



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

# Table of Contents

The Cisco Network Insights for Resources for Cisco APIC User Guide .....	3
New and Changed Information .....	4
Cisco Network Insights for Resources Installation .....	7
About Cisco Network Insights for Resources .....	7
Downloading Cisco NIR Application from the Cisco App Center .....	7
Installing Cisco NIR Application on Cisco APIC .....	7
Add a Site on Cisco Application Services Engine Using GUI .....	8
Installing Cisco NIR on Cisco Application Services Engine .....	9
Cisco Network Insights for Resources Setup and Settings .....	10
Cisco NIR Components in Cisco APIC .....	10
Guidelines and Limitations .....	11
Cisco NIR Setup .....	11
Cisco NIR Settings .....	13
Cisco Network Insights for Resources Dashboard .....	17
Navigating Cisco NIR .....	17
Site Dashboard .....	21
Dashboard Inventory .....	22
Dashboard Timeline .....	23
Site Dashboard Anomalies .....	24
Browse Anomalies .....	24
Top Nodes by Anomaly Score .....	25
Browse Anomaly Filters .....	26
Topology Dashboard .....	27
Devices .....	28
Browse Nodes .....	28
Cisco Network Insights for Resources System .....	29
System Resources .....	29
System Environmental .....	31
Cisco Network Insights for Resources Operations .....	34
Statistics Analytics .....	34
Statistics Dashboard .....	34
Browse Statistics Filters .....	34
Statistics Analytics Limitations .....	36
Browse Statistics .....	37
Interface Statistics .....	37
Protocol Statistics .....	37
Multicast Protocol Statistics .....	38
Internet Group Management Protocol Snoop .....	39

Flow Analytics .....	40
Flow Analytics Overview .....	40
Flow Analytics Pre-requirements .....	40
Flow Analytics Limitations .....	40
Flow Analytics Dashboard .....	41
Browse Flow Records .....	42
Endpoint Analytics .....	44
Endpoint Analytics Overview .....	44
Endpoint Analytics Dashboard .....	45
Endpoint Analytics Guidelines and Limitations .....	45
Browse Endpoint Analytics .....	45
Event Analytics .....	47
Third Party Integration for Cisco NIR .....	50
About AppDynamics Integration .....	50
Installing AppDynamics .....	51
Onboard AppDynamics Controller .....	51
Cisco NIR and AppDynamics Integration Dashboard .....	52
Browse AppDynamics Integration Application .....	53
Guidelines and Limitations .....	54
Topology View .....	54
Upgrade Cisco Network Insights for Resources .....	56
Upgrade Cisco NIR on Cisco APIC .....	56
Upgrade Cisco NIR on Cisco Application Services Engine .....	56
Upgrade Paths for Cisco NIR Application .....	57
Cisco NIR REST API Examples .....	59
all_resources() .....	59
anomalies_details() .....	59
anomalies_summary() .....	60
events_buckets() .....	61
events_details() .....	62
events_summary() .....	64
flows_details() .....	65
flows_summary() .....	67
flows_top_flows() .....	69
flows_top_nodes() .....	71
get_fabrics_anomaly_summary() .....	72
get_fabrics_list() .....	73
get_nodes_list() .....	74
get_protocols_details() .....	75
get_protocols_resources() .....	77
get_protocols_topentities() .....	79

get_protocols_topnodes() .....	80
health_diagnostics() .....	82
service_health() .....	82
utilization_node_details() .....	83
utilization_top_nodes() .....	85
Troubleshooting Cisco NIR application .....	87
Troubleshooting Cisco NIR Common GUI Issues .....	87
Total Audit Logs, Events, and Faults .....	88
Basic Debugging Commands for Cisco NIR on Cisco APIC .....	89
Basic Debugging Commands for Cisco NIR on Cisco Application Services Engine .....	94

First Published: 2020-07-26

Last Modified: 2020-11-17

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

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

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

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

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

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

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

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

© 2017-2020 Cisco Systems, Inc. All rights reserved.

# **The Cisco Network Insights for Resources for Cisco APIC User Guide**

# New and Changed Information

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

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

Feature	Description	Release	Where Documented
Add Site	Add a site on Cisco Application Services Engine. Applications installed on Cisco Application Services Engine can access the added site.	2.2.2	<a href="#">Add a Site on Cisco Application Services Engine Using GUI</a>
Multiple Site support	The multiple site and flow configuration enables you to onboard the site from the list of available sites.	2.2.2	<a href="#">Cisco NIR Multiple Site Setup</a>
Flow Ingest	The flow statistics are collected from Flow Collector and Flow Correlator to determine the health of the flow when the flow threshold is reached. The system status page lists the active system anomalies and flow thresholds.	2.2.2	<a href="#">System Status</a>
Dashboard Devices	The detailed view of the nodes with a graphical representation of top nodes and top resources.	2.2.2	<a href="#">Browse Nodes</a>



Feature	Description	Release	Where Documented
Dashboard Topology (Beta)	The topology view represents the stitching between the nodes connected to the Cisco APIC site. The Early Access Mode in the Network Insights Setup page lets you enable beta Network Insights features and enhancements. Once the beta features are enabled they cannot be disabled.	2.2.2	<a href="#">Topology Dashboard</a>
Multicast protocols PIM, IGMP, and IGMP Snoop	Support for PIM, IGMP, and IGMP Snoop IPv4 multicast operational and statistical data in the Protocol Statistics tab.	2.2.2	<a href="#">Multicast Protocol Statistics</a>
Endpoint Analytics	The Endpoint Analytics provides detailed analytics of endpoints learnt in the site. The anomalies detected as part of endpoint analytics include rapid endpoint moves across nodes, interface, and endpoint groups, and endpoints that do not get learnt back after a node reboot.	2.2.2	<a href="#">Endpoint Analytics</a>

Feature	Description	Release	Where Documented
AppDynamics Integration	AppDynamics provides the required metrics for monitoring, identifying, and analyzing the applications that are instrumented with AppDynamics agents. Cisco NIR provides flow analytics, statistics analytics, and topology view on these metrics to identify anomalies.	2.2.2	<a href="#">About AppDynamics Integration</a>
Troubleshooting	Debugging commands for Cisco NIR on Cisco Application Services Engine.	2.2.2	<a href="#">Basic Debugging Commands for Cisco NIR on Cisco Application Services Engine</a>

# Cisco Network Insights for Resources Installation

## 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.


## 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.

### Procedure

1. Log in to the Cisco APIC GUI with admin privileges.
  - a. If you do not have admin privileges, log in to the [Cisco App Center](#) to download the application.
2. Choose **Apps**.
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.
4. Search for Cisco Network Insights for Resources application on the search bar.
5. Select the Cisco Network Insights for Resources application you want to download and click **Download** for that app to begin the process of downloading the app to your local machine.
6. Review the license agreement and, if OK, click **Agree and download**. The Cisco Network Insights for Resources application is downloaded to your local machine.
7. 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

Use this procedure to install Cisco NIR application on Cisco APIC. These are required for software telemetry.

## Before you begin

You must have administrative credentials to install Cisco NIR application.

## Procedure

1. Log in to the Cisco APIC GUI with admin privileges.
2. Click the **Admin > Downloads** tab.
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.
4. Enter the name of the download file in the **Download Name** field.
5. In the **Protocol** field, choose **Secure Copy**.
6. In the **URL** field, enter the path to the download file image location.
7. Enter your name and password in the **Username** and **Password** fields.
8. Enter **Submit**.
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.
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.
11. Click **Enable** to open the application. A Details dialog appears.
12. Click **Enable**. The application icon appears with a blue **Open** button.
13. Click **Open**. The application opens with a splash screen welcome dialog for Cisco NIR.
14. Click **Begin First Time Setup** to setup the Cisco NIR application.
15. Continue with the setup of the Cisco Network Insights for Resources application located in the Cisco NIR Initial Setup section.

## Add a Site on Cisco Application Services Engine Using GUI

Use this procedure to add a site on to the Cisco Application Services Engine using GUI. Any apps installed on Cisco Application Services Engine can access the added sites.

## Before you begin

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

## Procedure

1. Log in to the Cisco Application Services Engine GUI with admin privileges.

2. Click **Infrastructure** > **Sites** on the left navigation pane.
3. Click **Actions** > **Add Site** from the far-right side.
4. On the **Add Site** page enter the following:
  - Site Name, Controller IP, User Name, Password, Login Domain, and Inband EPG. Controller IP is a comma separated list of IP addresses to access the site.
5. Click **Add**. This adds a site to the node. Any apps installed on Cisco Application Services Engine can access the added sites.
6. Continue with the installation of the Cisco Network Insights for Resources application on Cisco Application Services Engine using GUI.


## Installing Cisco NIR on Cisco Application Services Engine

Use this procedure to install Cisco Network Insights for Resources application on the Cisco Application Services Engine using GUI.

### Before you begin

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

### Procedure

1. Log in to the Cisco Application Services Engine GUI with admin privileges.
2. Click **Apps** tab on the left navigation bar.
3. Click **Actions** > **Upload App** from the far-right side.
4. In the **URL** enter the http address and click **Upload**. Click **Refresh** icon  on the far-right side of the Downloads work pane to check the upload status.
5. When the application installation is completed, the application icon appears with the **Enable** button.
6. Click **Enable** to open the application. A pre-enable Details dialog appears and then a post-enable Details dialog appears.
7. Once the application enable is completed, the application icon appears with a **Launch App** button.
8. Click **Launch App** from the Cisco NIR application dialog. The application opens with a splash screen welcome dialog for Cisco NIR.
9. Click **Begin First Time Setup** to setup the Cisco NIR application.
10. Continue with the setup of the Cisco Network Insights for Resources application. See the Settings section [Cisco NIR Setup](#).

# Cisco Network Insights for Resources Setup and Settings

## Cisco NIR 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 site nodes. As each data source is different and the format in which data is streamed is different, there are corresponding collectors running analytics that translate the telemetry events from the nodes into data records to be stored in the data lake. The data stored in the data lake is a format that the analytics pipeline can understand and work upon.

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

- **Resources Analytics**—This includes monitoring software and hardware resources of site nodes on the Cisco APIC.
- **Environmental**—This includes monitoring environmental statistics of hardware resources such as fan, CPU, memory, and power of the site nodes.
- **Statistics Analytics**—This includes monitoring of nodes, interfaces, and protocols on the Cisco APIC and site nodes.
- **Flow Analytics**—This includes monitoring of flows on the Cisco site 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 site nodes for rapid endpoint moves 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 site and correlating internal site 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

The following are the guidelines and limitations for the Cisco Network Insights for Resources ( Cisco NIR ) application in Cisco APIC:

- If the Cisco NIR app is enabled for a site using the following methods:
  - On Cisco APIC
  - Connected to the Cisco Application Services Engine cluster
  - Or, connected to some other Cisco Application Services Engine cluster

then installation and enabling of the Cisco NIR app fails with an error message.

- After Cisco Application Services Engine reboot, it is recommended to wait until the following are complete for the Cisco Application Services Engine to restore functionality:
  - The **acidiag** health state displays healthy.
  - The Cisco Application Services Engine cluster displays green.
- When you upgrade fabric policy or upgrade nodes, if there is a connectivity loss between the fabric and Cisco Application Services Engine cluster, the Cisco NIR app may raise incorrect missing Endpoint anomaly.
- Before Cisco NIR app installation, Interface and Port Channel down anomaly will not be raised when **oper-state** is down. After Cisco NIR app installation, anomaly is captured only when the **oper-state** is up or down.
- Inorder to configure a fabric node you must first configure Telemetry to enable netflow.

## Cisco NIR Setup

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:

On the welcome to Network Insights dialog, click **Begin First Time Setup**. The **Network Insights Setup** window appears.

