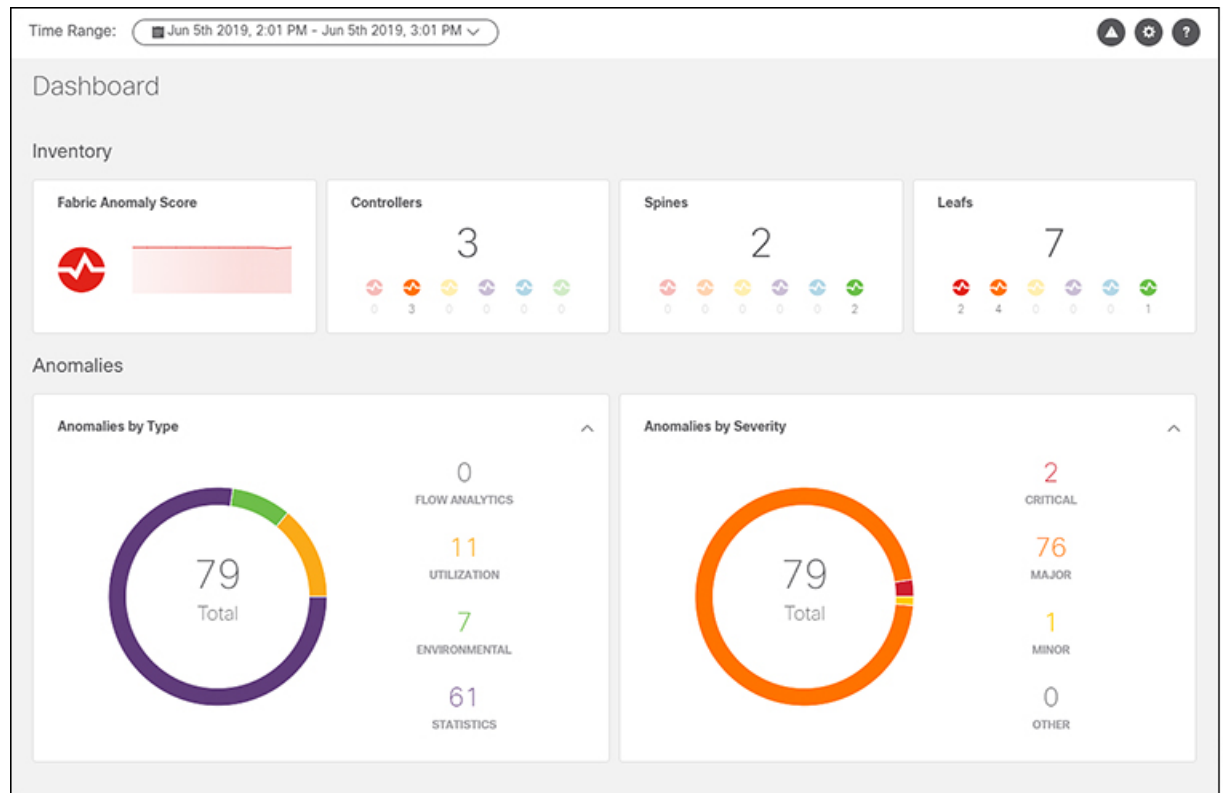
2 Browse View icon: Provides a detailed view of returned data for the selected telemetry type and allows for filtering to further isolate problem areas.

Work Pane

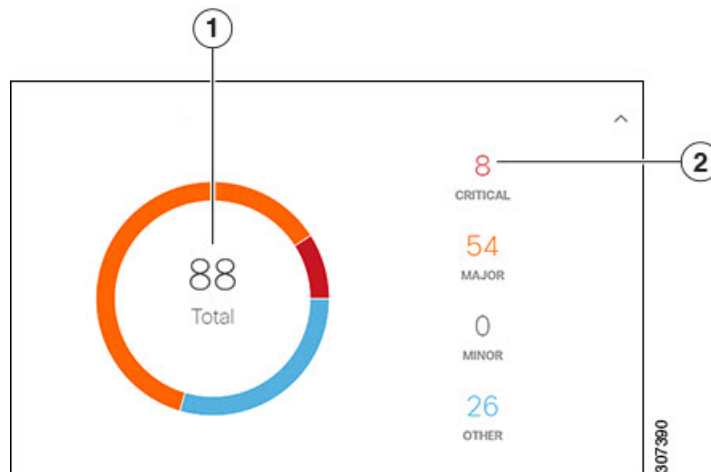
The work pane is the main viewing location in the Cisco NIR application. All information tiles, graphs, charts, and lists appear in the work pane.

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)

307381

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.

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, and are color coded based on severity: Critical: Red, Major: Orange, Minor: Yellow, Warning: Purple, Information: Blue, and 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 an anomalies are exceeded thresholds and excessive rates of change.

Inventory

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 switches in the fabric.

Property	Description
Leafs	Displays the total number of leaf switches in the fabric.

Anomalies

Click on any number to access the Browse Anomalies work pane.

