Cisco Nexus Dashboard Insights User Guide, Release 6.0.2 - For Cisco Application Centric Infrastructure

Table of Contents

First Published: 2021-12-17

Last Modified: 2022-08-23

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 figuresincluded 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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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)

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 the new features up to this release.

Table 1. New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
DNS Integration	Use DNS Integration to enable the name resolution feature to telemetry data.	6.0.2	*About DNS Integration*
Flow Rate Statistics	Figure out the incoming flow rate for your specific setup by viewing the incoming pipeline rates for the fabric and at the per-switch level.	6.0.2	*System Status*
AppDynamic SaaS integration support	Ability to connect to AppDynamics controller using a proxy for SaaS or cloud deployments.	6.0.2	*About AppDynamics Integration*
Digitize advisories	Digitize release notes, field notices, and EOL/EOS advisories.	6.0.2	*Viewing Defect Analysis*
Risk and Conformance report	Configure software and hardware conformance report.	6.0.2	*Risk and Conformance Report*
Additional pre-validation criteria for Firmware Update Analysis	Additional pre-validation criteria such as endpoint network redundancy for nodes for Firmware Update Analysis.	6.0.2	*Pre-Validation Criteria for Cisco APIC*
Offline sites enhancements	Ability to display PSIRTs, Field Notices, and EOL advisories for offline sites.	6.0.2	*Offline Script*

Feature	Description	Release	Where Documented
Export Data enhancement	Export Data enhancements collect data for specific resources at a greater frequency and export it directly for consumption by the user.	6.0.2	*Export Data*
Template Based Compliance	Configure a template and specify types of queries to select objects and attributes that enforce specific conditions when enabled.	6.0.2	*Template Based Compliance*
Configure Object Selectors for Naming Compliance	Configure a Naming Compliance to match selected objects using a template.	6.0.2	*Use a Template to Configure Object Selectors for Naming Compliance*
Configure Object Selectors Based on Tags and Annotations	Configure object selectors on tags and annotations using a template.	6.0.2	*Template Based Compliance*
Beta feature - VMware vCenter Integration	Add VMware vCenter integration to to collect data and metrics of the virtual machines and hosts monitored by VMware vCenter.	6.0.2	*About VMware vCenter Server Integration*
Export Data enhancement	Export Data enhancements collect data for specific resources at a greater frequency and export it directly for consumption by the user.	6.0.2	*Export Data*
Beta feature-Cisco Nexus Dashboard Orchestrator Integration and Assurance	Add Nexus Dashboard Orchestrator integration to enable and run assurance analysis for managed sites and Site Groups.	6.0.2	*Add Nexus Dashboard Orchestrator and Configure Assurance Analysis*

This document is available from your Cisco Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit Cisco Nexus Dashboard Insights Documentation.

Cisco Nexus Dashboard Insights Setup

About Nexus Dashboard Insights

Cisco Nexus Dashboard Insights (Nexus Dashboard Insights) is a real-time monitoring and analytics service.

Cisco Nexus Dashboard Insights Components

The Cisco Nexus Dashboard Insights (Nexus Dashboard Insights) monitors a data center network and pinpoints issues that can be addressed to maintain availability and reduce surprise outages. Nexus Dashboard Insights's understanding of your network allows it to provide proactive advice with a focus on maintaining availability and alerting customers about potential issues that can impact up-time.

Nexus Dashboard Insights provides log collection functionalities which are useful when working with Cisco TAC. It provides a way for Cisco customers to collect tech support across multiple devices and upload those tech supports to Cisco Intersight Cloud. Additionally, it enables capability for Cisco TAC teams to collect technical support on demand for a particular device.

An ACI site is comprised of the entire ACI fabric. An ACI fabric is made up of the APIC host and all leaf switches and spine switches controlled by the APIC controller. All the network nodes (APIC controller, leaf switches and spine switches, including border leaf and border spine switches) are analyzed together as part of the site. A Site Group is a logical entity that can contain a single site or multiple sites.

Nexus Dashboard Insights consists of the following components:

- Explore-Allows you to discover assets and their object associations in an easy-to-consume natural language query format.
- Pre-Change Analysis-Allows you to model the intended changes and verify if the changes generate the desired results.
- Configure Site Group—Settings to configure flows and schedule jobs to collect software telemetry and flow telemetry data.
    - Bug Scan—Provides access to configure, schedule, on-demand bug scan that runs for a selected site. Bug Scan generates system anomalies and alerts that are critical for a particular node on the site.
    - Assurance Analysis-Provides assurance in real time. For assurance analysis of sites in Site Groups, the data collection, model generation, and results generation are carried out simultaneously.
    - Export Data-Enables you to export data collected by Nexus Dashboard Insights over Kafka and Email.
    - Flows—Manage flow configuration rules on the site enabled on Nexus Dashboard Insights.
    - Microburst-Nexus Dashboard Insights raises anomalies based on the number of microbursts

    - at the interface level.
    - Alert Rules-Enables you to acknowledge all new detected anomalies that match a criteria and adjust the anomaly score accordingly.
    - Compliance-Enables you to achieve continuous compliance with security policies and compliance checks.
    - Collection Status—Displays the node capabilities and collection status of the nodes for the features that are supported and not supported.
- Third Party Integrations—Provides access to onboard a AppDynamics Controller on to Nexus Dashboard Insights.
- Export Data—Streams the data collected from Nexus Dashboard Insights through a Kafka exporter to send the summary of data in an email.
- Nodes—Provides various ways of viewing the behavior of the nodes based on Resource Utilization, Environmental, Statistics, Endpoints, and Flows.
- Analyze Alerts—Access to total advisories, notices, PSIRTs, hardware, software, and hardening check advisories applicable to your network.
    - Anomalies-Anomalies consists of anomalies raised for resource utilization, environmental issues, interface and routing protocol issues, flows, endpoints, events, adding sites and uploading files for assurance analysis, compliance, change analysis, and static analysis.
    - Advisories-Advisories consists of relevant impact due to field notice, EOL/EOS of software and hardware, PSIRTs at a node level and compliance.
        - Field Notices—Notices such as end-of-life notices for switch hardware and software.
        - PSIRTs—Product Security Incident Response Team notices that display three levels of advisory severity for switch hardware and software in your network.
- Troubleshoot
    - Delta Analysis-Delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two snapshots.
    - Log Collector—Collect and upload the logs for devices in your network to Cisco Intersight Cloud. Enables Cisco TAC to trigger on-demand collection of logs for user devices on the site and pull the logs from Cisco Intersight Cloud.
- Change Management
    - Firmware Update Analysis-This feature suggests an upgrade path to a recommended software version and determines the potential impact of the upgrade. It also helps with the pre-upgrade and post-upgrade validation checks.
    - Pre-Change Analysis-Tthis feature in allows you to model the intended changes, perform a Pre-Change Analysis against an existing base snapshot in the site, and verify if the changes generate the desired results.

Add a Site on Cisco Nexus Dashboard

Use this procedure to add a site in Cisco Nexus Dashboard using the GUI. Any services installed in Cisco Nexus Dashboard can access the added sites.

See Cisco Nexus Dashboard User Guide for more information.

Before you begin

- You have installed and configured Cisco Nexus Dashboard.
- You must have administrator credentials to add a site in Cisco Nexus Dashboard.
- You have configured fabric connectivity. See Cisco Nexus Dashboard User Guide for more information.

Procedure

1. Log in to the Cisco Nexus Dashboard GUI with admin privileges.
2. Click **Sites** in the left Navigation pane.
3. In the **Sites** page, click **Add Site**.
4. In the **Add Site** page perform the following actions:
    a. In the **Site Type** field, choose **ACI**.
    b. Enter the appropriate values for Site Name and Hostname/IP address.
    c. Enter the values for User Name and Password

> Enter your APIC username and password values, with admin privileges. A site name must be unique in the Cisco Nexus Dashboard Insights service.

d. (Optional) If you leave the **Login Domain** field empty, the site's local login is used.

e. In the **In-band EPG** field, enter the In-band EPG name from the controller.

5. Click **Add** to add a site to the node. Any services installed in Cisco Nexus Dashboard can access the added sites. You can view the new site in the **Sites** page.
6. In the **Site Type** area, click **Add**.
7. Continue with the installation of the Cisco Nexus Dashboard Insights on Cisco Nexus Dashboard using the GUI.

Setting Up Cisco Nexus Dashboard Insights

Use the following task to complete the initial setup of Cisco Nexus Dashboard Insights.

> Site Groups is a logical entity that can contain a single site or multiple sites. All sites within a Site Group must be of the same type.

Prerequisites

You have installed the Cisco Nexus Dashboard Insights service.

Procedure

1. In the Cisco Nexus Dashboard Insights service page, in the **Let's Configure the Basics** page, in the **Site Groups Setup** area, click **Configure**.
2. In the **Site Groups Setup** page, click **Add New Site Group**.
3. In the **Add New Site Group** dialog box, **General** area, in the **Name** field, enter a name for the Site Group.

   > A Site Group name must be unique in the Cisco Nexus Dashboard Insights service.

4. In the **Configuration** area, click **Add Site(s)**, and in the **Entity** area, click **Add Member**.
5. Click **Select Member**.
6. Click the **Select a Site** dialog box, to view the discovered sites that are listed.
7. In the **Add New Site Group** dialog box, **Configuration** area, choose **Add Site**.
8. Choose the appropriate site, and click **Select** to add the site.
9. In the **Add New Site Group** dialog box, **Status** field, choose the appropriate status to enable or disable the site.
10. Click the **Configure** link for your site.
11. In the **Configuration** dialog box, in the **General Configuration** area, enter values for the **Username** and **Password** fields.

    > The admin account must be used to perform these actions. Enter your APIC username and password values.

12. Check the checkmark for your site when done. Click **Save**.
13. In the in the **Site Groups Setup** page, click **Done**.