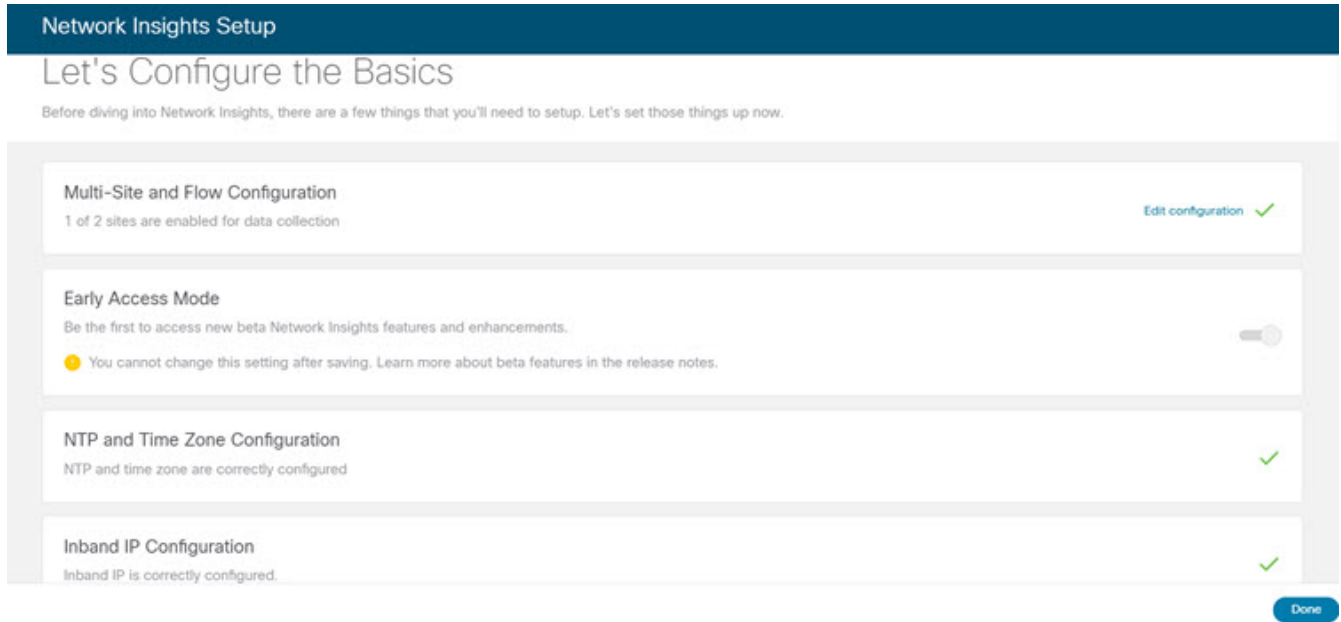
### Network Insights Setup

Make sure the following fields are checked for the Cisco NIR application.

- Multi-Site and Flow Configuration See [Cisco NIR Multiple Site Setup](#)
- Toggle to enable or disable Early Access Mode

- NTP and Time Zone Configuration
- Inband IP Configuration
- 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.

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



The multisite and flow configuration enables you onboard the site. Click **Edit Configuration** for a list of sites, status, and flow analytics status. The site status is disabled by default.

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

## Cisco NIR Multiple Site Setup

The multiple site and flow configuration enables you to enable or onboard the site from the list of available sites on Cisco NIR. Click **Edit Configuration** for a list of sites, status, enable, and disable sites. The site status is disabled by default.

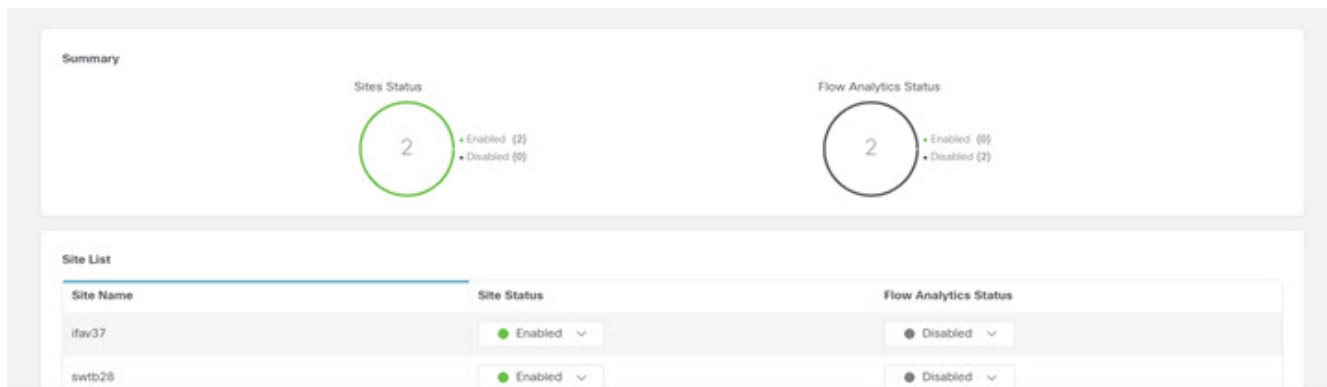
The following is the **Network Insights Setup - Multi-Site Configuration** page.



## Enable Multiple Sites

Enabling a site allows Network Insights to collect data to show powerful metrics, analytics, and other visualizations and configurations.

Enabling PTP is required and it will be switched on automatically. Telemetry needs to be enabled on Site Control Policy.



The page displays the list of sites that were added to the node.

1. Click **Enable** on the site to apply streaming policies onto the site and onboard the site.
2. Click **Enable** Flow Analytics for that site for flow telemetry configuration.

When you disable or offboard a site, the site status is then disabled and flow analytics is automatically disabled.

You can choose to enable software telemetry and flow telemetry per site.

## Cisco NIR Settings

Once Cisco NIR is installed, if there are faults present in the application, they will show on the **Faults** tab. To verify the functionality of the app, click the **Settings** icon and select **System 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. The collection status displays the data for the last hour.

On the **Site** dashboard work pane:

- The Time Range-Specify a time range and the summary table below displays the data that is collected during the specified interval.
- The Site-Allows you to choose a site containing the nodes from which to collect telemetry data.

## Flow Collection Configuration

Click **Settings** > **Flow Collection Configuration** to alter the following:

Flow Collection Configuration—Create VRF rules per tenant:

- Click the **Plus** icon and enter the filter Name.
- Select a **Name**, **Tenant**, and **VRF** from the drop-downs.
- Enter the subnet in the *Subnet* field and click **Add Subnet**.

- Click **Save**.



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

Click **Settings** > **System Status** to display Alerts, Capacity Usage per node, Network Insights usage, and time span.

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

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


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

The following system anomalies are summarized.

- **Flow Collector Level**—Flow collector reports the number of flow telemetry records known as flow events averaged over 30 seconds and specifies two thresholds; Lower and upper local threshold breached over a period of time. The collector container is stressed because it is processing more flow telemetry records than its local threshold.
- **Flow Correlator Level**—Flow correlator reports the stitched flows averaged over 30 seconds and specifies two thresholds; Lower and upper local global threshold breached over a period of time. The threshold occurs when the number of unique flows have increased and the system is under pressure.

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

Alerts



Active Critical Alert reported

Active Alerts

3

- Critical (1)
- Warning (2)

Cleared Alerts (Last Seven Days)

**132**

Total

[Hide All Alerts](#)

Filters ✕

Severity	Status	Start Time	End Time	Description	Recommendation
Warning	Active	Jul 06 2020 12:09:53.716 PM	Jul 06 2020 04:37:42.212 PM	[Category:FLOW Service Name:Flow Correlator Stat Name:incomingRecords Node Name:scale2-se-5] Crossed the lower threshold 54000 flows	Monitor the flows and be cautious enabling new flow
Critical	Active	Jul 06 2020 12:09:54.097 PM	Jul 06 2020 04:37:42.259 PM	[Category:FLOW Service Name:Flow Collector Stat Name:flowRecords Node Name:scale2-se-3] Crossed the upper	Reduce the numt of flows.

Service Level Thresholds

System Anomalies	Description
<b>Flow Collector Level</b>	The following are flow thresholds: <ul style="list-style-type: none"> <li>Lower Threshold—18000</li> <li>Global Lower Threshold—54000</li> <li>Upper Threshold—20000</li> <li>Global Upper Threshold—60000</li> </ul>
<b>Flow Correlator Level</b>	The following are flow thresholds: <ul style="list-style-type: none"> <li>Lower Threshold—54000</li> <li>Upper Threshold—60000</li> </ul>

Collection Status

Click **Settings > Collection Status**.

Collection Status—Displays if **Flow Collection** and **Software Telemetry** are functioning, you should see the green circles in the table indicating the nodes where the flows are being exported.

## Third Party Integrations

Click **Settings** > **Third Party Integrations**.


Third Party Integrations—Lets you integrate applications into Cisco NIR to provide statistical and flow analytics for the data metrics received from the integrated application.

## Network Insights Setup

Click **Settings** > **Network Insights Setup** > **Edit Configuration**.

Network Insights Setup—Lets you configure the Cisco NIR application setup for multi-site and flow configuration, enable or disable Early Access Mode on *Network Insights Setup* page.

## About Network Insights Setup

Click  icon allows you to view the following:

- **Quick Start Guide**—An overview of Cisco NIR application.
- **Welcome Screen**—The splash screen to start the Cisco NIR application from the beginning.
- **User Guide**—The documentation for installation, configuration, and use of Cisco NIR application.

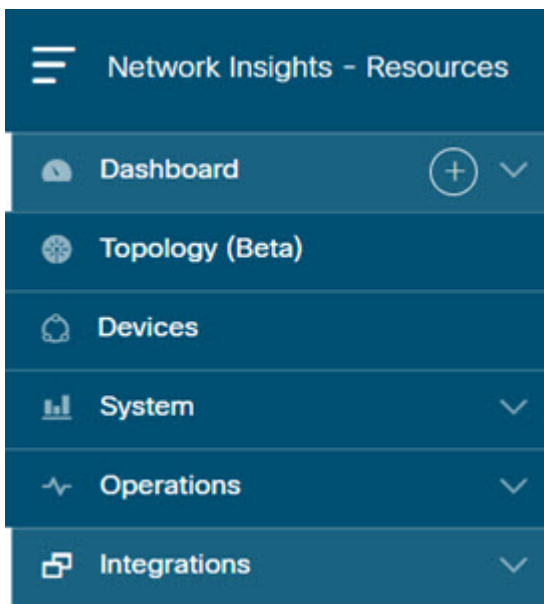
# Cisco Network Insights for Resources Dashboard

## 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 five categories:



**Dashboard:** The main dashboard for the Cisco NIR application provides immediate access to system dashboard with anomalies and timeline.

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

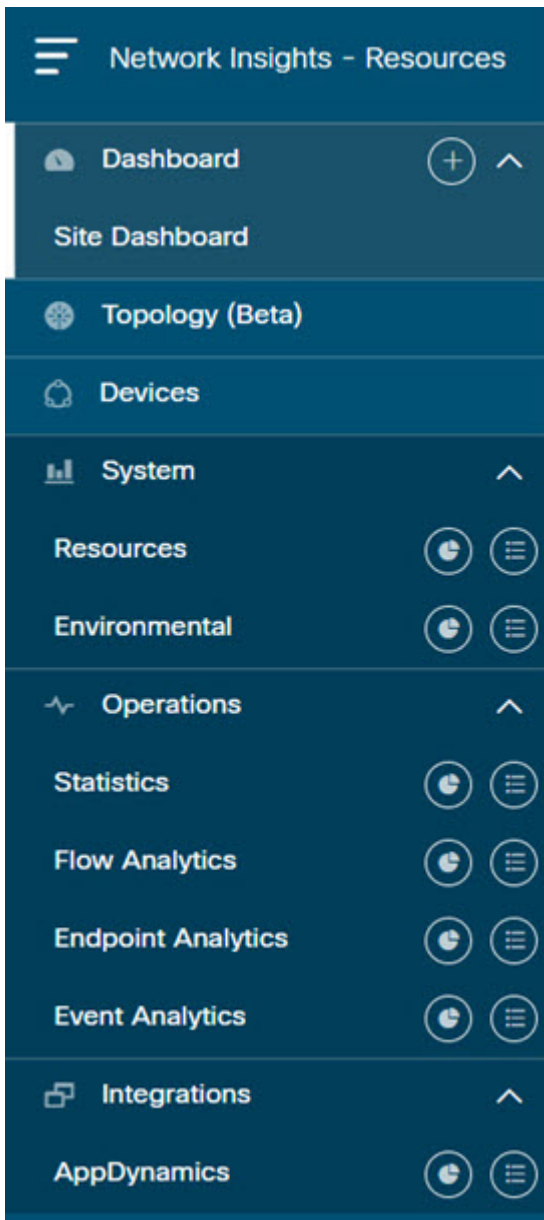
**Devices:** The detailed view of the nodes with a graphical representation of top nodes and top resources.

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

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

**Integrations:** AppDynamics integration allows Cisco NIR application to provide network insights for the data received from the AppDynamics metrics using the AppDynamics controller.