Property	Description
Anomalies by Type	Displays the number of Anomalies by their type. Anomaly types include: <ul style="list-style-type: none"> • Utilization • Environmental • Statistics • Flow Analytics
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 . <ul style="list-style-type: none"> • Critical • Major • Minor • Other

Browse Anomalies

View, sort, and filter anomalies through the Browse Anomalies work pane.

Filters

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.

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.

Anomaly Chart

Property	Description
Anomalies By Type	Displays the number of Anomalies by their type. Anomaly types include: <ul style="list-style-type: none"> • Utilization • Environmental • Statistics • Flow Analytics
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 . <ul style="list-style-type: none"> • Critical • Major • Minor • Other

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.

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Anomaly Score • Node • VRF • BD • EPG • VLAN
Hardware Resources	Displays a list of configuration resources based on resource utilization. List information includes: <ul style="list-style-type: none"> • Anomaly Score • Node • Port Usage • Port Bandwidth • LPM • Policy TCAM

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage
Environmental Resources (table)	Displays a list of the top node by anomaly score. Table columns include: <ul style="list-style-type: none"> • 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.
- **Event Analytics**—Displays charts for event occurrences over time.

Statistics

The Operations Statistics section of the Cisco NIR application contains 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 of each of it's interfaces.

Browse Statistics

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

Filters

You can refine the displayed statistics by the following filters:

- Node - display only nodes.
- Interface - display only interfaces.
- Protocol - display only protocols.
- Operational State -
- Admin 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: <ul style="list-style-type: none"> • Transmit Utilization • Receive Utilization • Error
Interface Statistics	Displays a list of interface statistics sorted by anomaly score. List information includes: <ul style="list-style-type: none"> • Anomaly Score • Interface • Node • Receive Utilization • Transmit Utilization • Errors
Protocol Statistics	Displays a list of protocol statistics sorted by anomaly score. List information includes: <ul style="list-style-type: none"> • Anomaly Score • Protocol • Node • Number of Interfaces • Errors

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

Each Cisco Application Centric Infrastructure (Cisco ACI) switch streams telemetry events from the fabric to an external service that analyzes the events and proactively detects issues in the fabric behavior. By analyzing the flows exported from all Cisco ACI leaf switches in the fabric it is possible to build a picture of all flows entering and leaving the fabric.

Each flow record 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 via Cisco APIC:

- The Flow Analytics for Cisco NIR application requires you to install Cisco Application Services Engine, Release 1.1.0a.
- For details on Flow Telemetry support for Cisco Nexus series switches, see [Hardware Requirements, on page 3](#).


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 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 anomalies. The details include, type of alarm, source destination, packet drops and latency.

Browse Flows

Browse flows filters the flows to visualize the top nodes by flow anomalies through the Browse Flow Analytics work pane.

Property	Description
	<p>Clicking on this icon allows you to alter the following:</p> <ul style="list-style-type: none"> • Application Settings—Enable or disable flow collection and assign a previously configured inband management EPG. <p>Note By default, flow collection is disabled. After the NIR application is downloaded, you must enable flow collection for this feature to function.</p> <ul style="list-style-type: none"> • Flow Collection Filters—Create VRF and EPG collection rules per tenant: <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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.



Note To verify that **Flow Collection** has started, check **Collection Status** in the **Settings** menu. If **Flow Collection** is functioning, you should see the green circles in the table indicating the nodes where the flows are being exported.

Flow Collection Filters

This section describes the active nodes, ingress nodes, egress nodes, and flow collection filters to display the anomalies in the behavior of fabric switches.

Property	Description
Nodes	Active nodes are leaf switches and spines that show the anomaly score for the top nodes by flow anomalies.
Ingress Nodes	Displays the Ingress node name and tenant that show the top nodes by flow anomalies.
Egress Nodes	Displays the Egress node name and tenant that show the top nodes by flow anomalies.

Property	Description
Filters	<p>You can display the node flow observations sorted by the following filters:</p> <ul style="list-style-type: none"> • Timestamp • Ingress Nodes • Egress Nodes • Source EPG • Source Address • Source Port • Destination EPG • Destination Address • Destination Port • Address Type • Protocol
Top 10 flows by	<p>Lists the top 10 flows that scored highest in the following:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> 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 switch 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 switch.

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: <ul style="list-style-type: none"> • Deletion • Creation • Modification
Events by Severity	Displays all events based on severity: <ul style="list-style-type: none"> • Critical • Major • Minor • Other

Property	Description
Faults by Severity	Displays all faults based on severity: <ul style="list-style-type: none">• Critical• Major• Minor• Other



CHAPTER 4

Cisco NIR REST API Examples

This chapter contains the following sections:

- [all_resources\(\)](#), on page 29
- [anomalies_details\(\)](#), on page 30
- [anomalies_summary\(\)](#), on page 31
- [events_buckets\(\)](#), on page 31
- [events_details\(\)](#), on page 32
- [events_summary\(\)](#), on page 33
- [get_fabrics_anomaly_summary\(\)](#), on page 34
- [get_fabrics_list\(\)](#), on page 35
- [get_nodes_list\(\)](#), on page 36
- [get_protocols_details\(\)](#), on page 36
- [get_protocols_resources\(\)](#), on page 38
- [get_protocols_topentities\(\)](#), on page 38
- [get_protocols_topnodes\(\)](#), on page 40
- [health_diagnostics\(\)](#), on page 40
- [service_health\(\)](#), on page 41
- [utilization_node_details\(\)](#), on page 42
- [utilization_top_nodes\(\)](#), on page 43

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/telemetry/anomalies/details.json'
```

Response :

```

{
  "totalItemsCount": 90,
  "totalResultsCount": 90,
  "offset": 0,
  "entries": [
    {
      "anomalyId": "QUE0000000000018",
      "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": "QUE0000000000007",
      "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/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/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": "13EncRtdIfF110176",
    "faultType": "operational",
    "highestSeverity": "warning",
    "occurrences": 1,
    "recordId": "bld15",
    "cause": "threshold-crossed",
    "changeSet": [
      {
        "oldValue": "",
        "propertyName": "dropRate",
        "newValue": "52039"
      }
    ],
    "subject": "counter",
    "severity": "warning",
    "eventType": "fault",
    "severityId": 2,
    "prevSeverity": "warning",
    "contextClass": "13EncRtdIf",
    "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
          }
        ]
      }
    ]
  }
}

```

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 anomaly scores of the fabric,

default:'no'

- history => Requires the timeseries data of sum(anomaly scores, default:'no'
- granularity => applicable if history = "yes" , granulariry 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/telemetry/nodes.json'
Response   :
            {
              "entries": [
                {
                  "nodeRole": "leaf",
                  "nodeId": "302",
                  "nodeName": "rleaf-scrimshaw2",
                  "nodeMgmtIp": "1.2.3.4"
                },
                {
                  "nodeRole": "spine",
                  "nodeId": "205",
                  "nodeName": "swmp14-dopplebock",
                  "nodeMgmtIp": "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_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/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 diagnostics.
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/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 5

Troubleshooting Cisco NIR Application

This chapter contains the following sections:

- [Cisco NIR Application on Cisco APIC Troubleshooting Commands, on page 45](#)

Cisco NIR Application on Cisco APIC Troubleshooting Commands

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 2: 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	<p>The current severity level of the event. The levels are:</p> <ul style="list-style-type: none"> • 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	
2	apic-ifc2	active	10.0.0.2	172.4.5.6	Apic	FCH1809V18S	apic-ifc1.node.ifav22.apic.local
3	apic-ifc3	active	10.0.0.3	172.7.8.9	Apic	FCH1809V191	apic-ifc2.node.ifav22.apic.local
							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 Modified	Group Image	Node	Status
kafka 0d 19h 37m 16s	bird_kafka-kafka.kafka apic-system/kafka:0.1.0	apic-ifc3	running
kafka 0d 19h 37m 16s	bird_kafka-kafka.kafka apic-system/kafka:0.1.0	apic-ifc1	running
kafka 0d 19h 37m 16s	bird_kafka-kafka.kafka apic-system/kafka:0.1.0	apic-ifc2	running

apic-ifc1# **acidiag scheduler appstatus elastic**

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

apic-ifc1# **acidiag scheduler appstatus Cisco_NIR**

Container Modified	Group Image	Node	Status
app-brain 0d 18h 58m 53s	Cisco_NIR-ClusterService.brain local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/brain:v1-0-1-827	apic-ifc2	running
app-scheduler 0d 18h 58m 54s	Cisco_NIR-ClusterService.scheduler local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/scheduler:v1-0-1-827	apic-ifc1	running
app-correlator 0d 18h 58m 53s	Cisco_NIR-ClusterService.correlator local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/correlator:v1-0-1-827	apic-ifc3	running
app-predictor 0d 18h 58m 53s	Cisco_NIR-ClusterService.predictor local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/predictor:v1-0-1-827	apic-ifc3	running
app-apicagent 0d 18h 58m 54s	Cisco_NIR-ClusterService.apicagent local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/apicagent:v1-0-1-827	apic-ifc2	running
app-logstash 0d 18h 59m 4s	Cisco_NIR-SystemService.logstash	apic-ifc1	running

```

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 B8X81ktsSnWzCckzms8JfQ 1 2
16 0 182.7kb 61kb
green open cisco_nir-aggfldb-2019.01.31.18.00.00 RnIB3S7fTBik007xPhquFw 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-NT2lQqMP54f1D44xzg	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			fdaRZvNVS2eVqEFluRFKcg	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			pqhaqo30Tv6E6y1zBwfwYg	5	2		
1539566		0	507.6mb	170.8mb					
green	open	cisco_nir-aggflowdb-2019.01.31.14.00.00			G6yngLSOqZyn1oMCDLIaQ	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			ZQdM12yxSaaNCdGXW-4YOg	9	2		
0		0	6.1kb	2kb					
green	open	cisco_nir-aggflowdb-2019.01.31.10.00.00			bt01x9A0Teakv2AdK_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#

```