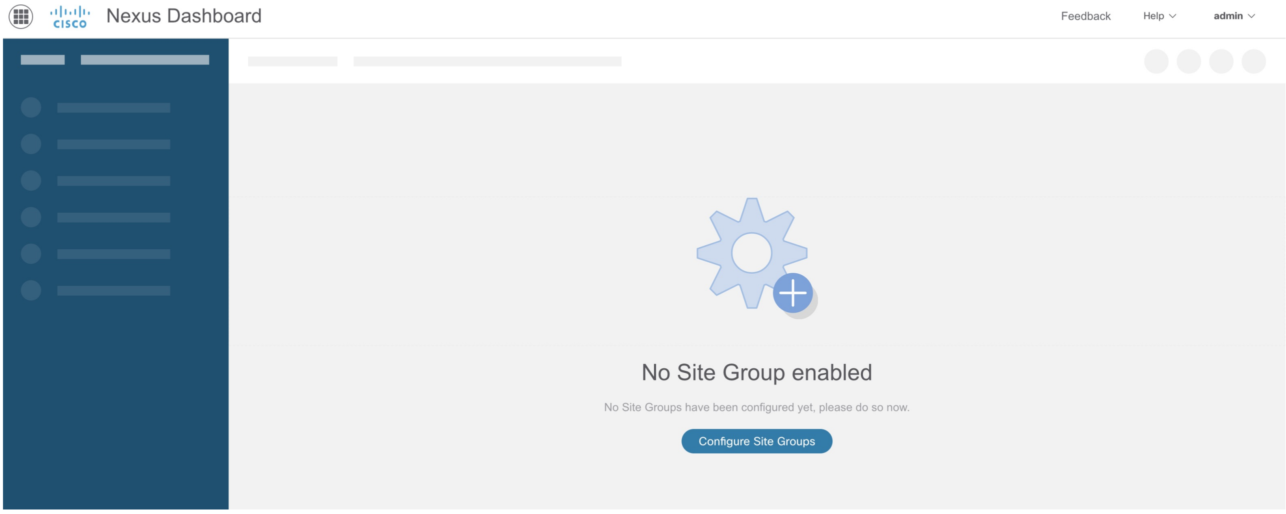
The site is enabled in the **Configure Site Group** > **General** tab. This completes the initial setup.

> A site must be enabled to perform further configurations or to enable other tasks in the service.

Cisco Nexus Dashboard Insights Configuring the Basics for Day 0 Setup

If you are performing the setup in Cisco Nexus Dashboard Insights for the very first time, then follow the steps in this section after your initial setup for Cisco Nexus Dashboard Insights is complete.

1. When you launch Nexus Dashboard Insights, in the **No Site Groups enabled** area, click **Configure Site Groups**.



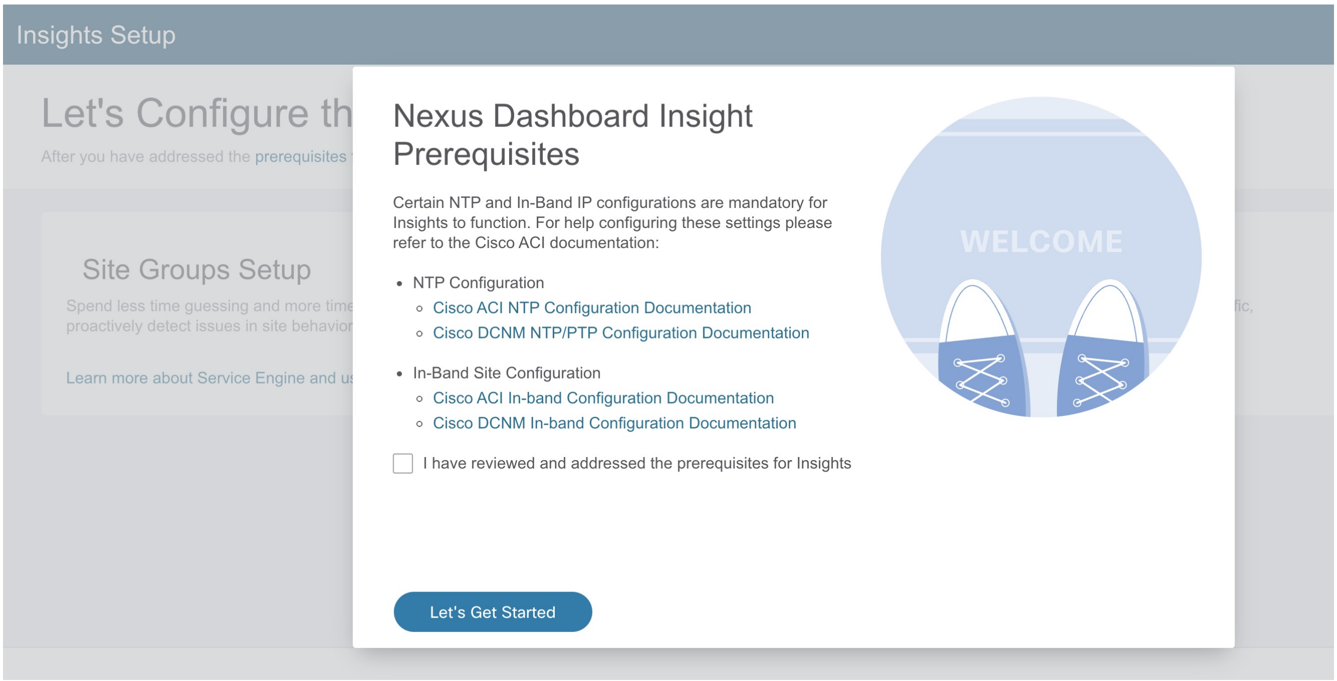
No Site Group enabled

No Site Groups have been configured yet, please do so now.

2. In the **Nexus Dashboard Insights Prerequisites** dialog box, verify that you have configured the required mandatory settings. If you need help configuring these settings, refer to the documentation links:

   a. NTP Configuration for Cisco ACI Cisco ACI NTP Configuration Documentation

   b. In-Band Site Configuration for Cisco ACI Cisco ACI In-band Configuration Documentation


Insights Setup
Let's Configure th
After you have addressed the prerequisites
Site Groups Setup
Spend less time guessing and more time
proactively detect issues in site behavior
Learn more about Service Engine and us
fic,
WELCOME

Nexus Dashboard Insight Prerequisites

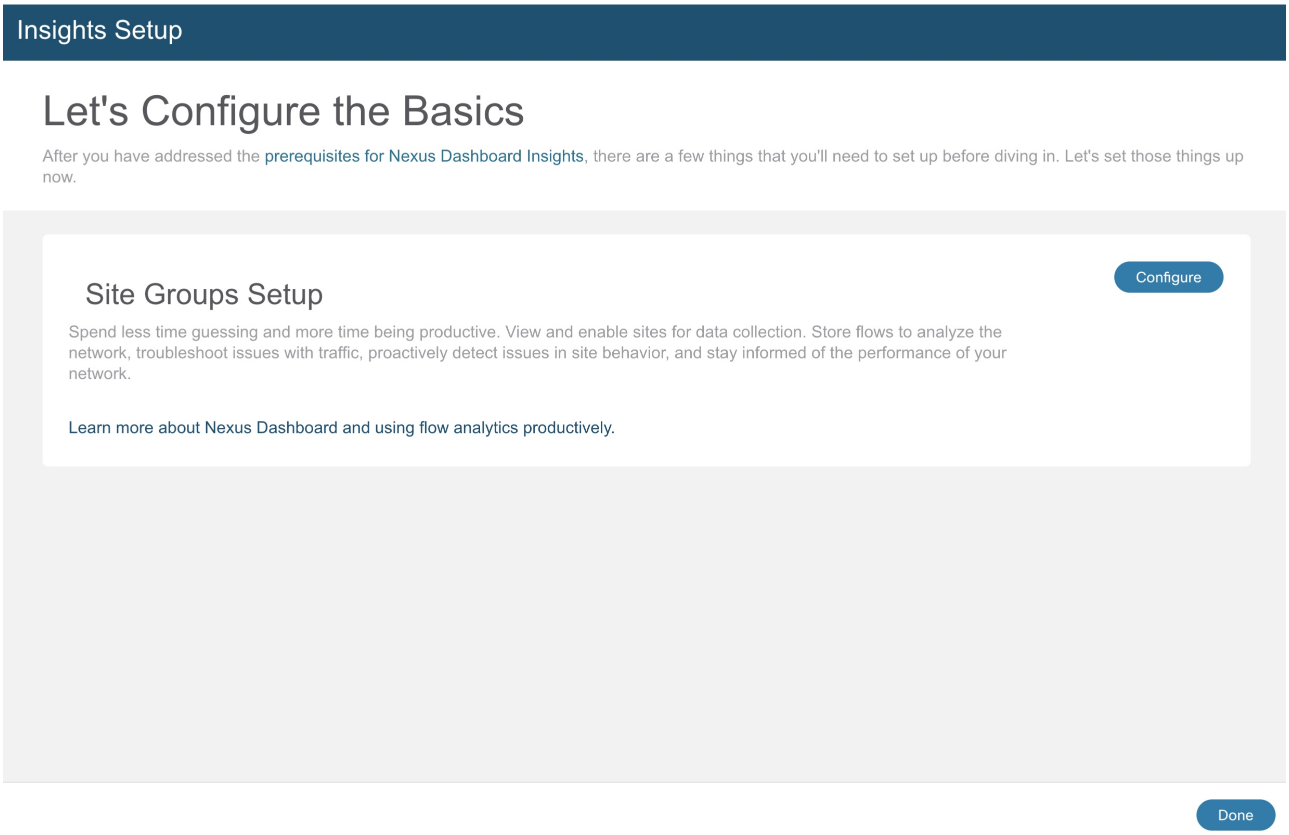
Certain NTP and In-Band IP configurations are mandatory for Insights to function. For help configuring these settings please refer to the Cisco ACI documentation:

- NTP Configuration
  - Cisco ACI NTP Configuration Documentation
  - Cisco DCNM NTP/PTP Configuration Documentation
- In-Band Site Configuration
  - Cisco ACI In-band Configuration Documentation
  - Cisco DCNM In-band Configuration Documentation

□ I have reviewed and addressed the prerequisites for Insights

   c. Check the check box for **I have reviewed and addressed the prerequisites for Cisco Nexus Dashboard Insights**, and click **Let’s Get Started**.

