



# Using Cisco Network Insights for Resources

This chapter contains the following sections:

- [Cisco NIR Components, on page 1](#)
- [Cisco NIR Setup and Settings, on page 2](#)
- [Guidelines and Limitations, on page 3](#)
- [Navigating Cisco NIR, on page 3](#)
- [Using the Cisco Network Insights for Resources Application, on page 6](#)

## Cisco NIR Components



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

The Cisco NIR application consists of the following components:

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

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

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

- **Flow Analytics**—This includes the anomalies in the behavior of fabric switches such as average latency, packet drop indicator, and flow move indicator across the entire ACI.
- **Resource and Environmental Utilization**—Resource analytics supports configuration, operational and hardware resources. Environmental covers CPU, memory, temperature, fan utilization, power, and storage related to the leaf switches, spine switches, and Cisco APIC. System analytics also covers anomalies, the trending information of each resource, and graphing of parameters, which help network operators debug devices over periods of time.
- **Predictive Analytics and Correlation**—The value-add of this platform is predicting failures in the fabric and correlating internal fabric failures to the user-visible/interested failures.
- **Anomaly Detection**—Involves understanding the behavior of each component well using different machine learning algorithms and raising anomalies when the resource behavior deviates from the expected pattern. Anomaly detector applications use different supervised and unsupervised learning algorithms to detect the anomalies in the resources and they log the anomalies in a anomaly database.

## Cisco NIR Setup and Settings

### Initial Setup

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

### Welcome to Network Insights

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

1. On the welcome dialog, click **Begin Set Up**.

The Set Up window appears.

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


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

3. Click **Done**.

### Settings

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

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

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

## Guidelines and Limitations

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

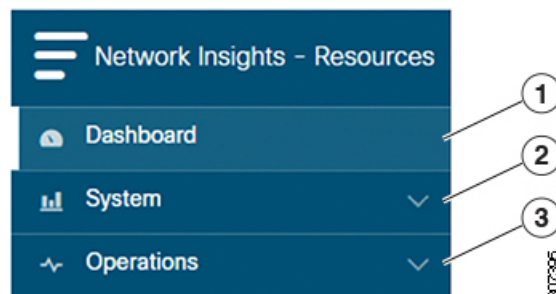
- When fabric is upgraded and nodes are reloaded, disable and enable the Cisco NIR app for the application to load the latest data.

## Navigating Cisco NIR

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

### Navigation Pane

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

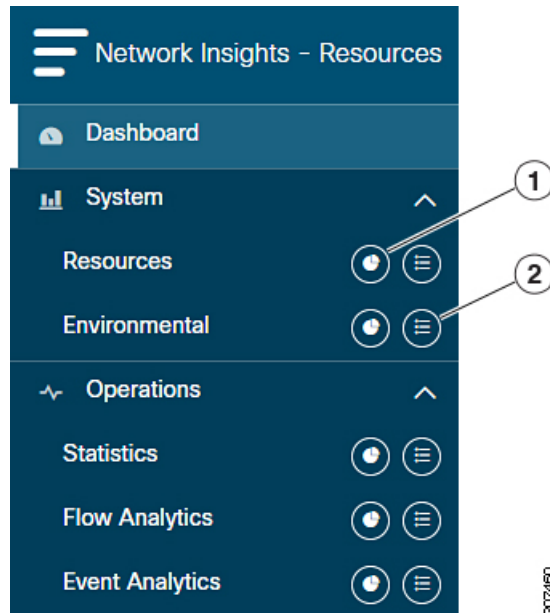


**1** Dashboard: The main dashboard for the Cisco NIR application providing immediate access to anomalies.

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

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

Expanding System and/or Operations reveals additional functions:



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

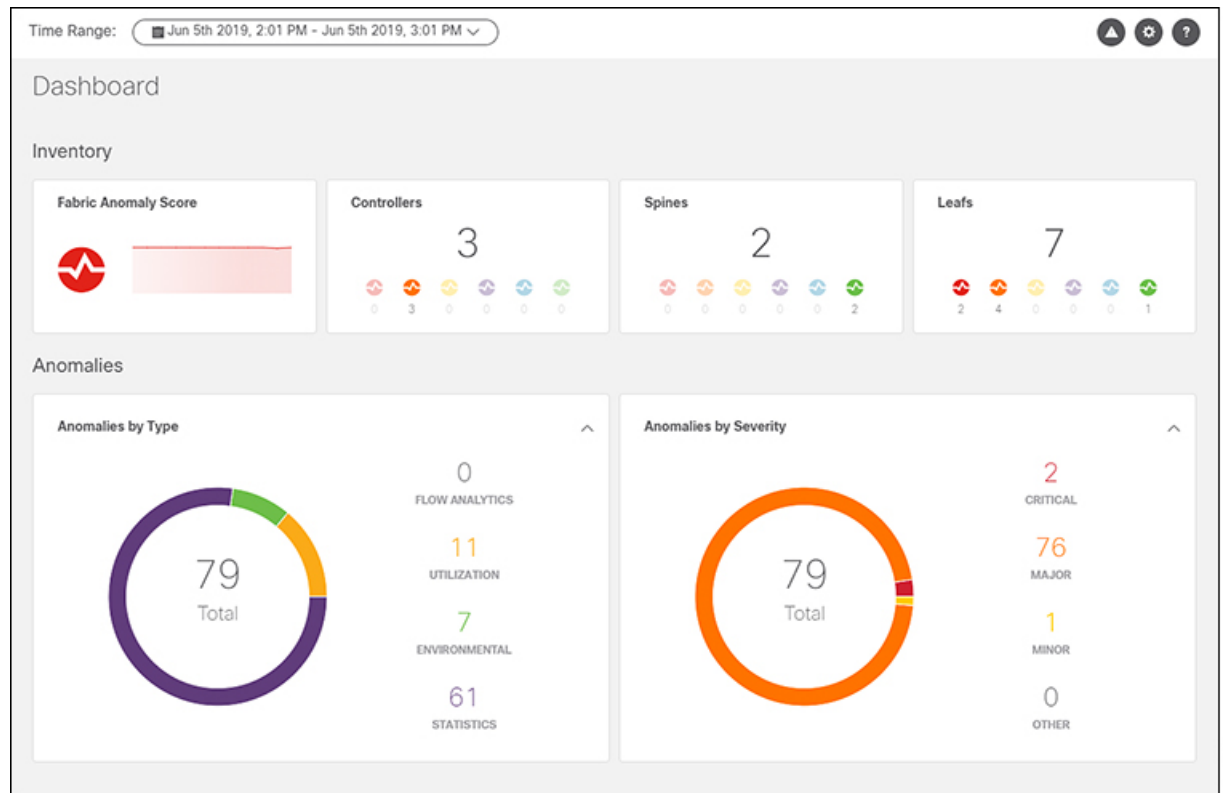
**2 Browse View icon:** Provides a detailed view of returned data for the selected telemetry type and allows for filtering to further isolate problem areas.

### Work Pane

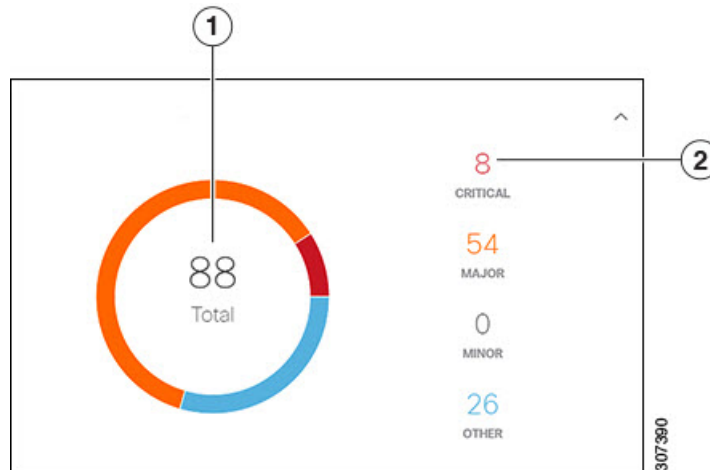
The work pane is the main viewing location in the Cisco NIR application. All information tiles, graphs, charts, and lists appear in the work pane.

#### Dashboard Work Pane

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



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






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

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

### Browse Work Pane

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

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

307381

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

### Details Work Pane

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

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

## Using the Cisco Network Insights for Resources Application

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

### Cisco NIR Dashboard

The Cisco Network Insights for Resources (Cisco NIR) application dashboard provides immediate access to anomalies occurring in the network. Anomalies are learned deviations from the last known "good" state of a switch and are displayed by type and severity. Anomalies include resource utilization, environmental, flow anomalies, and interface and protocol-level errors, and are color coded based on severity: Critical: Red, Major: Orange, Minor: Yellow, Warning: Purple, Information: Blue, and Healthy: Green.