Expanding Dashboard, System, Operations, and Integrations reveals additional functions:



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

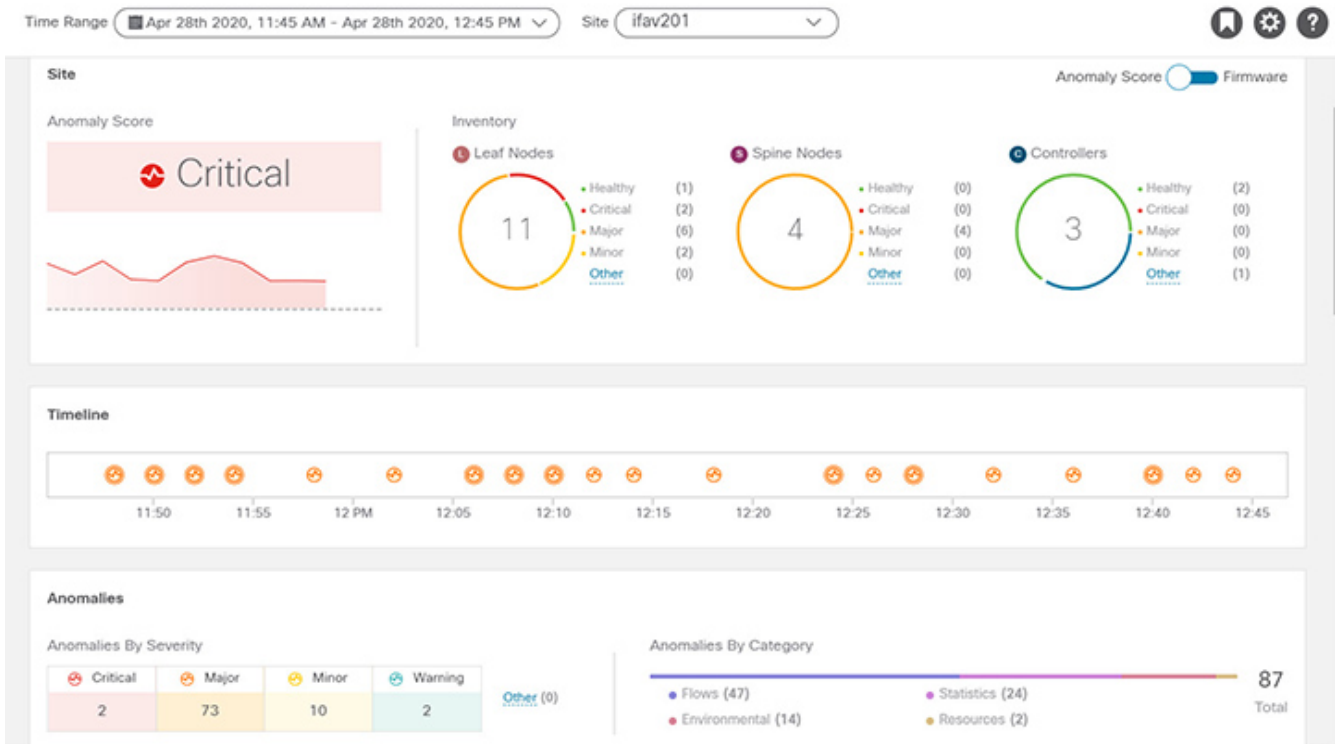
Browse View icon: Provides a detailed view of returned data for the selected telemetry type and allows for filtering to further isolate problem areas.

## Work Pane

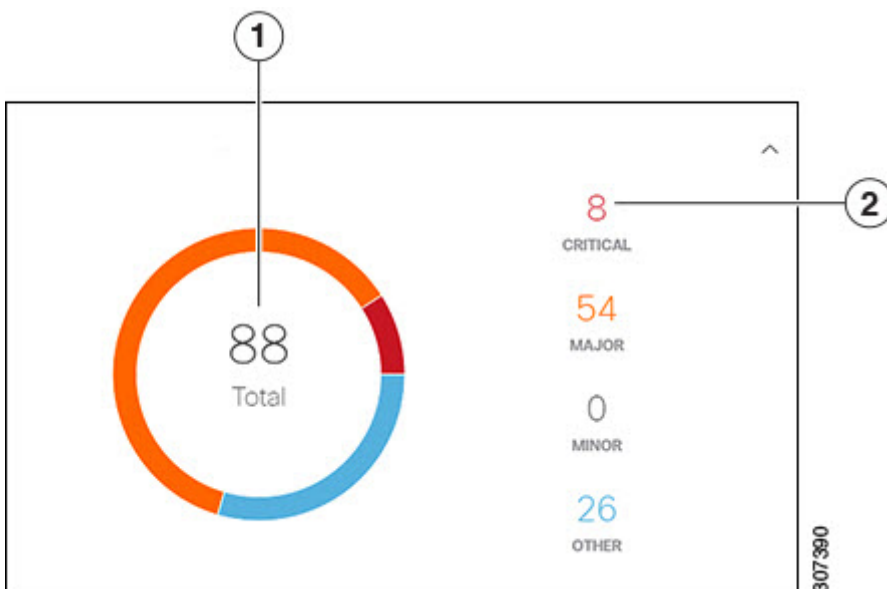
The work pane is the main viewing location in the Cisco NIR application. All information tiles, graphs, charts, and lists appear in the work pane.

### 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:

Severity	Detection Time	Last Seen Time	Resource Type	Nodes	Description	Cleared
 Major	Apr 21 2020 04:20:06.487 PM	Apr 21 2020 04:20:06.487 PM	flow	ifav201- leaf3	For flow from 80.10.1.135 port 56166 to 171.70.168.183 port 53, packet drop is detected due to forward drop.	true
 Major	Apr 21 2020 04:19:51.491 PM	Apr 21 2020 04:19:51.491 PM	flow	ifav201- leaf3	For flow from 80.10.1.135 port 39525 to 64.102.6.247 port 53, packet drop is detected due to forward drop.	 true
 Major	Apr 21 2020 04:20:12.492 PM	Apr 21 2020 04:20:12.492 PM	flow	ifav201- leaf3	For flow from 80.10.1.135 port 60372 to 64.102.6.247 port 53, packet drop is detected due to forward drop.	true


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

## Details Work Pane

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

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

## Top Navigation Pane

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

### Add a Bookmark

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

### View a Bookmark

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

### Delete a Bookmark

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



# Site Dashboard

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

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

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

## Custom Dashboard

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

### Create a Custom Dashboard

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

There is no limit for number of custom dashboards.

## Add Views on to the Custom Dashboard

1. Click any detailed view from the left navigation pane, for example, resource detail, event detail, flow detail, dashboard view, or any specific view.
2. Click the pin icon on the right top navigation pane.
  - To pin to an existing custom dashboard, check the box for the existing dashboard.
  - Or, to create a new custom dashboard, click **Add**. Enter a unique name in the text box.
3. Click **Save**.

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

## View the Custom Dashboard

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

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

## Delete Views from the Custom Dashboard

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

# Dashboard Inventory

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

Property	Description
<b>Site Anomaly Score</b>	Displays the health of the site through the anomaly score.
<b>Leaf Nodes</b>	Displays the total number of leaf nodes in the site with anomalies.
<b>Spine Nodes</b>	Displays the total number of spine nodes in the site with anomalies.
<b>Controllers</b>	Displays the total number of Cisco APIC in the site.

- Toggle between **Anomaly Score** and **Firmware**. Each node type display anomaly breakdown based on the detected firmware versions instead of the breakdown by anomaly scores.
- Click **Leaf Nodes**, **Spine Nodes**, and **Controllers** to view the details of the individual nodes in

the site from *Browse Nodes* work pane.

## Dashboard Timeline

The timeline displays various anomalies that occurred during the entire cycle of user selected time range. The graph displays the time zones when the anomalies occurred.

- On the **Timeline** Dashboard click the anomaly dots on the timeline at a particular time. The side pane lists the various anomalies at the selected time.
- Click **Analyze**, to display the **Anomaly Analytics** page.

The **Anomaly Analytics Details** page describes the life span of the anomaly, when the anomaly is created, cleared, estimated impact, and recommendations.

- Choose **Analyze Buffer** for anomaly time buffers. The life span displays the graph for the buffer time before and after the anomaly occurred.
- Toggle between **Current** and **Detection Time**. The estimated impact displays the detection time.
- Toggle between graphical or tabular view on the mutual occurrences section.

The mutual occurrences section displays the system view of the anomaly. The comparison chart describes the other faults, events, and audit logs that occurred at the same time this anomaly occurred.

The in-depth analysis section displays the resource utilization view of the anomaly. The comparison chart describes the statistics of the resource utilization for various resource types that is of interest to the anomaly. For example: DOM statistics.

The comparison charts also describe other related resource utilization information for anomaly analysis. For example: Compare and analyze statistical details such as flow configuration, interface utilization ingress, and interface utilization egress that are related to the anomaly type, which lets the user analyze the system resource utilization.

## Configure Analysis

1. Click **Dashboard > Timeline > Analyze** on the side pane.
2. Click **Configure Analysis** to analyze anomalies on nodes with a customizable graph. Select and add objects for each node to compare resource utilization for various resources.
3. On the Chart Selection Table, click **Add Chart** and then select **Chart Type** and **Chart Name**.
4. Select resource types such as Statistics, Environmental, Resources, and Flows. For each resource type, select resources such as DOM, FCS, CPU, Memory, and so on for the nodes with the anomalies.
5. Check the box against the added charts and click **Save** to save all added charts.
6. Click **Save**.

The comparison chart updates automatically and displays the resource utilization for the selected nodes with the anomalies. You can compare and analyze resources for the selected nodes with the

anomalies.

## Site Dashboard Anomalies

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

Property	Description
<b>Anomalies by Category</b>	Displays the number of Anomalies by their Category. Anomaly categories include: <ul style="list-style-type: none"><li>• Flow Analytics</li><li>• Utilization</li><li>• Environmental</li><li>• Statistics</li><li>• Endpoints</li></ul>
<b>Anomalies by Severity</b>	Displays the number of Anomalies (internal site failures) and their severity level. Clicking on the area shows detail fault information, such as <b>Node</b> and <b>Anomaly Score</b> . <ul style="list-style-type: none"><li>• Critical</li><li>• Major</li><li>• Minor</li><li>• Other</li></ul>
<b>Top Nodes by Anomaly Score</b>	Displays the overview of top nodes and their anomaly scores. The anomaly scores are based on the features that contribute to the anomaly.

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

## Browse Anomalies

The Browse Anomalies pane displays the graph with top nodes by anomaly score based on Type and Severity.

The page also displays the overview of the individual nodes in the site with severity, detection time, resource type, node name, description, cleared 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 anomaly, and estimated impact with a report on the interfaces, and applications that were affected.

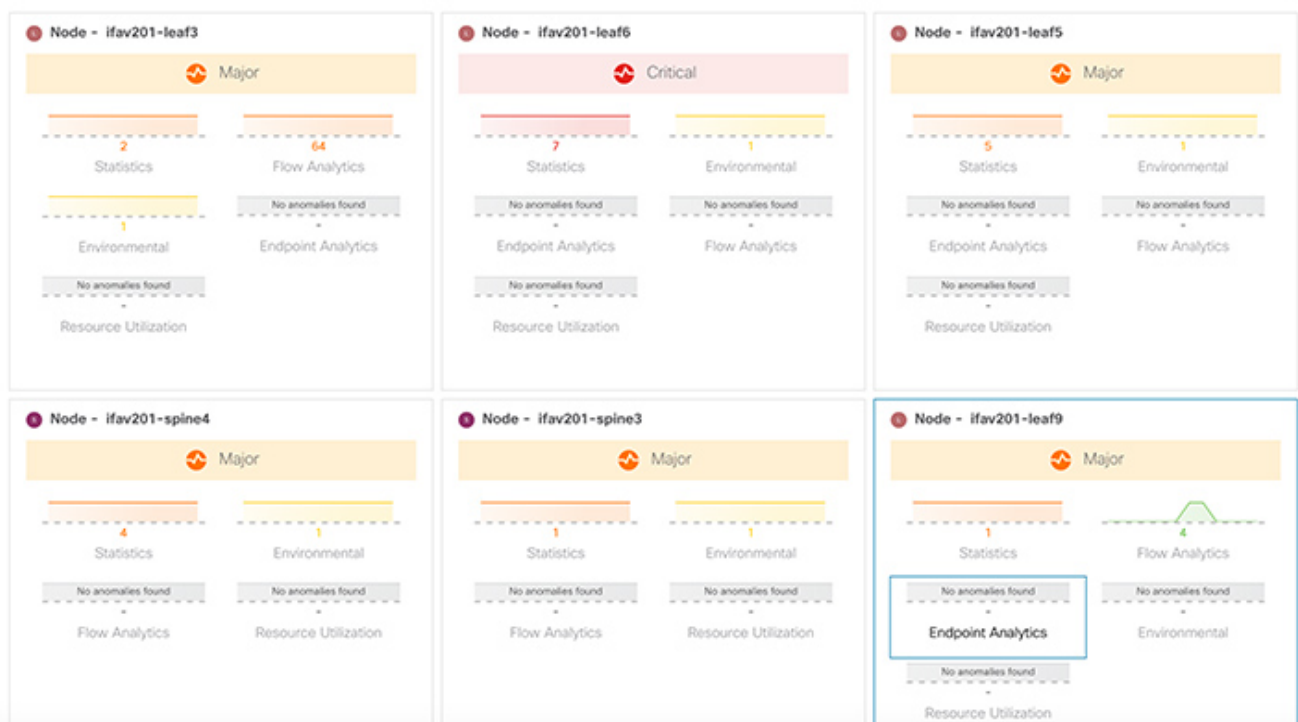
- Click **View Report** to see the details of the interfaces that were affected.
- On the **Anomaly Details** page for the selected node, click the ellipses icon on the right top navigation pane for additional related information for the node such as, Flows, Statistics, Resources, Anomalies, Endpoint 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.