3. In the **Let’s Configure the Basics** page, in the **Site Groups Setup** area, click **Configure**, and verify your site group is displayed as expected.



Insights Setup

Let's Configure the Basics

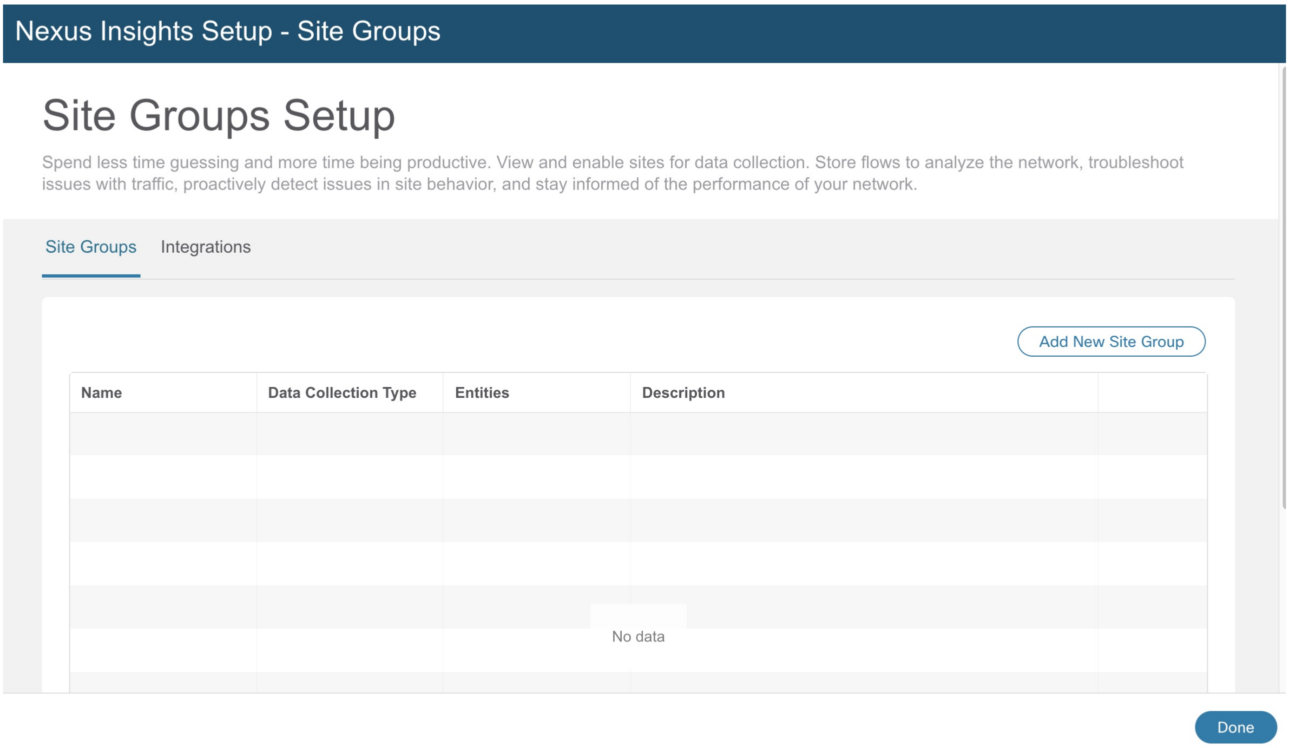
After you have addressed the prerequisites for Nexus Dashboard Insights, there are a few things that you'll need to set up before diving in. Let's set those things up now.

Site Groups Setup

Spend less time guessing and more time being productive. View and enable sites for data collection. Store flows to analyze the network, troubleshoot issues with traffic, proactively detect issues in site behavior, and stay informed of the performance of your network.

Learn more about Nexus Dashboard and using flow analytics productively.

4. In the **Site Groups Setup** area, click **Add New Site Group**.



Nexus Insights Setup - Site Groups

Site Groups Setup

Spend less time guessing and more time being productive. View and enable sites for data collection. Store flows to analyze the network, troubleshoot issues with traffic, proactively detect issues in site behavior, and stay informed of the performance of your network.

Name	Data Collection Type	Entities	Description
No data			

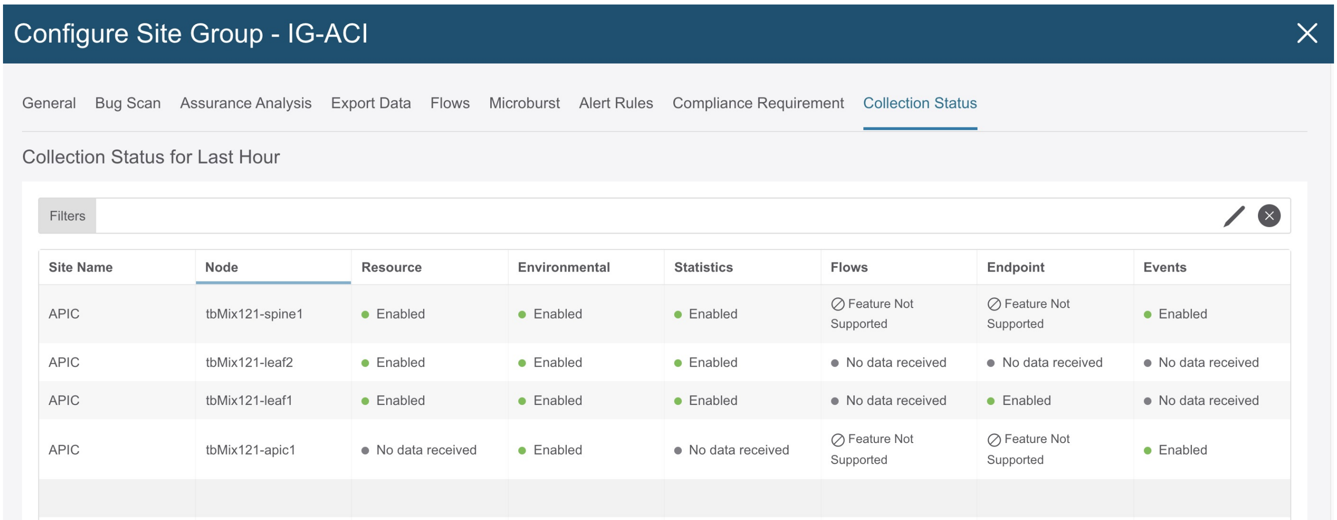
5. In the **Add New Site Group** dialog box **General** area, add the name and description for your Site Group.
6. In the **Configuration** area, in the **Data Collection Type** area, choose **Add Site(s)**. This will enable you to choose the sites that you want to add to this Site Group.
7. In the **Entity** area, click **Select Member**.

8. From the **Select a Site** dialog box, choose the appropriate site, and click **Select**. To add additional sites in the Site Group, repeat this step.
9. In the **Add New Site Group** dialog box, click the check mark to complete the task, and click **Save**. The site/s are added in the Site Group.
10. In the **Site Groups Setup** area, click **Done**.
11. In the **Let's Configure the Basics** page, click **Done**.

Enabling or Configuring Site Group Tabs

In Cisco Nexus Dashboard Insights, in the **Overview** page, at the top, choose your Site Group. Click the Actions menu next to it and choose **Configure Site Group**. In the **Configure Site Group** page, enable or configure the relevant features listed by tabs. You do not have to follow a sequential order to proceed with these tasks. You can perform/enable the tasks in any order.

- **General** tab: Site Group details are provided here including the site group name, data collection type and such. Site details related to sites that are in the site group are also listed here with details related to Collection Status, Configuration Status, Node Status, and Type.
- **Bug Scan** tab: For details, see Bug Scan.
- **Assurance Analysis** tab: For details about running Assurance Analysis on Site Groups containing sites or uploaded files, see Add a Site Group and Run Assurance Analysis for a Site Also see, Upload a File to a Site Group and Run Assurance Analysis.
- **Export Data** tab: For details, see Export Data.
- **Flows** tab: For details, see Configure Flows.
- **Microburst** tab: For details, see Microburst Support for Interface Statistics
- **Alert Rules** tab: For details, see Alert Rules.
- **Compliance Requirement** tab: For details, see Compliance.
- **Collection Status** tab: Telemetry data displaying a status check is displayed here such as Site Name, Node, Resource, Environmental, Statistics, Flows, Endpoints, Events. See the following example page.



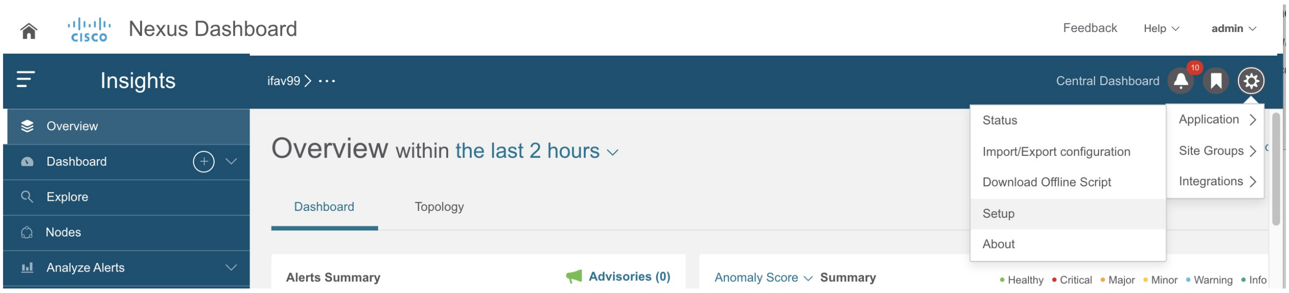
Collection Status for Last Hour

Site Name	Node	Resource	Environmental	Statistics	Flows	Endpoint	Events
APIC	tbMix121-spine1	● Enabled	● Enabled	● Enabled	⊘ Feature Not Supported	⊘ Feature Not Supported	● Enabled
APIC	tbMix121-leaf2	● Enabled	● Enabled	● Enabled	● No data received	● No data received	● No data received
APIC	tbMix121-leaf1	● Enabled	● Enabled	● Enabled	● No data received	● Enabled	● No data received
APIC	tbMix121-apic1	● No data received	● Enabled	● No data received	⊘ Feature Not Supported	⊘ Feature Not Supported	● Enabled

Cisco Nexus Dashboard Insights Configuring the Basics for Day N Setup

If your Day 0 setup is complete, and you are launching the Cisco Nexus Dashboard Insights service again, then perform the following actions.