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

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

#### Inventory

Property	Description
<b>Fabric Anomaly Score</b>	Displays the health of the fabric through the anomaly score.
<b>Controllers</b>	Displays the total number of Cisco APICs in the fabric.
<b>Spines</b>	Displays the total number of spine switches in the fabric.

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

### Anomalies

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

Property	Description
<b>Anomalies by Type</b>	Displays the number of Anomalies by their type. Anomaly types include: <ul style="list-style-type: none"> <li>• Utilization</li> <li>• Environmental</li> <li>• Statistics</li> <li>• Flow Analytics</li> </ul>
<b>Anomalies by Severity</b>	Displays the number of Anomalies (internal Fabric 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>

### Browse Anomalies

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

### Filters

You can refine the displayed anomalies by the following filters:

- Start Time - display only anomalies with a specific start time.
- End Time - display only anomalies with a specific end time.
- Description - display only anomalies with a specified description.
- Nodes - display only anomalies for specific nodes.
- Category - display only anomalies from a specific category.
- Resource Type - display only anomalies of a specific resource type.
- Severity - display only anomalies of a specific severity.

For the filter refinement, use the following operators:

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

- **contains** - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- **!contains** - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.
- **<** - with the initial filter type, this operator, and a subsequent value, returns a match less than the value.
- **<=** - with the initial filter type, this operator, and a subsequent value, returns a match less than or equal to the value.
- **>** - with the initial filter type, this operator, and a subsequent value, returns a match greater than the value.
- **>=** - with the initial filter type, this operator, and a subsequent value, returns a match greater than or equal to the value.

### Anomaly Chart

Property	Description
<b>Anomalies By Type</b>	Displays the number of Anomalies by their type. Anomaly types include: <ul style="list-style-type: none"> <li>• Utilization</li> <li>• Environmental</li> <li>• Statistics</li> <li>• Flow Analytics</li> </ul>
<b>Anomalies By Severity</b>	Displays the number of Anomalies (internal Fabric 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>

## Cisco NIR System

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

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

## Resources

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

### Resources Dashboard



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

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

### Browse Resources

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

### Filters

You can refine the displayed statistics by the following filters:

- Node - display only nodes.

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

- = - with the initial filter type, this operator, and a subsequent value, returns an exact match.
- != - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Property	Description
<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>• VLAN</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> </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>	Displays a list of configuration resources based on resource utilization. List information includes: <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>	Displays a list of configuration resources based on resource utilization. List information includes: <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>

## 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>• Memory</li> <li>• Temperature</li> <li>• Storage</li> <li>• Fan Utilization</li> <li>• Power Supply</li> <li>• CPU</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>Environmental Resources (table)</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 NIR Operations

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

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

## Statistics

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

### Statistics Dashboard

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

Property	Description
<b>Top Nodes by Interface Utilization</b>	Displays the top nodes based on the combined bandwidth utilization of it's interfaces.
<b>Top Nodes by Interface</b>	Displays the top nodes and lists the transmit and receive bandwidth utilization of each of it's interfaces.

### Browse Statistics

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

### Filters

You can refine the displayed statistics by the following filters:

- Node - display only nodes.
- Interface - display only interfaces.
- Protocol - display only protocols.
- Operational State -
- Admin State -

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

- = - with the initial filter type, this operator, and a subsequent value, returns an exact match.
- != - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- contains - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- !contains - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

Property	Description
<b>Top 10 Interfaces by</b>	Displays the top interfaces by: <ul style="list-style-type: none"> <li>• Transmit Utilization</li> <li>• Receive Utilization</li> <li>• Error</li> </ul>
<b>Interface Statistics</b>	Displays a list of interface statistics sorted by anomaly score. List information includes: <ul style="list-style-type: none"> <li>• Anomaly Score</li> <li>• Interface</li> <li>• Node</li> <li>• Receive Utilization</li> <li>• Transmit Utilization</li> <li>• Errors</li> </ul>
<b>Protocol Statistics</b>	Displays a list of protocol statistics sorted by anomaly score. List information includes: <ul style="list-style-type: none"> <li>• Anomaly Score</li> <li>• Protocol</li> <li>• Node</li> <li>• Number of Interfaces</li> <li>• Errors</li> </ul>

