



# Using Cisco Network Insights for Resources

This chapter contains the following sections:

- [Using the Cisco Network Insights for Resources Application, on page 1](#)

## Using the Cisco Network Insights for Resources Application

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

### Cisco NIR Dashboard

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

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

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

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

## Dashboard Inventory

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


Property	Description
<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 nodes in the fabric with anomalies.
<b>Leafs</b>	Displays the total number of leaf nodes in the fabric with anomalies.


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

### Browse Nodes

The Browse Nodes pane displays the graph with top nodes based on Resource Utilization, Environmental, Statistics, End Point Analytics, and Flow Anomaly, which are various ways of viewing the behavior of the nodes. The page also displays the overview of the individual nodes in the fabric with node name, switch models, node type and other details. Click **Node** for the node detail view. The **Node Overview** section displays the top five nodes based on Resource Utilization, Environmental, Flow analytics, and Endpoint Analytics with the break down of the faults and events. The **Anomalies** section displays the anomalies that the system detects.

The Browse Nodes pane displays the graph with top nodes based on Resource Utilization, Environmental, Statistics, and Flow Analytics, which are various ways of viewing the behavior of the nodes. The page also displays the overview of the individual nodes in the fabric with node name, switch models, node type and other details. Click the **Node** for the node summary pane to display all the gathered information for the selected node.

Click the  icon on the right top corner of the summary pane to show the Node Details page. The Node Details page displays General Information, Node Overview, and Anomalies. The **Node Overview** section displays the top five nodes based on Resource Utilization, Environmental, and Flow analytics with the break down of the faults and events. The **Anomalies** section displays the anomalies that the system detects.

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

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

## Dashboard Anomalies

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

Property	Description
<b>Anomalies by Type</b>	Displays the number of Anomalies by their type. Anomaly types 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 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>

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

## Browse Anomalies

The Browse Anomalies pane displays the graph with top nodes by anomaly score based on Type and Severity. The page also displays the overview of the individual nodes in the fabric with severity, resource type, node name, description, cleared, acknowledged and other details. Double-click the anomaly for the anomaly details. The **Anomaly Details** page displays the description of the anomaly, recommendations to resolve the 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.

## Browse Anomaly Filters

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

You can refine the displayed anomalies by the following filters:

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

- Nodes - Display only anomalies for specific nodes.
- Category - Display only anomalies from a specific category.
- Resource Type - Display only anomalies of a specific resource type.
- Severity - Display only anomalies of a specific severity.
- Acknowledged - Do not display the selected anomaly when checked to **T** for 20 minutes.

For the filter refinement, use the following operators:

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

## Top Nodes by Anomalies

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

## Browse Dashboard

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

## Cisco NIR System

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

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

## System Resources

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

### Resources Dashboard

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

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

### Browse Resources

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

### Filters

You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

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

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

Property	Description
<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>

## 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>• 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.
- **Endpoint Analytics**—Displays endpoint anomalies for the nodes collected across the entire fabric.
- **Event Analytics**—Displays charts for event occurrences over time.

## Statistics Analytics

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

### Statistics Dashboard

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

Property	Description
<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.

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 that are sorted by anomaly score. List information includes: <ul style="list-style-type: none"> <li>• Anomaly Score</li> <li>• Interface</li> <li>• Type</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 that are sorted by anomaly score. List information includes: <ul style="list-style-type: none"> <li>• Anomaly Score</li> <li>• Protocol</li> <li>• Type</li> <li>• Node</li> <li>• Number of Interfaces</li> <li>• Errors</li> </ul>

## Browse Statistics

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

### Interface Statistics

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

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

The interface type is physical, port channel, or virtual port channel (PC or vPC) interface. Double-click **type** > **physical** for interface details of the node such as, node name, physical interface name, operational status, and admin state. The page also displays protocols, QoS, and DOM properties of the physical interface.

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

Click **type > pc** for interface details of the node such as, node name, port channel name, operational status, and admin state. The page also displays the anomalies, traffic, and member interfaces associated in the port channel.