1. When you launch the Nexus Dashboard Insights service, the **Overview** page is displayed.
2. In the top right side of the page, click the Settings icon > **Application** > **Setup**.



3. In the **Let’s Configure the Basics** page, click **Click the Prerequisites for Cisco Nexus Dashboard Insights** link, and verify that you have configured the required mandatory settings.
4. After verifying, and if required, check the check box for **I have reviewed and addressed the prerequisites for Cisco Nexus Dashboard Insights**, and click **Let’s Get Started**.
5. In the **Site Groups Setup** area, click **Edit configuration**, and in the **Site Groups Setup** area, verify your site group is displayed as expected.

> If you want to perform edits to a Site Group, click the Actions menu > **Edit** for your Site Group and perform your edits. To edit a site in a Site Group, see Manage Site Groups.

6. Click **Done**.

Guidelines and Limitations

- After Cisco Nexus Dashboard reboot, it is recommended to wait until the following are complete for the Cisco Nexus Dashboard to restore functionality:
  - The Cisco Nexus Dashboard cluster displays green. Or
  - The `acs` health CLI command displays healthy.
- When you upgrade fabric policy or upgrade nodes, if there is a connectivity loss between the fabric and Cisco Nexus Dashboard cluster, Nexus Dashboard Insights may raise incorrect missing Endpoint anomaly.
- If the `oper-state` of Interface and Port Channel is down before Nexus Dashboard Insights installation, then Interface and Port Channel down anomaly will not be raised. After Nexus Dashboard Insights installation, anomaly is captured only when the `oper-state` is up or down.
- Nexus Dashboard Insights depends only on in-band network for all communication with the fabric and Cisco Nexus dashboard may not accurately reflect the reachability status for Nexus

Dashboard Insights.

- For flow telemetry the Nexus Dashboard Insights captures the maximum anomaly score for a particular flow, for the entire cycle of the user specified time range. This anomaly score calculation is inconsistent with the other resources anomaly calculation.

About Device Connector

Data center apps and services such as the Cisco Nexus Dashboard Insights service is connected to the Cisco Intersight cloud portal through a Device Connector which is embedded in the management controller of the Cisco Nexus Dashboard platform.

See Cisco Nexus Dashboard User Guide for Configuring the Device Connector and Claiming a Device.

For connectivity requirements, see Network Connectivity Requirements.

Overview

Navigating Nexus Dashboard Insights Overview Page

The Nexus Dashboard Insights GUI consists of the Navigation pane and Work pane.

Navigation Pane

The Nexus Dashboard Insights navigation pane contains the following categories:

Overview: The main page for Nexus Dashboard Insights provides immediate access to site groups, with advisories, anomalies, alerts, timeline, and top nodes by anomaly score, and topology view.

Dashboard: The custom dashboard allows you to create a unique dashboard and add views to the dashboard.

Explore: The Explore feature allows you to discover assets and their object associations in an easy-to-consume natural language query format.

Nodes: A detailed view of the nodes with a graphical representation of top nodes and top resources.

Analyze Alerts: Access to total advisories, field notices, and PSIRTs, as well as anomalies that include top nodes by anomaly score, severity, and other details. The sub-tabs in this area are as follows:

- Anomalies: The Anomalies Dashboard consists of anomalies raised for resource utilization, environmental issues, interface and routing protocol issues, flows, endpoints, events, assurance analysis for sites and uploaded files, compliance, change analysis, and static analysis.
- Advisories: The Advisories Dashboard consists of relevant impact due to field notice, EOL/EOS of software and hardware, PSIRTs at a node level and compliance.

Compliance: Compliance enables you to achieve continuous compliance with security policies and compliance checks.

Troubleshoot: The sub-tabs in this area are as follows:

- Delta Analysis: Delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two snapshots.
- Log Collector: Collect and upload the logs for devices in your network to Cisco Intersight Cloud. Enables Cisco TAC to trigger on-demand collection of logs for user devices on the site and pull the logs from Cisco Intersight Cloud.

Browse: The sub-tabs in this area are as follows:

- Resources: 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.

- Flows: This feature provides deep insights at a flow level giving details such as average latency, packet drop indicator and flow move indicator.
- Endpoints: 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.
- Interfaces: This includes monitoring of interfaces on the Cisco APIC and site nodes.
- Protocols: This includes monitoring protocols on the Cisco APIC and site nodes.
- Events: This includes monitoring of events, faults and configuration changes.

Change Management: The sub-tabs in this area are as follows:

- Firmware Update Analysis: This feature suggests an upgrade path to a recommended software version and determines the potential impact of the upgrade. It also helps with the pre-upgrade and post-upgrade validation checks.
- Pre-Change Analysis: This feature allows you to model the intended changes and verify if the changes generate the desired results.

Top Menu

Along the top of your Nexus Dashboard Insights page and above the Work pane, there are additional links and icons available as follows:

Site Group or Site: The link displays the name of the Site Group or a Site. To change the selection to a different Site Group or Site, click the Site Group or Site link to display the **Select Site Group or Site** dialog box and change your selection.

To configure the selected Site Group or Site, click the Actions menu next to the Site Group, and click **Configure Site Group**.

To add Compliance Requirements to the selected Site Group, click the Actions menu > **Add** > **Compliance Requirement**. To add Alert Rules to the selected Site Group, click the Actions menu > **Add** > **Alert Rules**.

Help Center: Above the **Central Dashboard**, **Notifications**, **Bookmark** and **Settings** icons is the **Help** drop-down menu. Click **Help** > **Help Center** to access the **Help Center** page which contains links to documentation resources. Click the Nexus Dashboard Insights tile to find the appropriate resources.

Central Dashboard: This link takes you to the Central Dashboard page which provides an overview of alerts at-a-glance, top site groups by anomalies or by advisories, and other site group related details.

Notifications icon: Click this icon to view notifications from Cisco : 🔔

- Anomalies occurred based on the selected time range
- Anomalies that are in progress
- New process, new advisory, and new anomaly notifications

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.

Settings icon:

⚙

In the drop-down menu for this icon, you see **Application**, **Site Groups**, **Integrations**.

When you click the **Application** icon, you can choose from **Status**, **Import/Export configuration**, **Download Offline Script**, **Setup**, **About**.

- Status: Click this to see Application Status such as alerts and capacity usage.
- Import/Export configuration: This feature allows you to import and export configurations such as Site Groups, Alert Rules, Export Settings and such.
- Download Offline Script: Click this to download the offline script that is required to upload files to run assurance analysis.
- Setup: Click this for the link to the Nexus Dashboard Insights setup page.
- About: Click this to get details about Nexus Dashboard Insights version number.

When you click the **Site Groups** icon, you can choose to **Manage** Site Groups. For details, see Manage Site Groups.

When you click the **Integrations** icon, you can choose to **Manage** or **Add** Integrations. For details, see Integrations.

Work Pane

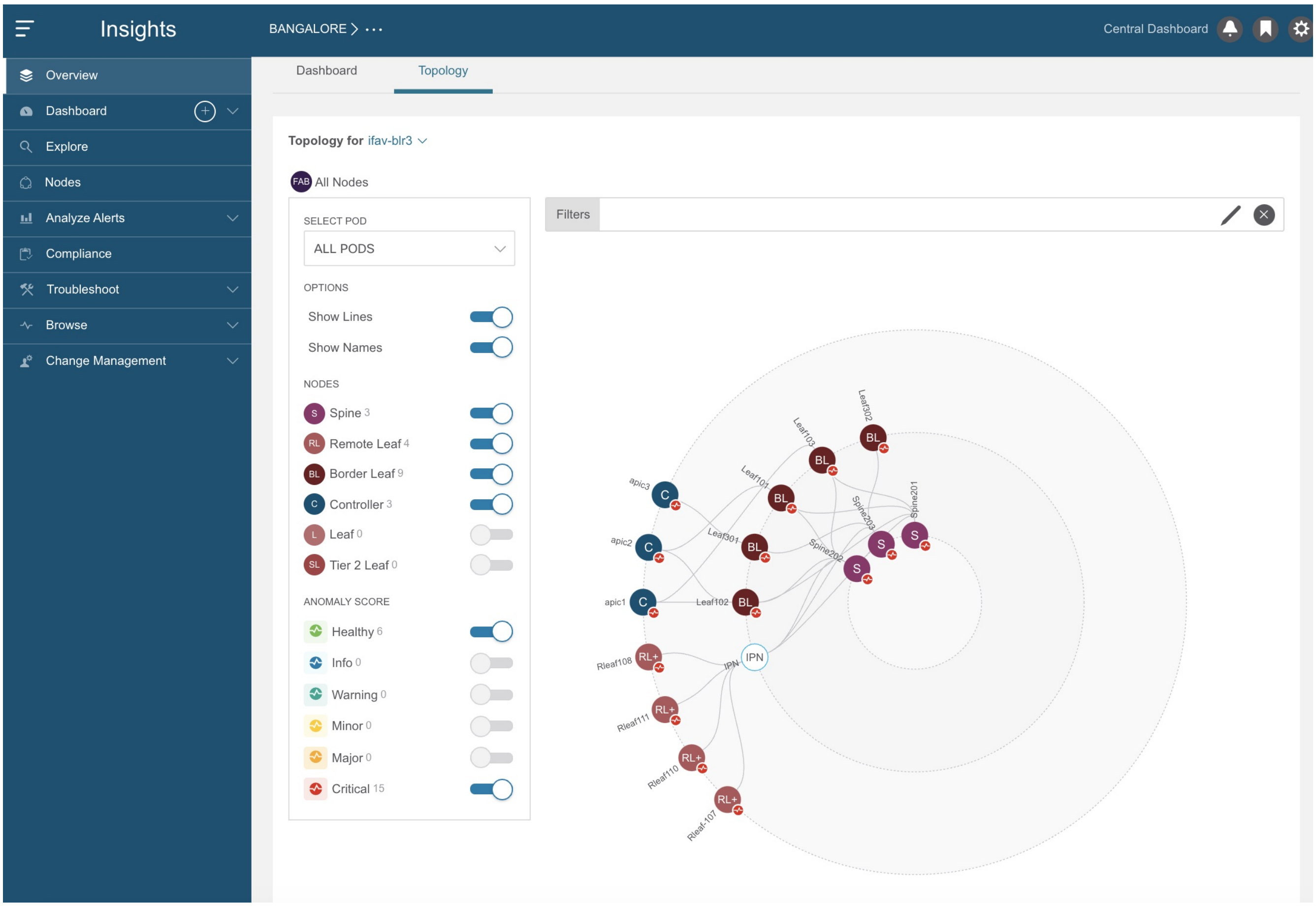
The Work pane is the main viewing location in Nexus Dashboard Insights. All information tiles, graphs, charts, and lists appear in the work pane. When viewing the **Overview** page, it contains the **Dashboard** tab and the **Topology** tab.