## Top Nodes by Anomaly Score

Navigate to the **Top Nodes by Anomaly Score** section on the **Site Dashboard** page.

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.

Top Nodes by Anomaly Score



## Anomaly Score and Anomaly Precedence

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

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

- A Leaf node has a critical anomaly and another Leaf node has nine major anomalies. In this

case the Leaf node with nine major anomalies takes precedence over the Leaf node with a critical anomaly.

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

## Browse Anomaly Filters

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

You can refine the displayed anomalies by the following filters:

- Detection Time - Display only anomalies with a specific detection time.
- Last Seen Time - Display only anomalies with a specific time.
- Description - Display only anomalies with a specified description.
- Cleared - Display only anomalies with cleared or uncleared status.
- Nodes - Display only anomalies for specific nodes.
- Category - Display only anomalies from a specific category.
- Resource Type - Display only anomalies of a specific resource type.
- Severity - Display only anomalies of a specific severity.

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.

## Topology Dashboard

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

The Topology feature is a Beta feature available in Cisco Network Insights for Resources app tab when Beta feature set is enabled.

The topology view represents the stitching between nodes deployed in a Virtual Machine, where these nodes are connected to the Cisco ACI site.

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

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

- Name - Display only nodes with a specific name.
- Tenant - Display only nodes with a specific tenant.
- Application Profile - Display only nodes with a specified profile.
- EPG - Display only nodes for a specific EPG.
- VRF - Display only nodes from a specific VRF.
- BD - Display only nodes of a specific bridge domain.
- Contract - Display only nodes of a specific contract.
- Endpoint - Display only nodes for a specific endpoint.
- IP - Display only nodes for a specific IP address.

Use the operators for filter refinement.

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

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


# Devices

## Browse Nodes


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

- Click *Node* for the node detail view. The *Node Overview* section displays the top five resources in each Network Insights Analytics - Resource Utilization, Environmental, Statistics, Flow analytics, Event 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 comparison chart 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 displays the overview of the individual nodes in the site with node name, switch models, node type and other details.

- Click *Node* for the node summary pane to display all the gathered information for the selected node.
- Click the  on the right top corner of the summary pane to show the Node Details page. The Node Details page displays General Information, Node Overview, and Anomalies.

The *Node Overview* section displays the top five resources in each Network Insights Analytics - Resource Utilization, Environmental, Statistics, Flow analytics, Event Analytics, and Endpoint Analytics with the break down of the faults and events 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 Flow Records](#) work pane, which filters the flows to view the top nodes by flow anomalies.
- Click **Statistics for the node** to open [Browse Statistics](#) pane, which filters the flows to view the top nodes by interface utilization.



# Cisco Network Insights for Resources System

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

- **Resources** —Site 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 nodes and spine nodes are displayed based on the factors that produced the high utilization.

Property	Description
<b>APIC Capacity</b>	Displays operational capacity for Cisco APIC objects in the site.
<b>Top Nodes by Utilization</b>	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
<b>Top Nodes by</b>	Displays the top nodes by: <ul style="list-style-type: none"> <li>• MAC (learned)</li> <li>• IPv4 (learned)</li> <li>• IPv6 (learned)</li> <li>• IPv4 Host Routes</li> <li>• IPv6 Host Routes</li> <li>• Multicast Routes</li> <li>• Endpoint Group</li> <li>• Bridge Domain</li> <li>• VRF</li> <li>• Port Usage</li> <li>• Ingress Port Bandwidth</li> <li>• Egress Port Bandwidth</li> <li>• LPM</li> <li>• Policy TCAM</li> <li>• VLAN</li> </ul>
<b>Operational Resources</b>	Displays a list of operational resources based on resource utilization. List information includes: <ul style="list-style-type: none"> <li>• Anomaly Score</li> <li>• Node</li> <li>• MAC (learned)</li> <li>• IPv4 (learned)</li> <li>• IPv6 (learned)</li> <li>• IPv4 Host Routes</li> <li>• IP v6 Host Routes</li> <li>• Multicast Routes</li> </ul>

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

## 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
<b>Top Nodes by Utilization</b>	Displays the percentage utilized per component: <ul style="list-style-type: none"> <li>• CPU</li> <li>• Memory</li> <li>• Temperature</li> <li>• Fan Utilization</li> <li>• Power Supply</li> <li>• Storage</li> </ul>

## 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
<b>Top Nodes by</b>	Displays a graph of the top nodes by: <ul style="list-style-type: none"> <li>• CPU</li> <li>• Memory</li> <li>• Temperature</li> <li>• Fan Utilization</li> <li>• Power Supply</li> <li>• Storage</li> </ul>

<b>Property</b>	<b>Description</b>
<b>Environmental Resources Summary</b>	Displays a list of the top node by anomaly score. Table columns include: <ul style="list-style-type: none"><li>• Anomaly Score</li><li>• Node</li><li>• CPU</li><li>• Memory</li><li>• Temperature</li><li>• Fan Utilization</li><li>• Power Supply</li><li>• Storage</li></ul>

# Cisco Network Insights for Resources Operations

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

- **Statistics** —Switch nodes interface usage and protocol statistics.
- **Flow Analytics** —Telemetry information collected from various devices in the site that were added to the site.
- **Endpoint Analytics** —Displays endpoint anomalies for the nodes collected across the entire site that were added to the site.
- **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
<b>Top Nodes by Interface Utilization</b>	Displays the top nodes based on the combined bandwidth utilization of its interfaces.
<b>Top Nodes by Interface</b>	Displays the top nodes and lists the transmit and receive bandwidth utilization for each of its 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.

*Table 2. Total Audit Logs, Events, and Faults*

<b>Property</b>	<b>Description</b>
<b>Creation Time</b>	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"> <li>• <b>Critical</b>—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.</li> <li>• <b>Major</b>—Serious problems exist with one or more components. These issues should be researched and fixed immediately.</li> <li>• <b>Minor</b>—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.</li> <li>• <b>Warning</b>—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.</li> <li>• <b>Info</b>—A basic notification or informational message, possibly independently insignificant.</li> <li>• <b>Cleared</b>—A notification that the condition that caused the fault has been resolved, and the fault has been cleared.</li> </ul>
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.

## Statistics Analytics Limitations

The following are Cisco NIR application limitations for Interface Statistics.

- Interface Statistics does not support the `eqptIngrCrcErrPkts5min` counter.
- Interface Statistics anomalies are not generated for port channel interface.



## 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 the 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.

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

The port channel is an aggregate of physical interfaces and they can be statistically channeled 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 a row in the **Interface Statistics** page for the side pane to display additional details of the node such as, node name, port channel name, operational status, and admin state. The page also displays the anomalies, traffic, and member interfaces associated in the port channel.

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

## Protocol Statistics

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

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

## Multicast Protocol Statistics

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

### Protocol Independent Multicast

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

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

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

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

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

- Double-click a row for the side pane to display additional details about the specific multicast PIM domain. This includes VNI IDs, flags that are enabled, various errors, and statistics information.

The **Multicast PIM Interfaces** section displays the interfaces that are enabled with PIM. It displays the interface name, tenant name, IP address, designated router address, neighbor addresses, and errors.

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

The **Multicast PIM Groups** section displays the PIM group related details such as source, group

address, tenant, VRF, incoming interfaces, RPF neighbor, outgoing interfaces, flags, and status of the PIM group. The status is inactive if there is no data flowing through the PIM group.

## Internet Group Management Protocol

Use filters from browse statistics page to display the summary of a specific node for IGMP. The **General Information** section displays the anomaly score, protocol, number of interfaces, number of nodes, and node name for which the protocol belongs.

The **Anomalies** section displays the anomalies that are generated on a node specific to IGMP. The errors related to IGMP are not displayed for a specific node.

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

- Double-click a row for the side pane to display additional details. This includes VRF ID, statistical data about error counters, flags that are enabled on IGMP, and packets received that are specific to the node.

The **Multicast Groups** section displays the IGMP groups related details such as source, multicast group, tenant, VRF name, last reporter, and outgoing interface specific to the IGMP group.

## Internet Group Management Protocol Snoop

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

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

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

The **IGMP Snoop Instances** section displays about a bridge domain such as tenant, VRF, BD, admin state, querier address, querier version, routing state (enabled or disabled), site querier state (enabled or disabled), and summary of errors.

- Double-click a row for the side pane to display other configured details specific to IGMP Snoop instance. This includes statistical details and various error counters specific to the IGMP Snoop instance.

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

# Flow Analytics

The Flow Analytics section of the Cisco NIR application displays the telemetry information collected from various devices in the site that were added to the site.

## Flow Analytics Overview

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

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

## Flow Analytics 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 [Cisco NIR Release Notes Compatibility Information](#) section.

## Flow Analytics Limitations

- The Cisco NIR app captures the maximum anomaly score for a particular flow, for the entire cycle of the user specified time range.
- For unknown IP address, the traffic from spine nodes will be dropped and flow records are not generated in Flow Telemetry.
- The packet count represents the number of packets entering the site for a particular flow do not match the source and destination IP address.
- Cisco Nexus 9300-EX platform switches do not support VRF based filtering. They support only bridge domain or subnet filtering of flow telemetry rules. Cisco NIR app gets the flows from the subnet if the subnet is across multiple VRFs.

The following are Cisco NIR application limitations for Flow Analytics on **Cisco Nexus EX** switches. For details on Flow Telemetry hardware support, see [Cisco NIR Release Notes Compatibility Information](#) section.

- Output port information for outgoing traffic from N9K-C93180YC-EX, N9K-C93108TC-EX, 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 supported.

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

- The spine switches do not export shared service flow records (VRFA to VRFB and vice-versa). Due to this limitation Cisco NIR app flow path summary will be incomplete.
- 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 node traffic (with spine node), 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 node traffic (with spine node), 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.

## Flow Analytics Dashboard

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

Property	Description
<b>Top Nodes by</b>	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.
<b>Top Nodes by Flow Anomalies</b>	Flow telemetry and analytics gives in-depth visibility of the data plane. The flow analytics collects the flow records streamed from the nodes and converts to understandable EPG-based flow records. Top nodes by flow anomalies displays the nodes in the network with the most anomalies.

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

### Flow Record Details

Click the node card in the **Top Nodes by Flow Anomalies** to display the flow record details. The

details include anomaly score, record time, flow type, aggregated flow information, summary of anomalies, path summary, and charts for flow properties.

**Flow Record Information**

ANOMALY SCORE	RECORD TIME	FLOW TYPE	PROTOCOL	LATENCY (µs)	PACKET DROP INDICATOR	FLOW MOVE INDICATOR
Info	Jul 16 2020, 09:52:49.827 AM	IPv4	TCP	0	0	0

[Show more details](#)

---

**Aggregated Flow Information**

ANOMALY SCORE	COUNT OF FLOW RECORDS	START TIME	END TIME	FLOW TYPE	PROTOCOL	LATENCY (µs)	PACKET DROP INDICATOR	FLOW MOVE INDICATOR
Info	8	Jul 16 2020, 09:52:49.827 AM	Jul 16 2020, 10:34:56.655 AM	IPv4	TCP	0	0	0

**Source**

ADDRESS	PORT
130.120.1.16	43484

**Destination**

ADDRESS	PORT
99.99.102.65	80

**Ingress**

NODES	TENANT	VRF
orion11-pod4-Loc3-RL4	te120	CTX1

**Egress**

NODES	TENANT	VRF	EPG
-	te120	CTX1	EXT-EPG120

**EPG**

PACKETS	BYTES	BURST MAX (Bytes)

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

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

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

**Path Summary**

Source: 130.120.1.16 (Port: 43484, EPG: CTX1\_BD1\_EPG1) → orion11-pod4-Loc3-RL4 (N/A eth1/99) → MPOD-SITE2-IPN-CALGARY (ethernet1/9 N/A) → unknown-spine (N/A N/A) → Destination: 99.99.102.65 (Port: 80, EPG: EXT-EPG120)

[View reverse path](#)

---

**Related Details**

**Average Latency By:** Trending

Y-axis: Average Latency (µs). X-axis: Time. Data point: 130.120.1.16:43484.

**Burst By:** Trending

Y-axis: Burst (Bytes). X-axis: Time. Legend: Ingress burst max (blue), Egress burst max (pink).

## Browse Flow Records

The Browse Flow Records page displays Site flows by Anomaly Score, Packet Drop Indicator, Average Latency, and Flow Move Indicator. The graph displays a time series plot for flow analytics properties recorded in the entire site. The node flows recorded for Top Sources and Top Destinations are also shown.