## Flow Analytics

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

### Flow Analytics Overview

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

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

## Flow Analytics Pre-requirements

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

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


## Flow Analytics Dashboard

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

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

## Browse Flows

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

Property	Description
	<p>Clicking on this icon allows you to alter the following:</p> <ul style="list-style-type: none"> <li>• <b>Application Settings</b>—Enable or disable flow collection and assign a previously configured inband management EPG.</li> </ul> <p><b>Note</b> By default, flow collection is disabled. After the NIR application is downloaded, you must enable flow collection for this feature to function.</p> <ul style="list-style-type: none"> <li>• <b>Flow Collection Filters</b>—Create VRF and EPG collection rules per tenant: <ul style="list-style-type: none"> <li>• Click the <b>Plus</b> icon and enter the filter Name.</li> <li>• Select a <b>Tenant</b>, and <b>VRF</b> from the drop-downs.</li> <li>• Enter the subnet in the <b>Subnet</b> field and click <b>Add Subnet</b>.</li> <li>• Click <b>Save</b>.</li> </ul> </li> </ul> <p><b>Note</b> To verify that <b>Flow Collection</b> has started, select <b>Collection Status</b>. On the <b>Collection Status</b> table, you should see the green circles indicating the nodes where the flows are being exported.</p> <ul style="list-style-type: none"> <li>• <b>System Status</b>—Displays service status of the flows, such as API Server, APIC Config Manager, Correlation Engine, Flow Manager, and Prediction Engine and Capacity Usage per node and Network Insights usage.</li> </ul>



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

## Flow Collection Filters

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

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



Property	Description
<b>Filters</b>	<p>You can display the node flow observations sorted by the following filters:</p> <ul style="list-style-type: none"> <li>• Timestamp</li> <li>• Ingress Nodes</li> <li>• Egress Nodes</li> <li>• Source EPG</li> <li>• Source Address</li> <li>• Source Port</li> <li>• Destination EPG</li> <li>• Destination Address</li> <li>• Destination Port</li> <li>• Address Type</li> <li>• Protocol</li> </ul>
<b>Top 10 flows by</b>	<p>Lists the top 10 flows that scored highest in the following:</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 fabric. <ul style="list-style-type: none"> <li><b>Note</b> A prerequisite for fabric latency measurement is that all the nodes shall be synchronized with uniform time.</li> </ul> </li> <li>• <b>Flow Move Indicator</b>—The number of times a Flow moves from one Cisco ACI leaf switch to another. The first ARP/RARP or regular packet sent by that endpoint appears as a flow entering the fabric through the new Cisco ACI leaf switch.</li> </ul>

## Event Analytics

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

### Event Analytics Dashboard

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

Property	Description
<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.
<b>Faults by Severity</b>	Displays all faults by severity.  A fault is represented as mutable, stateful, and persistent Managed Object (MO). When a failure occurs or an alarm is raised, the system creates a fault MO as a child object to the MO that is primarily associated with the fault. For a fault object class, the fault conditions are defined by the fault rules of the parent object class. Each fault includes information about the operational state of the affected object at the time the fault was raised. If the fault is transitional and the failure is resolved, then the object transitions to a functional state.

### Browse Audit Logs, Events & Faults

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

#### Filters

You can refine the displayed statistics by the following filters:

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

As a filter refinement, use the following operators:

- **=** - with the initial filter type, this operator, and a subsequent value, returns an exact match.
- **!=** - with the initial filter type, this operator, and a subsequent value, returns all that do not have the same value.
- **<** - with the initial filter type, this operator, and a subsequent value, returns a match less than the value.
- **<=** - with the initial filter type, this operator, and a subsequent value, returns a match less than or equal to the value.
- **>** - with the initial filter type, this operator, and a subsequent value, returns a match greater than the value.
- **>=** - with the initial filter type, this operator, and a subsequent value, returns a match greater than or equal to the value.
- **Audit Log (Type)** - display only audit logs.
- **Event (Type)** - display only events.
- **Fault (Type)** - display only faults.
- **Cleared (Severity)** - display only cleared events and faults.
- **Info (Severity)** - display only informational events and faults.
- **Warning (Severity)** - display only warning events and faults.
- **Minor (Severity)** - display only minor events and faults.
- **Major (Severity)** - display only major events and faults.
- **Critical (Severity)** - display only critical events and faults.
- **Creation (Action)** - display only created audit logs.
- **Deletion (Action)** - display only deleted audit logs.
- **Modification (Action)** - display only modified audit logs.

<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>

Property	Description
Faults by Severity	Displays all faults based on severity: <ul style="list-style-type: none"><li data-bbox="727 331 824 359">• Critical</li><li data-bbox="727 386 813 413">• Major</li><li data-bbox="727 441 813 468">• Minor</li><li data-bbox="727 495 808 522">• Other</li></ul>