Dashboard Tab

The **Dashboard** tab displays different tiles such as Alerts Summary, Anomaly Score, Alert Detection Timeline, Anomalies Breakdown, Advisories Breakdown, and Top Nodes by Anomaly Score. In an information tile, you can click a numeric value to switch to view more details about the specific item you clicked.

Topology Tab

In the Nexus Dashboard Insights topology view, information with a radial graph for the selected Site Group is displayed. There is a filters options available to choose what you want to view such as by nodes and anomaly scores.



Topology for ifav-blr3

FAB All Nodes

SELECT POD

ALL PODS

OPTIONS

Show Lines ●

Show Names ●

NODES

S Spine 3 ●

RL Remote Leaf 4 ●

BL Border Leaf 9 ●

C Controller 3 ●

L Leaf 0 ○

SL Tier 2 Leaf 0 ○

ANOMALY SCORE

Healthy 6 ●

Info 0 ○

Warning 0 ○

Minor 0 ○

Major 0 ○

Critical 15 ●

Configuring the Time Zone for Nexus Dashboard Insights

By default the Nexus Dashboard Insights GUI displays the user's local time zone date and time.

Starting with this release, you can configure your time zone setting to a different time zone in Nexus Dashboard. The time zone feature is available per user and is stored in your user preferences.

The time zone that you select will be reflected in the time values displayed in your GUI. All the detection timelines and timestamps that are shown in the GUI will be reflect the time values for the time zone you have selected.

Procedure

1. Log in to Nexus Dashboard.
2. Choose **admin** > **User Preferences**.
3. In the **User Preferences** page, in the **Time Zone** area, the default time zone value is selected as **Automatic**.

   This is the user’s local time zone.

4. In the **Time Zone Preference** field, choose **Manual**.
5. In the **Nearest City** field, enter your preferred city to populate the appropriate time zone in the **Time Zone** field.

   Alternatively, you can drag the pin in the map to the city of your choice, and it will populate the fields for **Nearest City** and **Time Zone**.

6. Click **Save**.

The time zone that you select will be reflected in the time values displayed in your Nexus Dashboard Insights GUI. All the detection timelines and timestamps that are displayed in the Nexus Dashboard Insights GUI will reflect the time values for the time zone you have selected.

Overview Page

The **Overview** page, in the Work pane contains the **Dashboard** tab and the **Topology** tab. These tabs are described in this section.

Dashboard Tab

The **Dashboard** tab displays the alerts detected and anomalies detected in the site nodes. It also displays recommended advisories for the nodes in the selected site.

Each Cisco ACI node streams telemetry events from the site to Nexus Dashboard Insights, which then analyzes the events and proactively detects issues in the site. In Nexus Dashboard Insights, you can view relevant information and select specific items to view details. The Cisco Nexus Dashboard Insights dashboard provides immediate access to advisories and anomalies occurring in the network.

The Advisories on the dashboard display three levels of advisory severity for switch hardware and software in your network. It categorizes by severity and identifies software versions and hardware platforms to which the advisories apply. Advisories are delivered based on the detection of relevant field notices, PSIRTs, bugs, software, hardware, and hardening violations. Cisco Nexus Dashboard Insights considers this information and recommends:

- Software or hardware upgrades to address bugs, PSIRTs, and field notices
- CALL TAC
- Cisco Recommendations
- Software Upgrade Path

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.

In this page, you can also view a breakdown of anomalies by severity when you choose **Anomalies Breakdown by Severity**. Next to the colored severity dots, the numbers are a count of devices at that anomaly level. The sum of these anomaly counters will be the same as the large total count of anomalies.

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

The **Dashboard** tab provides the following details in tiles:

Property	Description
Anomalies By Category	Displays the number of Anomalies by their Category. Anomaly categories include: • Flows • Resources • Environmental • Statistics • Endpoints • Bug

Property	Description
Advisories By Category	Displays the number of Anomalies (internal site failures) and their severity level. Clicking on the area shows detail fault information, such as **Node** and **Anomaly Score**. • PSIRT • Field Notice • HW EOL • SW EOL • Compliance
Top Nodes by Anomaly Score	Displays the overview of top nodes and their anomaly status. The anomaly status is based on the features that contribute to the anomaly. Click each of these features to display specific information for the selected node. • PSIRTS • Field Notices • HW EOL • SW EOL

Click any property from **Anomalies by Category** and **Advisories by Category** to access the *Analyze Alerts* work pane.

Node Inventory

The dashboard displays the following information of the nodes in the site.

Property	Description
Anomaly Score	Displays the overview of top nodes and their anomaly scores. The anomaly scores are based on the features that contribute to the anomaly.
Leaf Nodes	Displays the total number of leaf nodes in the site with anomalies.
Spine Nodes	Displays the total number of spine nodes in the site with anomalies.
Controllers	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.

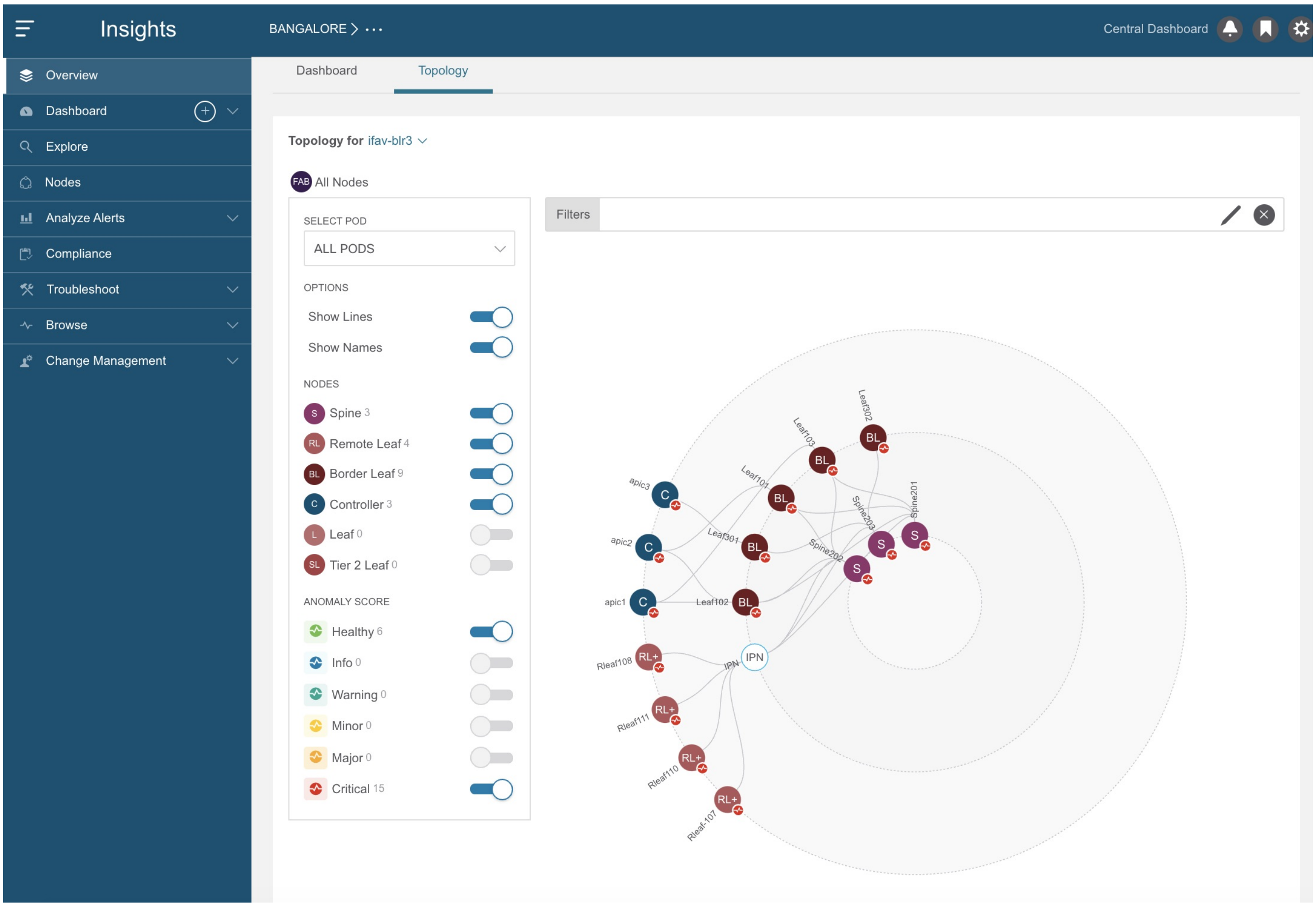
Topology Tab

For a topology view of all the nodes with anomalies in the Site Group, in the **Overview** page, view the Work pane **Overview** area. Click the **Topology** tab.

Topology displays the interconnection of the nodes in the fabric using the LLDP protocol information. The page displays the list of nodes, node types, interface names, LLDP information from a leaf node to another leaf node, IPN, and anomaly score on the link. In this view, you can distinguish between a spine node, leaf node, and border leaf node with different colors and interface names.