Property	Description
<b>Filters</b>	<p data-bbox="801 161 1460 241">Display the node flow observations using the following filters:</p> <ul data-bbox="826 277 1123 1066" style="list-style-type: none"><li data-bbox="826 277 1023 309">• Record Time</li><li data-bbox="826 338 938 369">• Nodes</li><li data-bbox="826 398 991 430">• Flow Type</li><li data-bbox="826 459 963 490">• Protocol</li><li data-bbox="826 519 1059 551">• Source Address</li><li data-bbox="826 580 1010 611">• Source Port</li><li data-bbox="826 640 1123 672">• Destination Address</li><li data-bbox="826 701 1070 732">• Destination Port</li><li data-bbox="826 761 1027 792">• Ingress Node</li><li data-bbox="826 822 1051 853">• Ingress Tenant</li><li data-bbox="826 882 1011 913">• Ingress EPG</li><li data-bbox="826 943 1016 974">• Egress Node</li><li data-bbox="826 1003 1040 1034">• Egress Tenant</li><li data-bbox="826 1064 1002 1095">• Egress EPG</li></ul>

Property	Description
<b>Site Flows by</b>	<p>A time series plot for flow analytics properties such as anomaly score, average latency, packet drop indicator, and flow move indicator that are recorded in the entire site for the time interval you selected. The node flows recorded for <b>Top Sources</b> and <b>Top Destinations</b> are also shown.</p> <ul style="list-style-type: none"> <li>• <b>Anomaly Score</b>—The score is based on the number of detected anomalies logged in the database.</li> <li>• <b>Packet Drop Indicator</b>—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.</li> <li>• <b>Latency</b>—The time taken by a packet to traverse from source to destination in the site. A prerequisite for site latency measurement is that all the nodes shall be synchronized with uniform time.</li> <li>• <b>Flow Move Indicator</b>—The number of times a Flow moves from one leaf node to another. The first ARP/RARP or regular packet sent by that endpoint appears as a flow entering the site through the new leaf node.</li> </ul>

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

## Endpoint Analytics

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

## Endpoint Analytics Overview

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

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



information and correlation to virtual machine and hypervisor.

- The policies applied on an endpoint - view the discover configuration and operational information of the endpoint.

The following anomalies are detected as part of endpoint analytics:

- The rapid endpoint moves across nodes, interface, and endpoint groups.
- Detect 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 site.

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

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

## Endpoint Analytics Guidelines and Limitations

- Endpoint Analytics is not supported for endpoint groups when `allow-micro-seg` and `useg eggs` are enabled.
- In the endpoint history, the anomaly records with 'Aged out' status for an endpoint move are displayed healthy or green while anomaly is active.
- Endpoint Analytics is not supported for Policy Based Redirect graph deployed in your network.
- Endpoint Analytics is not supported for dot1Q tunnel.

## Browse Endpoint Analytics

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

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

- 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.
- 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.

## Endpoint Analytics Summary

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

Click an endpoint in the summary table to display a side pane with general information, configuration, and operational details of the endpoint.

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

Double-click the endpoint in the summary table to display the *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/L3Out, BD, VRF, and Encap details for the selected endpoint. The operational section displays the Node name, Interface, VM id, hypervisor id, and other details.

The following anomalies are detected as part of endpoint analytics:

- The rapid endpoint moves across nodes, interface, and endpoint groups.
- Detect missing endpoints that fail to get learnt after a node reboot.
- Detect endpoints that have duplicate IP address.

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

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

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

## 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, events by severity, and faults by severity.

Property	Description
<b>Event Analytics by time</b>	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.
<b>Audit Logs by Actions</b>	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.
<b>Events by Severity</b>	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.

Property	Description
<b>Faults by Severity</b>	<p data-bbox="802 163 1201 199">Displays all faults by severity.</p> <p data-bbox="802 248 1457 739">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.</p>

## 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.

<b>Property</b>	<b>Description</b>
<b>Audit Logs by Action</b>	Displays audit logs by: <ul style="list-style-type: none"> <li>• Deletion</li> <li>• Creation</li> <li>• Modification</li> </ul>
<b>Events by Severity</b>	Displays all events based on severity: <ul style="list-style-type: none"> <li>• Critical</li> <li>• Major</li> <li>• Minor</li> <li>• Other</li> </ul>
<b>Faults by Severity</b>	Displays all faults based on severity: <ul style="list-style-type: none"> <li>• Critical</li> <li>• Major</li> <li>• Minor</li> <li>• Other</li> </ul>

# Third Party Integration for Cisco NIR

## About AppDynamics Integration

Cisco Network Insights for Resources app provides insights to monitor the most common and complex challenges in the maintenance of infrastructure operations, which involves monitoring, troubleshooting, identification and resolving the network issues.

AppDynamics provides application performance management (APM) and IT operations analytics that helps manage the performance and availability of applications in the data center. AppDynamics provides the required metrics for monitoring, identifying, and analyzing the applications that are instrumented with AppDynamics agents.

AppDynamics hierarchy consists of the following components:

- Network Link—Provides the functional means to transfer data between network entities.
- Node—A node is a working entity of an application and is a process running on a virtual machine.
- Tier—A tier is a grouping of nodes into a logical entity. Each tier can have one or more nodes.
- Application—A set of tiers make up an application.
- Controller—A controller consists of a set of accounts with each account comprising a list of applications. Each account in the controller is an instance.

Integrating AppDynamics allows Cisco NIR to collect operational data and metrics of the applications monitored by AppDynamics, and then correlate the collected information with the data collected from the Cisco ACI site.

In a scenario where an application communicates through the Cisco ACI site, AppDynamics provides various metrics about the application and the network, which can be used to isolate the cause of the anomaly. The anomaly can be in the application or the underlying network. This in turn allows network operators to monitor the network activity and detect anomalies.

The AppDynamics agents are plug-ins or extensions, hosted on the application. They monitor the health, and performance of the network nodes and tiers with minimal overhead, which in turn report to the AppDynamics controller. The controller receives real-time metrics from thousands of agents and helps troubleshoot and analyze the flows.

Cisco NIR app connects to the AppDynamics controller and pulls the data periodically. This data from AppDynamics controller, rich in application specific information is fed to the Cisco NIR app, thereby providing Network Insights for the traffic flowing through the Cisco ACI site.

From AppDynamics, you can create your own health rule on the available metrics, which contributes to the overall anomaly score of the entity.

The integration of Cisco NIR with AppDynamics enables the following:

- Monitoring and presenting AppDynamics hierarchy in Cisco NIR.

- Gathering and importing network related metrics into the Cisco NIR application.
- Presenting statistics analytics, flow analytics, and topology view on the data collected from AppDynamics controller.
- Detecting anomaly trends on metrics collected from AppDynamics controller and raising anomalies on detection of such events.

## Installing AppDynamics

Before you begin using Cisco NIR application **Integrations**, you must install AppDynamics Application Performance Management and Controller. See [Getting Started](#) for details.

## Onboard AppDynamics Controller

Use this procedure to onboard a AppDynamics Controller on to the Cisco NIR application using GUI.

### Before you begin

- You must have installed AppDynamics application and controller.
- You must have administrator credentials for Cisco NIR application.
- You must have user credentials for AppDynamics controller.

### Procedure

1. Click **Dashboard** on the left navigation pane.
2. Select a site at the top of the **Site** dashboard to onboard the AppDynamics controller.
3. Click the **Settings** icon on the far-right side of the work pane.
4. Click **Third Party Integrations**.
5. Click **Add Integration** on the far-right side of the work pane.
  - Enter Controller Name, Controller IP, and Controller Port. Controller Name can be alphanumeric and spaces are not allowed.
  - Select Controller Protocol.
  - Enter AppDynamics Account Name, User Name, and Password. Cisco NIR app supports only password based authentication while onboarding controller.
  - Click **Save**.
6. Click **Done**.

### AppDynamics Controller in Cisco NIR

On the **Third Party Integration** work pane, the active status indicates that the controller is active to fetch data. The down status indicates that the Cisco NIR will not fetch data from the AppDynamics controller. You can hover over the red dot to see the reason for down status. You can delete a controller on the Third Party Integration work pane from **Actions**.

Each controller supports multiple account names for the same host name. Each account name supports multiple applications monitored by the controller. Therefore, a controller can support multiple applications monitored by AppDynamics.

## Cisco NIR and AppDynamics Integration Dashboard

The AppDynamics Dashboard allows you to onboard controllers and presents a view of the **Top Applications by Anomaly Score** along with various metrics. Once a controller is onboarded, data related to applications monitored by that controller is pulled by Cisco NIR. It can take up to 5 minutes for the first set of data to appear on the GUI. The AppDynamics health state information provided for each entity is aggregated and reported by Cisco NIR on the dashboard.

The AppDynamics dashboard displays the overview of the applications monitored by the AppDynamics controller.

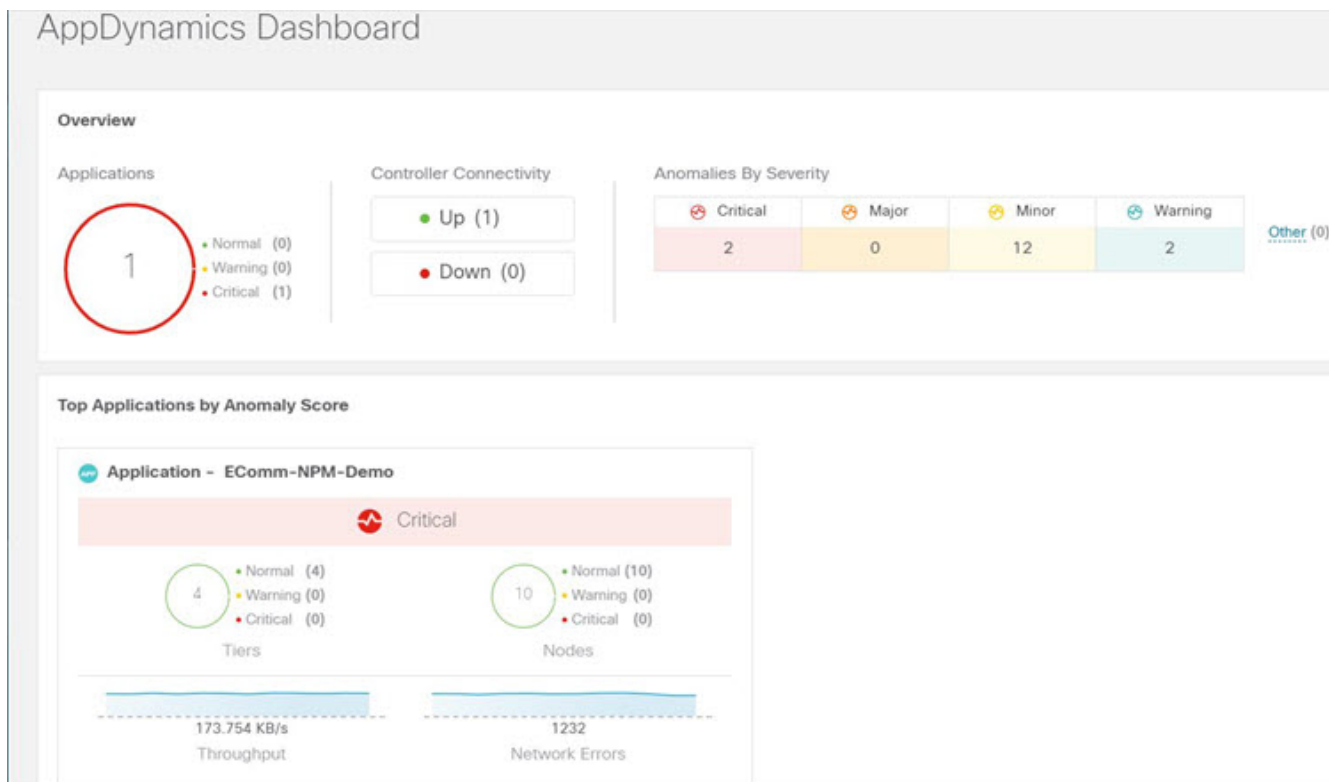
Controller Connectivity— Represents the number of integrations that are **Up** or **Down**.

Anomalies by Severity—The Cisco NIR app runs statistical analytics on the metrics received from the AppDynamics controller.

The **Top Applications by Anomaly Score** displays top six out of all the applications based on the anomaly score.

- Click the number on **Anomalies by Severity** to see the [Browse Anomalies](#) page.

The application widget displays the top application by anomaly score. The anomaly score of the application as computed in Cisco NIR, health state of tiers and nodes as reported by AppDynamics is also included.




Click the widget for additional details about the monitored application.



# Browse AppDynamics Integration Application

The browse page presents the applications and history of the anomaly score plotted on a timeline. Detailed information including operational, statistics, and metrics, for each tier or application is also presented.

The summary pane lists the anomaly score, controller name, account, application name, number of tiers, number of nodes, throughput, TCP loss, and errors.