The vPC is a logical interface that spans across two physical switches for fault tolerance. Double-click **type > vpc** for interface details of the node such as, node name, virtual port channel name, domain id, operational status, and admin state. The page also displays the anomalies, traffic, and the member interfaces associated in the nodes that are in the virtual port channel.

### Protocol Statistics

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

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

Double-click **protocol > BGP** for protocol details of the node such as, node name, protocol name, admin state, operational state and additional details. This page also displays the anomalies, neighbor nodes that are active, errors in the node, neighbor IP address, details about the established neighbors and not connected neighbors that the BGP protocol is using from the node family. Double-click a **Neighbor** node for the **Neighbor Details** window to popup with more details.

Double-click **protocol > CDP**, **protocol > LLDP**, or **protocol > LACP** for protocol details of the node such as, node name, protocol name, anomalies, interfaces that are active, errors in the node, and more details of the interface.

### Browse Statistics Limitations

The following are Cisco NIR application limitations for Interface Statistics.

- Interface Statistics does not support *eqptIngrCrcErrPkts5min* counter.

## Flow Analytics

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

### Flow Analytics Overview

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

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

### Flow Analytics Pre-requirements

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

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

### Flow Analytics Limitations

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

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

### Flow Analytics Dashboard

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

Property	Description
<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.

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

## Browse Flows

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

Property	Description
<b>Nodes</b>	Active nodes are leaf nodes 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.
<b>Filters</b>	Display the node flow observations sorted by the following filters: <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>

Property	Description
Top 10 flows by	<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.</li> </ul> <p><b>Note</b> A prerequisite for fabric latency measurement is that all the nodes shall be synchronized with uniform time.</p> <ul style="list-style-type: none"> <li>• <b>Flow Move Indicator</b>—The number of times a Flow moves from one Cisco ACI leaf node to another. The first ARP/RARP or regular packet sent by that endpoint appears as a flow entering the fabric through the new Cisco ACI leaf node.</li> </ul>

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

## Endpoint Analytics

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

### Endpoint Analytics Overview

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

- The endpoints present on the leaf switches - browse endpoint analytics using filter options, such as IP address, MAC address, node, entity name and so on.
- The endpoints in the fabric at a particular time - view the endpoint history.
- The endpoint information for compute administrator - view the endpoint placement information and correlation to virtual machine and hypervisor.
- The policies applied on an endpoint - view the discover configuration and operational information of the endpoint.

The following anomalies are detected as part of endpoint analytics:

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

## Endpoint Analytics Dashboard

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

Property	Description
<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 health of each node with endpoint anomalies.

## Browse Endpoint Analytics

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

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

- Tenant - Displays nodes with tenant name.
- VRF - Displays nodes with IP address.
- BD - Displays nodes with domain id.
- EPG/l3 out - Displays nodes with entity type - L3out or EPG (L2 endpoint).
- MAC Address - Display nodes with MAC address.
- Nodes - Display only nodes.
- Interface - Display only interfaces.
- IP address - Display nodes with IP address.
- Status - Display nodes with the status.
- Time - Display endpoints that had the last update happened at this time.

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

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

Browse Endpoints	Description
<b>Top 10 Endpoints by Anomaly Score</b>	Displays the top endpoints based on the time series information collected for number of endpoints. Displays the following: <ul style="list-style-type: none"> <li>• Endpoint</li> <li>• Anomaly Score</li> </ul>
<b>Table of Endpoints</b>	Displays a list of endpoints that are sorted by anomaly score. List information includes: <ul style="list-style-type: none"> <li>• Anomaly Score</li> <li>• Tenant</li> <li>• VRF</li> <li>• BD</li> <li>• EPG/I3 out</li> <li>• MAC Address</li> <li>• IP Address</li> <li>• Nodes</li> <li>• Interface</li> <li>• Status</li> <li>• Time</li> </ul>

### Endpoint Details

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

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

## Event Analytics

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

### Event Analytics Dashboard

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



Property	Description
<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="771 331 868 363">• Critical</li><li data-bbox="771 384 852 415">• Major</li><li data-bbox="771 436 852 468">• Minor</li><li data-bbox="771 489 852 520">• Other</li></ul>