IPN links are spine node links connected to the IPN and are distinguished from the links connected to the internal leaf nodes. The IPN is shown as a physical entity in the topology.

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.



Topology for ifav-blr3

FAB All Nodes

SELECT POD
ALL PODS

OPTIONS
Show Lines ●
Show Names ●

NODES
S Spine 3 ●
RL Remote Leaf 4 ●
BL Border Leaf 9 ●
C Controller 3 ●
L Leaf 0 ○
SL Tier 2 Leaf 0 ○

ANOMALY SCORE
Healthy 6 ●
Info 0 ○
Warning 0 ○
Minor 0 ○
Major 0 ○
Critical 15 ●

Use the zoom-in capability to narrow down on portions of the infrastructure based on logical constructs such as EPG, VRF, Tenant.

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 pane displays general additional anomaly details for the node.

Guidelines and Limitations

- Nodes that do not have LLDP information are not shown in the topology.
- Cisco Nexus 9200, 9300-EX, -FX, and -GX platform switches, and N9K-C9316D-GX and N9K-C9364C-GX switches are not discovered and displayed in the topology.

Alert Detection Timeline

The timeline displays various alerts that occurred during the entire cycle of user selected time range. In the **Overview** page, in the Work pane, in the **Dashboard** tab, in the **Alert Detection Timeline**, The graph displays the time zones when the alerts occurred. The timeline displays anomalies and advisories The color of an anomaly or advisory is based on its severity.

For further details, see Analyze Alerts.

Alert Detection Timeline Icons

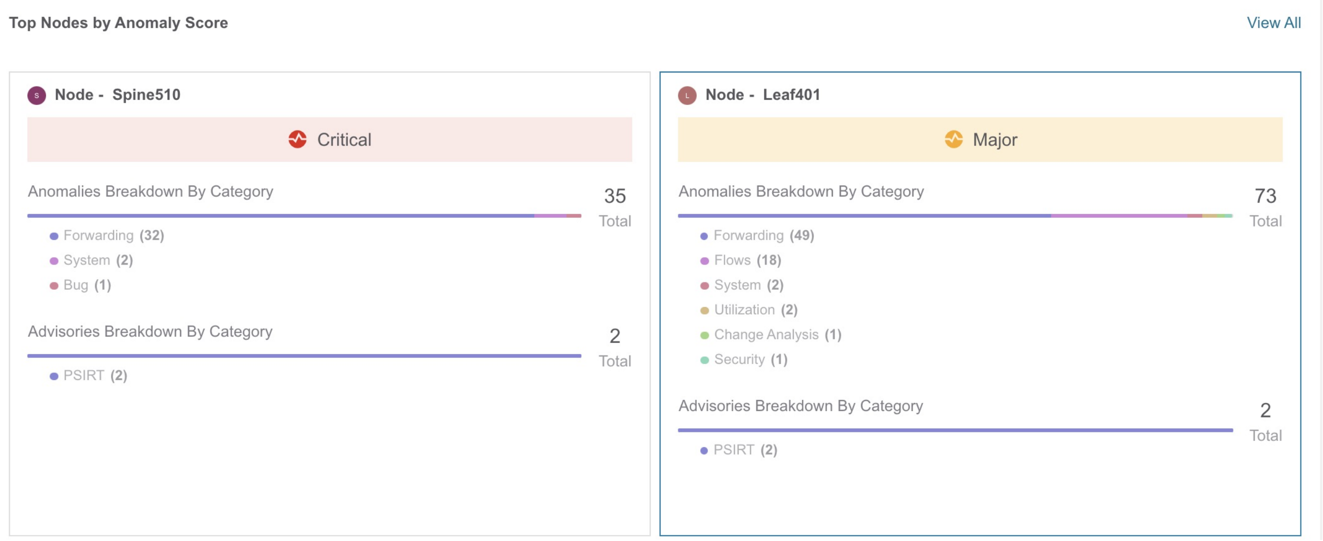
- The colored round dots correspond to events, faults, and audit logs for the node.
- Multiple rings around it in the timeline represents a group of objects. A ring by itself in the timeline represents single object.
- The heart icon represents the anomalies exclusively. The blue circle indicates the currently selected anomaly.

Top Nodes by Anomaly Score

In the **Overview** page, in the Work pane, in the **Dashboard** tab, the **Top Nodes by Anomaly Score** area is displayed.

This section displays the overview of top nodes and their anomaly scores. Each node card displays anomalies and advisories that are further broken down by categories.

Click a 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 categories of the node such as Resource Utilization, Environmental, Statistics, Flows, and Events. Click each of these features to display specific information for the selected node.



Top Nodes by Anomaly Score

View All

Node - Spine510

Critical

Anomalies Breakdown By Category — 35 Total

- Forwarding (32)
- System (2)
- Bug (1)

Advisories Breakdown By Category — 2 Total

- PSIRT (2)

Node - Leaf401

Major

Anomalies Breakdown By Category — 73 Total

- Forwarding (49)
- Flows (18)
- System (2)
- Utilization (2)
- Change Analysis (1)
- Security (1)

Advisories Breakdown By Category — 2 Total

- PSIRT (2)

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

Add and Manage Sites in Site Groups and Run Assurance Analysis

Assurance Analysis

Nexus Dashboard Insights enables you to perform assurance analysis using two methods:

- You can select and analyze sites that are part of a Site Group.
- You can upload files as part of a Site Group and run assurance analysis on the uploaded files.

Select and analyze sites that are part of a Site Group: Assurance analysis involves collecting data from sites, running the analysis to create a model with the collected data, and generating the results.

Assurance analysis provides assurance in real time. For assurance analysis of sites in Site Groups, the data collection, model generation, and results generation are carried out simultaneously. The collected data is analyzed immediately after collection followed by result generation. This is repeated after a fixed time interval as specified by the user. For details, see Add a Site Group and Run Assurance Analysis for a Site.

Upload files as part of a Site Group and run assurance analysis on the uploaded files For assurance analysis of uploaded files, a one-time assurance is provided. This assurance analysis allows you to decouple the data collection stage from the analysis stage. The data is collected using a Python script and the collected data is then uploaded to Nexus Dashboard Insights to provide a one-time assurance. The collected data can also be analyzed at a later time. It enables the user to collect the data during change management windows and then perform the analysis. For details, see Offline Script and Upload a File to a Site Group and Run Assurance Analysis.

Add a Site Group

In this procedure, in Cisco Nexus Dashboard Insights, you add a Site Group, and you select site/s that are displayed in Cisco Nexus Dashboard Insights. Before sites can be selected for a Site Group, they must first be added in Cisco Nexus Dashboard.

Prerequisites

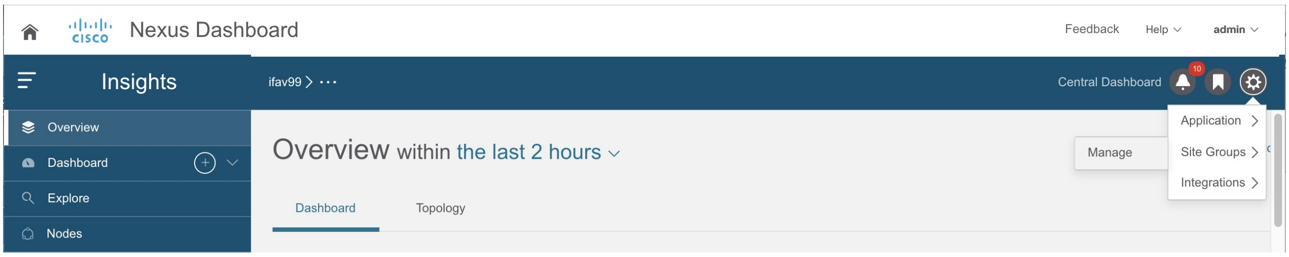
Before you start this procedure, the administrator for Cisco Nexus Dashboard must have completed adding the appropriate site/s in the **Sites** area. For more details, see the *Cisco Nexus Dashboard User Guide*. When this task is complete in Cisco Nexus Dashboard, click the Cisco Nexus Dashboard Insights service from the **Services** area of the Cisco Nexus Dashboard Navigation pane, and wait for the service to load.

If there is no Site Group in Cisco Nexus Dashboard Insights already created, the **No Site Group enabled** page will be displayed when you enter the service. Click the **Configure Site Group** tab, and follow the steps below. If a Site Group is already configured when you enter Cisco Nexus Dashboard Insights, the **Overview** page is displayed.

Procedure

Follow these steps to add site/s to your Site Group.

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Settings icon on the top right > **Site Groups** > **Manage**.



3. In the **Manage Site Groups** page, click **Add New Site Group**.
4. In the **Add New Site Group** dialog box **General** area, add the name and description for your Site Group.
5. In the **Configuration** area, in the **Data Collection Type** area, choose **Add Site(s)**. This will enable you to choose the sites that you want to add to this Site Group.
6. In the **Entity** area, click **Select Member**.
7. From the **Select a Site** dialog box, choose the appropriate site, and click **Select**. To add additional sites in the Site Group, repeat this step.
8. In the **Add New Site Group** dialog box, click the check mark to complete the task, and click **Save**. The site/s are added in the Site Group.

To run Assurance Analysis for your Site Group, after adding a Site to a Site Group, see Run Assurance Analysis for a Site.

Run Assurance Analysis for a Site

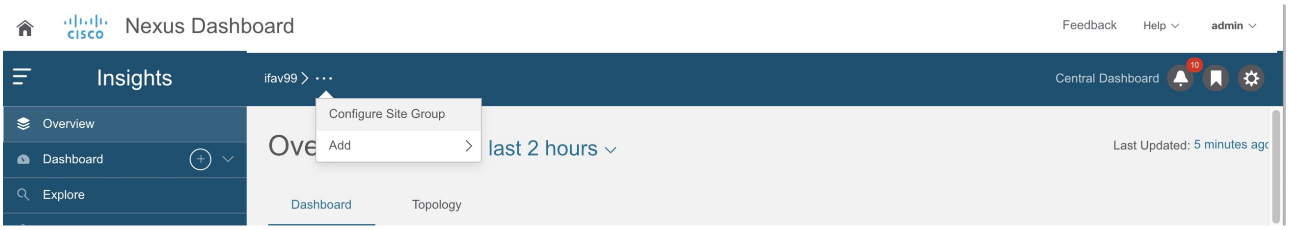
Prerequisites

The required site/s are added to your Site Group. For details see Add a Site Group.