- Click **Number of Tiers** in the summary pane for the side pane to list the available tiers. Click each tier from the list to display health score, number of nodes, and usage statistics.
- Click **Number of Nodes** in the summary pane for the side pane to list the available nodes. Click each node from the list to display statistics about the node.
- Click **Application Name** in the summary pane for the side pane to display additional details such as general information of the application, controller name, controller IP, account name, health of the tier, health of the node, business transaction health, and usage analytics.
- On the side summary pane, click the  icon on the right top corner to open **AppDynamics Application** details page. This page displays application statistics details such as anomaly score, application tiers summary, application nodes summary, network charts for the node communication, and summary table of anomalies.

The **Application Network Links** table shows how the different components of AppDynamics application network flow map are communicating among each other. Detailed information about a network link, including flow counts and anomalies are used for further analysis.

- Double-click each row in the summary pane for the particular AppDynamics monitored application to display **AppDynamics Application View** page.

## AppDynamics Application View

The AppDynamics Application View page presents an overview of the application health state including tier health, node health, and business transaction health.

The **Application Statistics** section displays the graphical representation of the flow properties and a timeline graph representing the properties.

The **Tiers** section displays the health state of the tiers in the application. Click each row in the tier section for the side panel to display additional tier usage details.

The **Nodes** section displays the health state of the nodes in the application. Click each row in the node section for the side panel to display additional node usage details.

The **Application Network Links** section displays the link summary for the nodes.

- Click **Network Connection** for the side panel to display additional flow connection details.
- Click **Browse Network Flows** on the side pane to navigate to [Browse Flow Records](#) with the flow properties set in the filter.

The **Anomalies** section summarizes the anomalies with severity and other essential details of the anomaly.

1. Click each row in the **Anomalies** section for the side pane to pop up with additional details of the anomaly.
2. Click **Analyze** for in-depth analysis, mutual occurrences, estimated impact, lifespan, and recommendations on the anomaly.
3. Click **Done**.

## Guidelines and Limitations

- After Cisco NIR app upgrade, AppDynamics takes about 5 minutes to report the information in AppDynamics UI.
- Connectivity from Cisco NIR to AppDynamics controller using proxy is not supported.
- The health and count of AppDynamics business transactions displayed in the application details page do not match the flow count in Cisco NIR app.
- Cisco NIR does not support fabric topologies as transit-leaf does not have the VRF deployed and flow table in transit-leaf will not export the flow record to Cisco NIR. Hence Cisco NIR will not stitch the path fully and will not display complete path summary with all the information.

## Topology View

The topology view represents the stitching between nodes where these nodes are connected to the Cisco ACI site.

The topology view includes the application nodes and leaf nodes. Toggle between show or not show the nodes with anomaly score. The anomaly score is represented by the dot in the topology.

The topology view represents a hierarchical view of **Application > Node > Cisco ACI Leaf** and the links between them with a logical or network view of how various objects are related.

## Anomalies

From AppDynamics application, you can create your own health rule on the available metrics, which contributes to the overall anomaly score of the entity. If the health rules are violated and a violation is generated by the AppDynamics controller, then Cisco NIR pulls these health violations and generates anomalies on these violations.

The anomalies in the summary table include the following:

- Anomalies raised on the metrics from the AppDynamics controller.
- Health violation on the network metrics that the AppDynamics controller raised.
- Anomalies at the application level and node level.

If there is an anomaly on the interface of application(s) impacted by the interface, then an anomaly is identified and shown.

Depending on the anomaly score and the level at which the anomaly occurs, the corresponding flows impacted are identified. Information related to the flow metrics with the Cisco ACI leaf information enable statistics analytics, pin point the source of the anomaly, whether it is the application or network, and the impacted entities.



# Upgrade Cisco Network Insights for Resources

## Upgrade Cisco NIR on Cisco APIC

### Before you begin

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

### Procedure

1. Log in to the Cisco APIC GUI with admin privileges.
2. Click the **Admin > Downloads** tab.
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.
4. Enter the name of the download file in the **Download Name** field.
5. In the **Protocol** field, choose **Secure Copy**.
6. In the **URL** field, enter the path to the download file image location.
7. Enter your name and password in the **Username** and **Password** fields.
8. Enter **Submit**.
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.
10. After installing, click the **Operations > NIR** tab at the top of the GUI.
11. When the application installation is completed, then click the **Apps** tab.

The Cisco NIR application upgrading progress dialog appears.

12. Click **Open** from the Cisco NIR application dialog.

This upgrade procedure preserves the user data from the previous installation. The Cisco NIR app detects and adds the onboarded site automatically since the data is already available.


After you upgrade from Cisco NIR 2.2.1 to Cisco NIR 2.2.2 on Cisco APIC, you can not downgrade Cisco NIR app.

## Upgrade Cisco NIR on Cisco Application Services Engine

## Before you begin

- 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.

## Procedure

1. Log in to the Cisco Application Services Engine GUI with admin privileges.
2. Click **Apps** tab on the left navigation bar.
3. Click **Actions > Upload App** from the far-right side.
4. In the **URL** enter the http address and click **Upload**. Click **Refresh** icon  on the far-right side of the Downloads work pane to check the upload status.
5. When the application installation is successful, the application icon appears with a **Launch App** button.
6. Click the ellipses icon on the right top Cisco NIR application tile.
7. Click **Available Versions**.

The popup window displays the available Cisco NIR application versions.

8. Click **Activate** on the upgrade version.

The Cisco NIR application preparing to upgrade and finishing upgrade dialog appears.

9. Once the new version appears on the Cisco NIR application tile, the upgrade is complete.
10. Click **Launch** to launch the upgraded Cisco NIR App.

This upgrade procedure preserves the user data from the previous installation. The Cisco NIR app detects and adds the onboarded site automatically since the data is already available.

After you upgrade from Cisco NIR 2.2.1 to Cisco NIR 2.2.2 on Cisco Application Services Engine, you can not downgrade Cisco NIR app.

Note: The Cisco NIR app release 2.2.2 can be launched only on Cisco Application Services Engine. All Cisco NIR app lifecycle operations such as install, enable, launch, and upgrade are available from the Cisco Application Services Engine GUI. You cannot cross launch the Cisco NIR app from Cisco APIC.

## Upgrade Paths for Cisco NIR Application

Table 3. Supported Upgrade Paths for Cisco Network Insights for Resources Application

From	To
Cisco NIR on Cisco Application Services Engine 2.2.1	Cisco NIR on Cisco Application Services Engine 2.2.2

<b>From</b>	<b>To</b>
Cisco NIR on Cisco APIC 2.2.1	Cisco NIR on Cisco APIC 2.2.2

# Cisco NIR REST API Examples

## 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 information.*

```

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": [
        ""
    ]
}
]
],
"nodeName": [
    "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/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 anomaly scores of the fabric,
  default:'no'
  history                 => Requires the timeseries data of sum(anomaly scores,
  default:'no'
  granularity             => applicable if history = "yes" , granularity 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
                }
              ]
            }
          ]
        }
      ],
      "sourceName": "phys-[eth1/11]",
      "entries": [
        {
```

<--snip-->



```
    "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/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/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/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/telemetry/utilizationnodeDetails.json'
Response   :
  {
    "totalResultsCount": 157,
```

```

"totalItemCount":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 -->
}
]
}

```

# Troubleshooting Cisco NIR application

## Troubleshooting Cisco NIR Common GUI Issues

- The Cisco NIR app has the ability to display historical data. The specific time duration can be selected from the available calendar to see data within that particular time range.
- The majority of issues will be due to receiving data from the APIs other than what was expected. Opening the **Developer Tools Network** tab and repeating the last action will show the API data received. If the issue is with the APIs, then troubleshooting will need to continue on the backend.
- If the API requests and responses are accurate then check the **Developer Tools Console** tab for any errors.
- After initial installation the application needs time to start. During this time, the GUI may exhibit incomplete or unstable behavior. It is recommended to wait several minutes before starting to use the application.
- Take screenshots just before and just after reproducing an issue. 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 sites then this means the `fabrics.json` API is not responding or not returning any sites.
- If the site anomaly score does not agree with reported anomalies, or the node counts are incorrect, then check the `fabricsSummary.json` response for the site `anomalyScore` value, and check the `nodes.json` response for the types and counts of nodes reported.
- If the expected sites are not shown in the site selection dropdown, first verify that they are not included in the `fabrics.json` response entries, then rerun setup and edit the data collection setup configuration to view the state of the configured sites. Make sure the appropriate sites are enabled and that no errors are reported. This data comes from the `get_nir_fabrics` request.
- For Flow Analytics issues make sure the following requirements are met:
  - The `capability.json` request is made when the GUI loads and returns true. If it returns false, it means the site does not support this feature.
  - Navigate to **Application Settings** tab and make sure **Flow Collection** has been enabled and verify that the flow collection filters have been correctly configured.
  - On the Cisco Application Services Engine GUI, navigate to **Infrastructure > Sites** and make sure site is configured with correct Cisco APIC In-Band EPG name.
  - To verify the MOs are using `visore`, navigate to `uni > site > flowcol` to check the configuration and check the classes `telemetrySelector`, `telemetrySubnetFltGrp`, and `telemetrySubnetFilter`.
  - Navigate to **Collection Status** tab and check if the nodes are returning flow telemetry.

# 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 4. Total Audit Logs, Events, and Faults

Property	Description
Creation Time	The day and time of when the audit log, event, or fault instance occurred.
Severity	<p>The current severity level of the event. The levels are:</p> <ul style="list-style-type: none"><li>• <b>Critical</b>—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.</li><li>• <b>Major</b>—Serious problems exist with one or more components. These issues should be researched and fixed immediately.</li><li>• <b>Minor</b>—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.</li><li>• <b>Warning</b>—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.</li><li>• <b>Info</b>—A basic notification or informational message, possibly independently insignificant.</li><li>• <b>Cleared</b>—A notification that the condition that caused the fault has been resolved, and the fault has been cleared.</li></ul>
Code	The code that helps to categorize and identify different types of fault instance objects.

Property	Description
<b>Last Transition</b>	The day and time on which the severity last changed. If the severity has not changed, this field displays the original creation date.
<b>Description</b>	Additional descriptive information on the audit log, event or fault.

## Basic Debugging Commands for Cisco NIR on Cisco APIC

```
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
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 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 local-docker-repo/cisco-nir/aci-docker-reg-cisco-com/telemetry/logstash:v1-0-1-827	apic-ifc1	running
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-aggflowdb-2019.01.31.18.00.00 RnIB3S7fTBik007xPhquFw  9  2
0          0    6.1kb            2kb
green open  cisco_nir-sysmetrics-2019.01.31      HBP_iJgsRQyGTy0a-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         6RrCkrhxT60Wz-M8eIfjrw  5  2
0          0    3.4kb           1.1kb
green open  cisco_nir-sysmetrics-2019.01.30     wz3Jif_8SM0hc40r8MEXNg  7  2
41870      0    19.2mb          6.4mb
green open  cisco_nir-fabric_issuesdb          tj-Y0cP4SF20dfMkumqcqQ  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           pqhaqo30Tv6E6y1zBfwYg  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 ZQdM12yxSaaNCdGXW-4Y0g  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#

```

# Basic Debugging Commands for Cisco NIR on Cisco Application Services Engine

```
[rescue-user@cisco-se-1 ~]$ acidiag health
All components are healthy
```

```
[rescue-user@cisco-se-1 ~]$ acidiag health -d
All components are healthy
```