Procedure

Follow these steps to run Assurance Analysis for your Site Group.

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to it and choose **Configure Site Group**.



3. In the **Configure Site Group** page, perform the following actions:
    a. Click the **Assurance Analysis** tab, click the pencil/edit icon.
    b. In the **Configuration** dialog box, set the **State** field to **Enabled**, to enable the Assurance Analysis.
    c. Specify the appropriate Analysis start time, the repeat frequency of the analysis cycle, and when you want the analysis to end. Click **Save**.
4. In the **Configure Site Group** page, you can see your site, and the **State** displays that your Assurance Analysis is enabled.

> In the **Assurance Analysis** tab, if there is no other analysis currently running for a site, you have the option to click the **Run Now** button for that site to run a one-time instant analysis.

Offline Script

In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Download Offline Collection Script** to download the Python script. Run the downloaded script to collect the data for assurance.

> The python offline data collection script is only supported on Mac OS or CentosOS. Running the script from a Windows server will result in an error and Cisco Nexus Dashboard Insights will indicate that the APIC version is unsupported.

The following items are provided in the Offline Script:

- Data Collection Script for Assurance Analysis
- Alert Rules Migration Script
- Compliance Requirements Migration Script
- Script to display PSIRTs, Field Notices, and EOL advisories for offline sites

Data Collection Script for Assurance Analysis

The Nexus Dashboard Insights data collection script is a Python script that polls the Cisco APIC and Cisco DCNM clusters for a series of REST API and CLI calls. For information about the REST API calls and CLI calls, see the readme.md file that is included with the script.

See the readme.md file for information on the Python dependencies and the process to install the dependencies in a virtual environment. The readme.md file provides the complete list of objects and **show** commands collected from the Cisco APIC, spine switches, and leaf switches. The readme.md file is available inside the same zip file with the offline analysis script file. The offline analysis script is downloadable directly from the Nexus Dashboard Insights) appliance from the settings icon.

The workstation on which the script is being launched must have out-of-band management connectivity to the Cisco APIC and Cisco DCNM clusters. Make sure that every node in the Cisco ACI fabric has an out-of-band management IP address configured. Make sure that the firewall does not block HTTPS (for using the REST API) and SSH (for connecting to the leaf switches and spine switches). Make sure that the proxy settings are properly set to allow HTTPS connections.

The readme.md file provides the syntax for using the script. By default, the script will run 3 iterations of the data collection at a 3 minute interval between iterations, although you can specify the number of iterations by using the **-iterations** option. The total expected collection time ranges between 18 to 20 minutes from start to finish for 3 snapshots for a fabric with around 20 leaf switches. Larger fabrics will take longer time depending on complexity of the configuration and scale of the fabric.

Alert Rules Migration Script

This script is to migrate the Event Rules in Cisco Network Assurance Engine (Cisco NAE) release 5.1 to Alert Rules in Cisco Nexus Dashboard Insights, release 6.0.1. You will require the exported configuration file and the Assurance group name from the Cisco NAE setup to run this script.

Compliance Requirements Migration Script

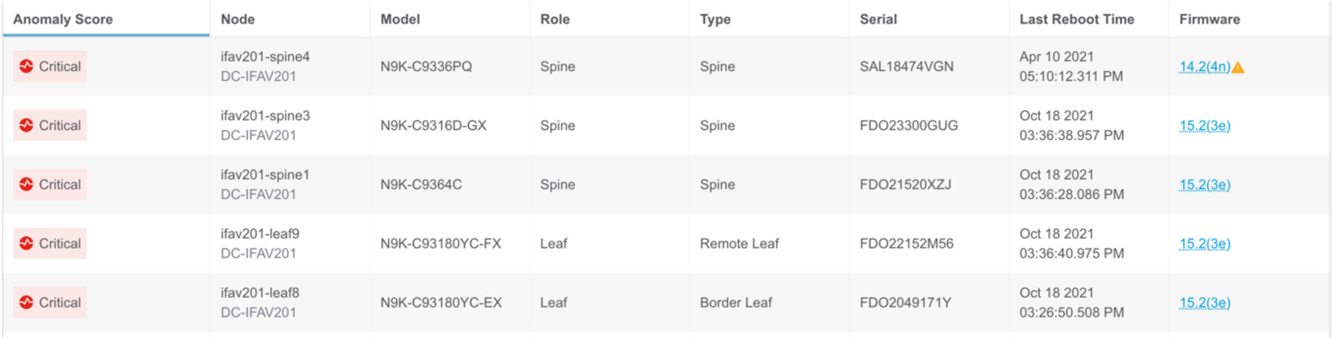
This script is to migrate the compliance requirements from Cisco Network Assurance Engine (Cisco NAE) release 5.1 to a given site group in Cisco Nexus Dashboard Insights, release 6.0.x.

Script to display PSIRTs, Field Notices, and EOL advisories for offline sites

This script is to display PSIRTs, Field Notices, and EOL advisories for offline sites. It also displays Cisco Recommended Version for offline sites.

After you upload a file to a Site Group, select the Site Group or site. See Upload a File to a Site Group and Run Assurance Analysis. The PSIRTs, Field Notices, and EOL advisories are displayed in the **Overview Page** in the Advisories Breakdown area.

To view the Cisco Recommended Version for offline sites, navigate to the **Nodes** page. In the **Nodes** table, hover around the orange triangle icon to view the Cisco Recommended Version for the node.



Anomaly Score	Node	Model	Role	Type	Serial	Last Reboot Time	Firmware
Critical	ifav201-spine4 DC-IFAV201	N9K-C9336PQ	Spine	Spine	SAL18474VGN	Apr 10 2021 05:10:12.311 PM	14.2(4n)⚠
Critical	ifav201-spine3 DC-IFAV201	N9K-C9316D-GX	Spine	Spine	FDO23300GUG	Oct 18 2021 03:36:38.957 PM	15.2(3e)
Critical	ifav201-spine1 DC-IFAV201	N9K-C9364C	Spine	Spine	FDO21520XZJ	Oct 18 2021 03:36:28.086 PM	15.2(3e)
Critical	ifav201-leaf9 DC-IFAV201	N9K-C93180YC-FX	Leaf	Remote Leaf	FDO22152M56	Oct 18 2021 03:36:40.975 PM	15.2(3e)
Critical	ifav201-leaf8 DC-IFAV201	N9K-C93180YC-EX	Leaf	Border Leaf	FDO2049171Y	Oct 18 2021 03:26:50.508 PM	15.2(3e)

Upload a File to a Site Group and Run Assurance Analysis

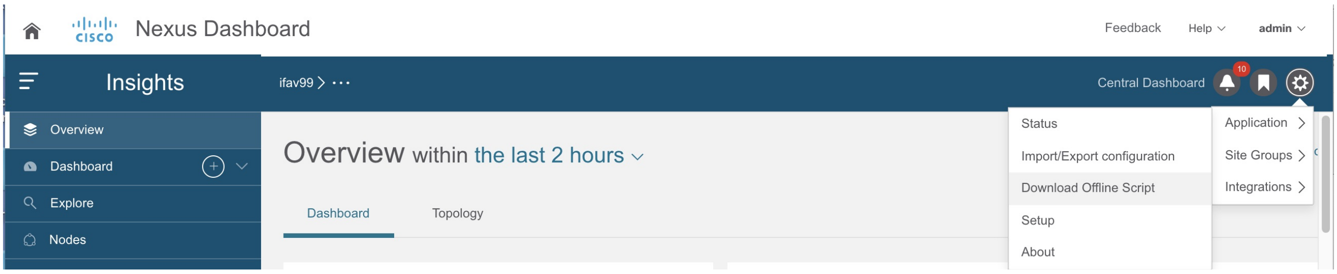
In this procedure, in Cisco Nexus Dashboard Insights, you add a Site Group, and you upload files of Data Collection Type **Upload File** to the Site Group. Then you run Assurance Analysis for your Site

Group.

Prerequisites

If required, download the Python script to collect the data for assurance.

In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Download Offline Collection Script** to download the Python script. Run the downloaded script to collect the data for assurance.



The python offline data collection script is only supported on Mac OS or CentosOS. Running the script from a Windows server will result in an error and Cisco Nexus Dashboard Insights will indicate that the APIC version is unsupported.

Use the following procedure to upload a file to a Site Group and run Assurance Analysis. This Assurance Analysis will be a point-in-time snapshot based analysis. To perform an Assurance Analysis on an uploaded file, create a Site Group first. Then upload and associate the file containing data with the Site Group.

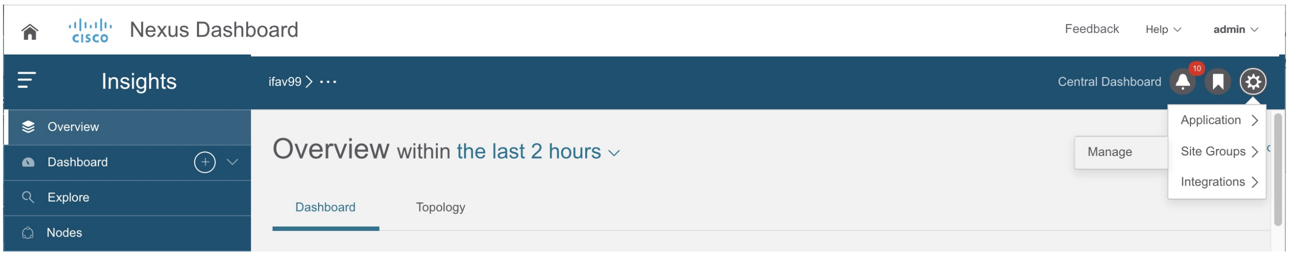
As you have uploaded the file in Cisco Nexus Dashboard Insights, the Cisco Nexus Dashboard Site Manager will not be aware of such uploaded files.