Debug Information

-----

```
kubectl get pods -A -o wide
```

-----

NAMESPACE	NAME	READY	STATUS	RESTARTS	
AGE	IP	NODE	NOMINATED NODE	READINESS GATES	
apigw		apigw-krsn5	4/4	Running	0
2d1h	172.17.27.89	cisco-se-2	<none>	<none>	
apigw		apigw-qk8fc	4/4	Running	0
2d1h	172.17.27.43	cisco-se-3	<none>	<none>	
apigw		apigw-x64xr	4/4	Running	0
2d1h	172.17.27.22	cisco-se-1	<none>	<none>	
cisco-intersightdc		deviceconnector-bb6zm	1/1	Running	2
22d	172.17.27.129	cisco-se-1	<none>	<none>	
cisco-intersightdc		deviceconnector-fdqhm	1/1	Running	0
20d	172.17.27.247	cisco-se-6	<none>	<none>	
cisco-intersightdc		deviceconnector-fjh56	1/1	Running	1
7d23h	172.17.27.208	cisco-se-5	<none>	<none>	
cisco-intersightdc		deviceconnector-hdxrm	1/1	Running	0
20d	172.17.27.228	cisco-se-4	<none>	<none>	
cisco-intersightdc		deviceconnector-tf7v4	1/1	Running	3
22d	172.17.27.85	cisco-se-2	<none>	<none>	
cisco-intersightdc		deviceconnector-w68bf	1/1	Running	3
22d	172.17.27.130	cisco-se-3	<none>	<none>	
cisco-nir		apicagent-557854d59c-67x6b	1/1	Running	0
32h	172.17.27.122	cisco-se-2	<none>	<none>	
cisco-nir		apicagent-557854d59c-tgwt7	1/1	Running	0
32h	172.17.27.180	cisco-se-3	<none>	<none>	
cisco-nir		apicagent-557854d59c-w4d8z	1/1	Running	0
23h	172.17.27.219	cisco-se-1	<none>	<none>	
cisco-nir		apiserver-service-76bd5c4f4-f5g22	1/1	Running	0
32h	172.17.27.133	cisco-se-4	<none>	<none>	
cisco-nir		apiserver-service-76bd5c4f4-s2m4q	1/1	Running	0
32h	172.17.27.193	cisco-se-6	<none>	<none>	
cisco-nir		apiserver-service-76bd5c4f4-vbgm6	1/1	Running	0
23h	172.17.27.236	cisco-se-2	<none>	<none>	
cisco-nir		brain-6745bccbb8-hm55b	0/1	Running	0
23h	172.17.27.171	cisco-se-4	<none>	<none>	

cisco-nir	brain-6745bccbb8-vvj54	0/1	Running	0
32h	172.17.27.86	cisco-se-3	<none>	<none>
cisco-nir	brain-6745bccbb8-vxrdj	1/1	Running	0
32h	172.17.27.156	cisco-se-2	<none>	<none>
cisco-nir	collector-7cdbc5f5699-7jkxk	1/1	Running	0
32h	172.17.27.153	cisco-se-3	<none>	<none>
cisco-nir	collector-7cdbc5f5699-cqfj2	1/1	Running	0
23h	172.17.27.186	cisco-se-1	<none>	<none>
cisco-nir	collector-7cdbc5f5699-h5h7v	1/1	Running	0
32h	172.17.27.232	cisco-se-2	<none>	<none>
cisco-nir	eventcollector-7d6bb7967-4xqh9	1/1	Running	0
32h	172.17.27.161	cisco-se-6	<none>	<none>
cisco-nir	eventcollector-7d6bb7967-h74r4	1/1	Running	0
32h	172.17.27.34	cisco-se-4	<none>	<none>
cisco-nir	eventcollector-7d6bb7967-jqshd	1/1	Running	0
32h	172.17.27.154	cisco-se-2	<none>	<none>
cisco-nir	flinkjm-5977889db5-9m4rk	0/1	Running	0
32h	172.17.27.162	cisco-se-6	<none>	<none>
cisco-nir	flinkjm-5977889db5-jvtpl	0/1	Running	0
32h	172.17.27.238	cisco-se-4	<none>	<none>
cisco-nir	flinkjm-5977889db5-nxmlb	1/1	Running	0
23h	172.17.27.191	cisco-se-2	<none>	<none>
cisco-nir	flinktm-b565fc77c-fk6jb	1/1	Running	0
32h	172.17.27.215	cisco-se-4	<none>	<none>
cisco-nir	flinktm-b565fc77c-kfmrh	1/1	Running	0
32h	172.17.27.126	cisco-se-6	<none>	<none>
cisco-nir	flinktm-b565fc77c-wjvfn	1/1	Running	0
32h	172.17.27.150	cisco-se-1	<none>	<none>
cisco-nir	flowsink-7f49fccccf-7vr2g	1/1	Running	2
32h	172.17.27.142	cisco-se-6	<none>	<none>
cisco-nir	flowsink-7f49fccccf-mf2bt	1/1	Running	4
32h	172.17.27.21	cisco-se-1	<none>	<none>
cisco-nir	flowsink-7f49fccccf-qm7bj	1/1	Running	4
32h	172.17.27.251	cisco-se-4	<none>	<none>
cisco-nir	genie-7d67c95945-kpzjm	1/1	Running	0
23h	172.17.27.200	cisco-se-3	<none>	<none>
cisco-nir	genie-7d67c95945-px59q	1/1	Running	0
32h	172.17.27.242	cisco-se-6	<none>	<none>
cisco-nir	genie-7d67c95945-w4l1t	1/1	Running	0
32h	172.17.27.69	cisco-se-4	<none>	<none>
cisco-nir	health-service-5b9b974ccf-bhcxq	1/1	Running	0
32h	172.17.27.127	cisco-se-4	<none>	<none>
cisco-nir	health-service-5b9b974ccf-chstx	1/1	Running	0
32h	172.17.27.100	cisco-se-1	<none>	<none>
cisco-nir	nginx-6458cf57b8-n9wkj	1/1	Running	0
32h	172.17.27.136	cisco-se-1	<none>	<none>
cisco-nir	nginx-6458cf57b8-rqkbp	1/1	Running	0
23h	172.17.27.190	cisco-se-3	<none>	<none>
cisco-nir	sensei-69c489fdb7-8njpx	1/1	Running	0
32h	172.17.27.76	cisco-se-1	<none>	<none>
cisco-nir	telegraf-7bc5c784cb-2vt5g	1/1	Running	0

32h	172.17.27.7	cisco-se-6	<none>	<none>		
confd		confd-f45d9777d-jsmrv		1/1	Running	151
11d	172.17.27.10	cisco-se-1	<none>	<none>		
confd		confd-f45d9777d-lgxz2		0/1	Running	154
11d	172.17.27.210	cisco-se-2	<none>	<none>		
confd		confd-f45d9777d-wwqm2		0/1	Running	0
5d23h	172.17.27.241	cisco-se-3	<none>	<none>		
elasticsearch-nir		es-data-0		1/1	Running	22
11d	172.17.27.9	cisco-se-1	<none>	<none>		
elasticsearch-nir		es-data-1		1/1	Running	1
11d	172.17.27.79	cisco-se-2	<none>	<none>		
elasticsearch-nir		es-data-2		1/1	Running	0
5d22h	172.17.27.92	cisco-se-3	<none>	<none>		
elasticsearch-nir		es-puredata-7bd8644fb-6jng4		1/1	Running	0
5d23h	172.17.27.216	cisco-se-4	<none>	<none>		
elasticsearch-nir		es-puredata-7bd8644fb-jqng		1/1	Running	0
23h	172.17.27.40	cisco-se-5	<none>	<none>		
elasticsearch-nir		es-puredata-7bd8644fb-p85qc		1/1	Running	0
20d	172.17.27.248	cisco-se-6	<none>	<none>		
elasticsearch		es-data-0		1/1	Running	23
11d	172.17.27.234	cisco-se-2	<none>	<none>		
elasticsearch		es-data-1		1/1	Running	0
5d22h	172.17.27.145	cisco-se-3	<none>	<none>		
elasticsearch		es-data-2		1/1	Running	0
11d	172.17.27.74	cisco-se-1	<none>	<none>		
elasticsearch		es-puredata-7c45d87f68-cl44s		1/1	Running	0
20d	172.17.27.250	cisco-se-6	<none>	<none>		
elasticsearch		es-puredata-7c45d87f68-lfkr5		1/1	Running	0
5d22h	172.17.27.167	cisco-se-4	<none>	<none>		
elasticsearch		es-puredata-7c45d87f68-z97xt		1/1	Running	0
23h	172.17.27.118	cisco-se-5	<none>	<none>		
eventmgr		eventmgr-86fff4559-5j4ss		1/1	Running	0
9d	172.17.27.64	cisco-se-1	<none>	<none>		
firmware		firmware-0		1/1	Running	0
5d22h	172.17.27.113	cisco-se-3	<none>	<none>		
firmware		firmware-1		1/1	Running	2
11d	172.17.27.44	cisco-se-1	<none>	<none>		
firmware		firmware-2		1/1	Running	8
11d	172.17.27.192	cisco-se-2	<none>	<none>		
firmware		firmware-agent-77f9497ccc-vqrck		1/1	Running	0
9d	172.17.27.128	cisco-se-1	<none>	<none>		
hms		hms-8696f5ffc5-44dhs		1/1	Running	1
8d	172.17.27.233	cisco-se-2	<none>	<none>		
hms		hms-8696f5ffc5-9t8vj		1/1	Running	0
5d23h	172.17.27.107	cisco-se-1	<none>	<none>		
hms		hms-8696f5ffc5-t877l		1/1	Running	0
11d	172.17.27.62	cisco-se-6	<none>	<none>		
installer		installer-d8c49ccd9-jfndp		1/1	Running	1
9d	172.17.27.80	cisco-se-2	<none>	<none>		
kafka		kafka-0		2/2	Running	1
5d16h	172.17.27.177	cisco-se-4	<none>	<none>		

kafka		kafka-1		2/2	Running	0
7h57m	172.17.27.143	cisco-se-5	<none>	<none>		
kafka		kafka-2		2/2	Running	1
5d16h	172.17.27.83	cisco-se-3	<none>	<none>		
kafka		kafka-3		2/2	Running	0
5d16h	172.17.27.235	cisco-se-6	<none>	<none>		
kafka		kafka-4		2/2	Running	1
5d16h	172.17.27.54	cisco-se-2	<none>	<none>		
kafka		kafka-5		2/2	Running	3
5d16h	172.17.27.28	cisco-se-1	<none>	<none>		
kube-system		coredns-cisco-se-1		1/1	Running	3
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		coredns-cisco-se-2		1/1	Running	6
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		coredns-cisco-se-3		1/1	Running	6
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		docker-registry-cisco-se-1		1/1	Running	3
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		docker-registry-cisco-se-2		1/1	Running	5
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		docker-registry-cisco-se-3		1/1	Running	6
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		etcd-server-cisco-se-1		1/1	Running	9
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		etcd-server-cisco-se-2		1/1	Running	0
5d16h	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		etcd-server-cisco-se-3		1/1	Running	12
9d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		flex-provisioner-cisco-se-1		1/1	Running	7
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		flex-provisioner-cisco-se-2		1/1	Running	23
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		flex-provisioner-cisco-se-3		1/1	Running	13
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		ip-masq-agent-cisco-se-1		1/1	Running	2
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		ip-masq-agent-cisco-se-2		1/1	Running	3
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		ip-masq-agent-cisco-se-3		1/1	Running	3
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		ip-masq-agent-cisco-se-4		1/1	Running	0
20d	111.2.1.169	cisco-se-4	<none>	<none>		
kube-system		ip-masq-agent-cisco-se-5		1/1	Running	3
7d23h	111.2.1.171	cisco-se-5	<none>	<none>		
kube-system		ip-masq-agent-cisco-se-6		1/1	Running	1
20d	111.2.1.173	cisco-se-6	<none>	<none>		
kube-system		kube-apiserver-cisco-se-1		1/1	Running	24
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		kube-apiserver-cisco-se-2		1/1	Running	24
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		kube-apiserver-cisco-se-3		1/1	Running	23

22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		kube-controller-manager-cisco-se-1	1/1	Running	8	
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		kube-controller-manager-cisco-se-2	1/1	Running	39	
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		kube-controller-manager-cisco-se-3	1/1	Running	11	
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		kube-proxy-cisco-se-1	1/1	Running	4	
22d	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		kube-proxy-cisco-se-2	1/1	Running	6	
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		kube-proxy-cisco-se-3	1/1	Running	7	
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		kube-proxy-cisco-se-4	1/1	Running	1	
20d	111.2.1.169	cisco-se-4	<none>	<none>		
kube-system		kube-proxy-cisco-se-5	1/1	Running	3	
7d23h	111.2.1.171	cisco-se-5	<none>	<none>		
kube-system		kube-proxy-cisco-se-6	1/1	Running	0	
20d	111.2.1.173	cisco-se-6	<none>	<none>		
kube-system		kube-scheduler-cisco-se-1	1/1	Running	5	
5d16h	111.2.1.163	cisco-se-1	<none>	<none>		
kube-system		kube-scheduler-cisco-se-2	1/1	Running	14	
22d	111.2.1.165	cisco-se-2	<none>	<none>		
kube-system		kube-scheduler-cisco-se-3	1/1	Running	18	
22d	111.2.1.167	cisco-se-3	<none>	<none>		
kube-system		mond-54ffdf9bb4-45ft7	3/3	Running	2	
11d	172.17.27.32	cisco-se-1	<none>	<none>		
kube-system		mond-54ffdf9bb4-4z42s	3/3	Running	0	
5d23h	172.17.27.205	cisco-se-3	<none>	<none>		
kube-system		mond-54ffdf9bb4-sfgtk	3/3	Running	20	
11d	172.17.27.204	cisco-se-2	<none>	<none>		
kubese		kubese-admission-7d4778bcf4-86dj8	1/1	Running	1	
11d	172.17.27.70	cisco-se-2	<none>	<none>		
kubese		kubese-admission-7d4778bcf4-pd87x	1/1	Running	0	
5d23h	172.17.27.29	cisco-se-3	<none>	<none>		
kubese		kubese-admission-7d4778bcf4-xl7bq	1/1	Running	0	
11d	172.17.27.18	cisco-se-1	<none>	<none>		
kubese		kubese-ctrl-89df4b767-c698q	1/1	Running	0	
5d23h	172.17.27.61	cisco-se-3	<none>	<none>		
kubese		kubese-ctrl-89df4b767-pqbn7	1/1	Running	3	
11d	172.17.27.5	cisco-se-1	<none>	<none>		
kubese		kubese-ctrl-89df4b767-zj86j	1/1	Running	3	
11d	172.17.27.197	cisco-se-2	<none>	<none>		
kubese		resourcemgr-6c84cd748d-brc4p	0/1	Running	0	
2d4h	172.17.27.73	cisco-se-2	<none>	<none>		
kubese		resourcemgr-6c84cd748d-krnpd	1/1	Running	0	
2d4h	172.17.27.115	cisco-se-1	<none>	<none>		
kubese		resourcemgr-6c84cd748d-z5jp6	0/1	Running	0	
2d4h	172.17.27.246	cisco-se-3	<none>	<none>		
mongodb		mongodb-0	2/2	Running	0	
5d22h	172.17.27.11	cisco-se-3	<none>	<none>		

mongodb		mongodb-1		2/2	Running	0
6d1h	172.17.27.134	cisco-se-1	<none>	<none>		
mongodb		mongodb-2		2/2	Running	2
6d1h	172.17.27.50	cisco-se-2	<none>	<none>		
nodemgr		nodeagent-68cm5		1/1	Running	0
20d	172.17.27.249	cisco-se-6	<none>	<none>		
nodemgr		nodeagent-8mkcf		1/1	Running	1
7d23h	172.17.27.213	cisco-se-5	<none>	<none>		
nodemgr		nodeagent-kfdjp		1/1	Running	0
20d	172.17.27.227	cisco-se-4	<none>	<none>		
nodemgr		nodeagent-sntd4		1/1	Running	2
22d	172.17.27.151	cisco-se-1	<none>	<none>		
nodemgr		nodeagent-t2nwc		1/1	Running	3
22d	172.17.27.202	cisco-se-2	<none>	<none>		
nodemgr		nodeagent-xcqq7		1/1	Running	3
22d	172.17.27.141	cisco-se-3	<none>	<none>		
nodemgr		nodectrlr-5f5544f8c6-7m9jm		1/1	Running	180
11d	172.17.27.33	cisco-se-1	<none>	<none>		
nodemgr		nodectrlr-5f5544f8c6-frpqz		0/1	Running	190
11d	172.17.27.125	cisco-se-2	<none>	<none>		
nodemgr		nodectrlr-5f5544f8c6-x8jj5		0/1	Running	0
5d23h	172.17.27.223	cisco-se-3	<none>	<none>		
sm		sm-7999cc4b79-p96p4		1/1	Running	314
9d	172.17.27.132	cisco-se-2	<none>	<none>		
ts		tsagent-4b72k		1/1	Running	3
22d	172.17.27.138	cisco-se-3	<none>	<none>		
ts		tsagent-6tqfz		1/1	Running	1
7d23h	172.17.27.120	cisco-se-5	<none>	<none>		
ts		tsagent-8wwnz		1/1	Running	0
20d	172.17.27.225	cisco-se-4	<none>	<none>		
ts		tsagent-jc4ml		1/1	Running	2
22d	172.17.27.137	cisco-se-1	<none>	<none>		
ts		tsagent-kmxtq		1/1	Running	3
22d	172.17.27.46	cisco-se-2	<none>	<none>		
ts		tsagent-lk9zc		1/1	Running	0
20d	172.17.27.245	cisco-se-6	<none>	<none>		
ts		tsctrlr-697fb85b68-jjgfv		0/1	Running	9
11d	172.17.27.31	cisco-se-1	<none>	<none>		
ts		tsctrlr-697fb85b68-kg22t		0/1	Running	28
11d	172.17.27.237	cisco-se-2	<none>	<none>		
ts		tsctrlr-697fb85b68-sjlfk		1/1	Running	0
5d23h	172.17.27.52	cisco-se-3	<none>	<none>		
ui		ui-6cf47cfc5d-bqgj7		1/1	Running	0
5d23h	172.17.27.176	cisco-se-3	<none>	<none>		
ui		ui-6cf47cfc5d-jll9q		1/1	Running	12
6d1h	172.17.27.160	cisco-se-2	<none>	<none>		
ui		ui-6cf47cfc5d-lbbnj		1/1	Running	0
11d	172.17.27.13	cisco-se-1	<none>	<none>		
zk		zk-0		1/1	Running	0
5d16h	172.17.27.201	cisco-se-3	<none>	<none>		
zk		zk-1		1/1	Running	0

```

5d16h 172.17.27.255 cisco-se-1 <none> <none>
zk zk-2 1/1 Running 0
5d16h 172.17.27.27 cisco-se-2 <none> <none>

```

```
[rescue-user@cisco-se-1 ~]$ acidiag cluster get config
```

ATTRIBUTES	APP SE CONFIG
ActiveMasters	3
AllMastersUp	true
AppNetwork GatewayIP	<nil>
AppNetwork Iface	app-vnic
AppNetwork IfaceIP	<nil>
AppNetwork Subnet	172.17.0.1/16
ClusterVersion	1.1.3c
DNSDomain	SECluster.case.local
ExistingCluster	true
HealthyCluster	true
ID	fa0da1d8-1a9f-46bf-bced-045f1ee0abcd
InbandIface	bond0.4094
MaxMasters	3
Mode	standalone
Name	SECluster
NameServers	[173.36.131.10 171.70.168.183]
NtpServers	[171.68.38.65 171.68.38.66 72.163.32.44]
SeedList	[{WZP233907DA 111.2.1.165} {WZP23361A1R 111.2.1.167}]
ServiceNetwork GatewayIP	<nil>
ServiceNetwork Iface	



```

ServiceNetwork IfaceIP | <nil>
ServiceNetwork Subnet  | 100.80.0.0/16
TargetVersion          |
WorkerList             | [WZP2341087G WZP234316ZP WZP234316ZW]

```

```
[rescue-user@cisco-se-1 ~]$ acidiag cluster get masters
```

```

ATTRIBUTES          | cisco-SE-1          | cisco-SE-2
cisco-SE-3
CleanReboot         | false               | false
false
FirmwareVersion     | 1.1.3c              | 1.1.3c
1.1.3c
FirstMaster         | true                | false
false
ID                  | 87cb864d-4730-40e9-822d-4dfa0302b5a6 | 8300a02c-6c66-
476b-8229-907fe4c8a9d3 | eca1c47d-d034-49c1-bf49-11a5c350ef0d |
InbandNetwork GatewayIP | 111.2.1.1          | 111.2.1.1
111.2.1.1
InbandNetwork Iface | bond0.4094         | bond0.4094
bond0.4094
InbandNetwork IfaceIP | 111.2.1.163        | 111.2.1.165
111.2.1.167
InbandNetwork Subnet | 111.2.1.163/24     | 111.2.1.165/24
111.2.1.167/24
Labels
Model               | SE-NODE-G2         | SE-NODE-G2
SE-NODE-G2
Name                | cisco-se-1         | cisco-se-2
cisco-se-3
OobNetwork GatewayIP | 172.23.96.1        | 172.23.96.1
172.23.96.1
OobNetwork Iface    | bond1              | bond1
bond1
OobNetwork IfaceIP  | 172.23.96.163     | 172.23.96.165
172.23.96.167
OobNetwork Subnet   | 172.23.96.163/21  | 172.23.96.165/21
172.23.96.167/21

```

Role	Master	Master
Master		
SecondaryStatus	Alive	Alive
Alive		
Self	true	false
false		
SerialNumber	WZP233610W0	WZP233907DA
WZP23361A1R		
Status	Active	Active
Active		

```
[rescue-user@cisco-se-1 ~]$ acidiag cluster get workers
```

ATTRIBUTES	cisco-SE-4	cisco-SE-5
cisco-SE-6		

CleanReboot	false	false
true		
FirmwareVersion	1.1.3c	1.1.3c
1.1.3c		
FirstMaster	false	false
false		
ID	be40cf85-80c7-40aa-a9fd-bb5c7d628450	eedb7b9f-014b-46f6-9a36-c18ea8239185
5ce246f4-bc4f-41c3-9fb7-f619e6faf2d5		
InbandNetwork GatewayIP	111.2.1.1	111.2.1.1
111.2.1.1		
InbandNetwork Iface	bond0.4094	bond0.4094
bond0.4094		
InbandNetwork IfaceIP	111.2.1.169	111.2.1.171
111.2.1.173		
InbandNetwork Subnet	111.2.1.169/24	111.2.1.171/24
111.2.1.173/24		
Labels		
Model	SE-NODE-G2	SE-NODE-G2
SE-NODE-G2		
Name	cisco-se-4	cisco-se-5
cisco-se-6		
OobNetwork GatewayIP	172.23.96.1	172.23.96.1
172.23.96.1		
OobNetwork Iface	bond1	bond1
bond1		

OobNetwork IfaceIP	172.23.97.197	172.23.97.198
172.23.97.199		
OobNetwork Subnet	172.23.97.197/23	172.23.97.198/23
172.23.97.199/23		
Role	Worker	Worker
Worker		
SecondaryStatus	Alive	Alive
Alive		
Self	false	false
false		
SerialNumber	WZP2341087G	WZP234316ZW
WZP234316ZP		
Status	Active	Active
Active		

```
[rescue-user@cisco-se-1 ~]$ acidiag app show
```

```
[ { 'adminState': 'Disabled',
    'apiEndpoint': '/query',
    'apiURLPrefix': '/appcenter/cisco/nir/api/',
    'creationTimestamp': '2020-06-17T21:04:36.471719343Z',
    'description': 'Network Insights - Resources is a platform for '
                  'predictive analytics, correlation and alerting using '
                  'streaming telemetry data for networking fabrics.',
    'displayName': 'Network Insights - Resources',
    'id': 'cisco-nir:2.2.2.81',
    'insertionURL': 'Operations',
    'name': 'cisco-nir',
    'operStage': 'PostInstall',
    'operState': 'Disabled',
    'schemaversion': '',
    'uiEndpoint': 'app-start.html',
    'uiURLPrefix': '/appcenter/cisco/nir/ui/',
    'vendorID': 'Cisco',
    'version': '2.2.2.81'},
  { 'adminState': 'Disabled',
    'apiEndpoint': '/query',
    'apiURLPrefix': '/appcenter/cisco/nir/api/',
    'creationTimestamp': '2020-06-19T00:38:24.802649813Z',
    'description': 'Network Insights - Resources is a platform for '
                  'predictive analytics, correlation and alerting using '
                  'streaming telemetry data for networking fabrics.',
    'displayName': 'Network Insights - Resources',
    'id': 'cisco-nir:2.2.2.84',
    'insertionURL': 'Operations',
    'name': 'cisco-nir',
    'operStage': 'PostInstall',
    'operState': 'Disabled',
```

```

'schemaversion': '',
'uiEntrypoint': 'app-start.html',
'uiURLPrefix': '/appcenter/cisco/nir/ui/',
'vendorID': 'Cisco',
'version': '2.2.2.84'},
{
'adminState': 'Disabled',
'apiEntrypoint': '/query',
'apiURLPrefix': '/appcenter/cisco/nir/api/',
'creationTimestamp': '2020-06-21T15:31:40.090506474Z',
'description': 'Network Insights - Resources is a platform for '
                'predictive analytics, correlation and alerting using '
                'streaming telemetry data for networking fabrics.',
'displayName': 'Network Insights - Resources',
'id': 'cisco-nir:2.2.2.87',
'insertionURL': 'Operations',
'name': 'cisco-nir',
'operStage': 'PostInstall',
'operState': 'Disabled',
'schemaversion': '',
'uiEntrypoint': 'app-start.html',
'uiURLPrefix': '/appcenter/cisco/nir/ui/',
'vendorID': 'Cisco',
'version': '2.2.2.87'},
{
'adminState': 'Enabled',
'apiEntrypoint': '/query',
'apiURLPrefix': '/appcenter/cisco/nir/api/',
'creationTimestamp': '2020-06-23T15:43:10.300979601Z',
'description': 'Network Insights - Resources is a platform for '
                'predictive analytics, correlation and alerting using '
                'streaming telemetry data for networking fabrics.',
'displayName': 'Network Insights - Resources',
'id': 'cisco-nir:2.2.2.89',
'insertionURL': 'Operations',
'name': 'cisco-nir',
'operStage': 'Enable',
'operState': 'Running',
'schemaversion': '',
'uiEntrypoint': 'app-start.html',
'uiURLPrefix': '/appcenter/cisco/nir/ui/',
'vendorID': 'Cisco',
'version': '2.2.2.89'}}]

```