Upload a file containing your collected data and associate it with a Site Group.

If there are no Site Groups in the Cisco Nexus Dashboard Insights service already created, the **No Site Group enabled** page will be displayed when you enter the service. Click the **Configure Site Group** tab, and follow the steps below. If a Site Group is already configured when you enter the Cisco Nexus Dashboard Insights service, the **Overview** page is displayed.

Follow these steps to add a file to your Site Group.

1. Click the Settings icon on the top right > **Site Groups** > **Manage**.
2. In the **Manage Site Groups** page, click **Add New Site Group**.



3. In the **Add New Site Group** dialog box **General** area, add the name and description for your

Site Group.

4. In the **Configuration** area, in the **Data Collection Type** area, choose **Upload File**. This will enable you to upload the file that you want to add to this Site Group.
5. In the **Site** field, add a name.
6. Select or drag and drop a file in the **Select a file or drag and drop it in here** area. Accepted files are .gz.
7. Click **Save**. The file is added in the Site Group.

Follow these steps to run Assurance Analysis for your Site Group.

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to it, and choose **Configure Site Group**.
3. In the **Configure Site Group** page, **General** tab, under **Sites**, verify that the **Collection Status** for your file is enabled.
4. Click the **Assurance Analysis** tab, locate your uploaded file, and click the **Run Offline Analysis** tab to run a one-time instant analysis.
5. After the analysis is completed, in the **Overview** page, in the **Alert Detection Timeline** area, choose the snapshot time when the data in the uploaded file was collected.

   > The snapshot should be added for when the data in the uploaded file was collected and not when the analysis was run on the uploaded file.

6. Click **Apply** to view the Alerts.

Guidelines and Limitations for Configuring Assurance Analysis for Site Groups

- Cisco Nexus Dashboard Insights supports ACI and DCNM fabrics simultaneously. However, only homogenous fabric types are supported for addition to Site Groups. In a single Site Group, only a single site type is supported. You cannot combine ACI and DCNM sites in a Site Group.
- To add additional sites to the Site Group, you must first add the site in Cisco Nexus Dashboard **Site Manager**. Then you can enable them in the Site Group.
- If you take the Assurance Analysis from a Site Group and export the raw data set to upload a file to a Site Group, the uploaded file Assurance Analysis will only generate assurance related anomalies.
- Currently, if you begin an Assurance Analysis for an uploaded file site in Cisco Nexus Dashboard Insights, you can simultaneously continue to run the Assurance Analysis for sites that are already in progress. They will all run without any disruption to the behavior.
- If there are multiple files in a Site Group, choose a specific site and run Assurance Analysis on that site. For uploaded files, you must run Assurance Analysis on demand. You can run the Assurance Analysis multiple times, although it will be on the same data.
- For Assurance Analysis of uploaded files, when you upload a file in a specific Site Group, you

cannot associate that file with another Site Group.

- Alert Rules and Compliance Rules are valid in Assurance Analysis for uploaded files.
- In the **Configure Site Group** > **Assurance Analysis** page, the default frequency rate is set to run at every 15 minutes. If you observe that the jobs you have scheduled are queuing up, or the frequency is set to a time that is less than the time it takes to complete the jobs, then make the following adjustments to your jobs: Increase the frequency interval time so that the jobs do not overlap and the scheduler is able to complete one job before the next job is added to the scheduler queue. It is recommended that you set the frequency rate at 30 minutes.

Manage Site Groups

This section describes how to edit or delete sites from a Site Group and Integrations.

Edit a Site in a Site Group

To edit a site in a site group, perform the following actions:

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Settings icon on the top right > **Site Groups** > **Manage**.
3. In the **Manage Site Groups** page, **Site Groups** tab, click the Actions menu associated with the site you want to edit, and choose **Edit**.
4. In the **Edit Site Group** page, modify the site, and click **Save** to save your edits.

Delete a Site from a Site Group

To delete a site from a site group, perform the following actions:

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Settings icon on the top right > **Site Groups** > **Manage**.
3. In the **Manage Site Groups** page, **Site Groups** tab, click the Actions menu to the right of the site you want to edit, and select **Edit**.
4. In the **Edit Site Group** dialog box, click the **x** to the right of the site you want to edit, and click **Save** to delete the site.

Alternatively, you can delete a site from a site group as follows.

1. In the **Overview** page, click the Actions menu next to the selected Site Group name, and choose **Configure Site Group**.
2. In the **General** tab, click **Edit Site Group**.
3. Click the **x** to the right of the site you want to edit, and click **Save** to delete the site.

> If the site you want to delete is the last site in a Site Group, then you must delete the entire Site Group as there is a restriction that all Site Groups must contain at least one site.

Delete the Last Site from a Site Group

To delete a Site Group and the last site in it, perform the following actions:

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Settings icon on the top right > **Site Groups** > **Manage**.
3. In the **Manage Site Groups** page, **Site Groups** tab, click the Actions menu associated with the site you want to delete, and choose **Delete**.

This deletes the Site Group and the last remaining site in it.

If you want to perform a corrective action after the site is removed, and you want to add the site back, follow the steps to add a site in Nexus Dashboard Insights.

Delete an Uploaded File from a Site Group

To delete an uploaded file and the associated site from a site group, perform the following actions:

1. In the **Overview** page, choose you Site Group.
2. Click the Actions menu next to your Site Group > **Configure Site Group**.
3. In the **Configure Site Group** screen, click the **File Management** tab.
4. Click the delete icon to the right of the site you want to delete.

> ℹ When you delete an uploaded file from a Site Group, you delete the uploaded file and also remove the associated site.

Integrations

For details about Integrations, see the following section.

- About AppDynamics Integration

Configure Site Groups

Bug Scan

The Bug Scan feature enables you to schedule a bug scan or run an on-demand bug scan on your network. Nexus Dashboard Insights collects technical support information from all the nodes and runs them against known set of signatures, and flags the corresponding defects and PSIRTs. Nexus Dashboard Insights also generates advisories for PSIRTs and anomalies for defects. See Analyze Alerts for more information.

This feature allows you to choose a site containing the nodes from which to collect telemetry data. If the CPU and memory usage is below the set threshold then the tech support logs are collected and the scheduled bug scan is carried out for the nodes. If the CPU and memory usage is above the set threshold, the nodes are excluded from the scheduled bug scan.

In case the site is not configured properly to communicate with the device, Nexus Dashboard Insights notifies the following:

- The device is not configured for node interaction.
- You can not run on-demand bug scan job on the device.
- Nexus Dashboard Insights cannot connect to the device.

If the node interaction is not healthy on the device, you cannot select the device for bug scan to collect logs. The device cannot be selected to configure a job.

Default Bug Scan

When Nexus Dashboard Insights is installed, the service runs a default bug scan per site. When the site is enabled in Nexus Dashboard Insights, the default schedule and frequency of the bug scan is enabled. You can edit the default schedule of the bug scan.

The default bug scan follows the following schedule.

1. When the first site is added to Nexus Dashboard Insights, default bug scan is scheduled for once a week starting the closest Monday at 12 AM GMT.
2. When a new site is added to Nexus Dashboard Insights, default bug scan is scheduled for once a week starting 6 hours after the previous default time. The schedule will loop back to Monday at 12 AM at 28 sites.

Table 2. Example

Site Number	Bug Scan Schedule
Site 1	Once a week starting Monday at 12 AM
Site 2	Once a week starting the closest Monday at 6 AM
Site 3	Once a week starting Monday at 12 PM
Site 4	Once a week starting Monday at 6 PM

Site Number	Bug Scan Schedule
Site 5	Once a week starting Tuesday at 12 AM

Bug Scan Guidelines and Limitations

- The recommended time interval for scheduling a bug scan is dependent on the load on the Cisco Nexus Dashboards, the number of nodes in a site, and tech support file size. We recommend to run the bug scan run on 100 nodes over a 24 hour period.

  For example, if there are multiple sites such as site1 with 100 nodes, site2, site3, site4, and site5 with 25 nodes each, bug scan can be scheduled for site1 on alternate days, say at 12:00 AM. Rest of the sites, adding up to 100, can also be scheduled together for alternate days, but not on the same day as the site1. Since site2, site3, site4 and site5 each have 25 nodes and add to 100, the bug scan could be staggered and scheduled every 6 hours starting at 12 AM. So, based on above, the schedule could look like:

  Day 1

  - site1 at 12:00 AM

    Day 2

  - site2 at 12:00 AM
  - site3 at 6:00 AM
  - site4 at 12:00 PM
  - site5 at 6:00 PM

    You can measure the time taken by each site and a schedule bug scan accordingly with some buffer time for each site.

- The status of the bug scan is displayed as **unavailable** after updating the frequency of the schedule.
- If a bug scan job is running, and another bug scan job is scheduled, the second bug scan job will fail.

Schedule Bug Scan

Use this procedure to schedule a bug scan.

Procedure

1. From the Site Group menu, select a Site Group or site.
2. From the Actions menu next to the Site Group, choose **Configure Site Group** > **Bug Scan** to schedule a bug scan on the selected sites.

   The **Bug Scan** page appears. By default, bug scan is enabled for a site. The **General** table displays all the sites.

3. Click ✎ to schedule a bug scan job for the selected site.
4. Complete the following fields.
    a. Select **Enabled** to enable a bug scan.
    b. Select the Start Time, Frequency, and End Time.
    c. Click Save.
    d. Click **Scan Now**

    > If the CPU and memory is above 65%, the nodes are excluded from the bug scan.

5. The **History** table displays bug scan job information such as site name, status, type, nodes, start and end time.
6. Click the job in the table for the side pane to display additional job details.
7. Click the ↗ icon to display **Bug Scan** status page.
8. (Optional) Select an In Progress job and click **Stop** to stop a job.

On-Demand Bug Scan

Use this procedure to run an on-demand bug scan.

Procedure

1. From the Site Group menu, select a Site Group or site.
2. From the Actions menu next to the Site Group, choose **Configure Site Group** > **Bug Scan** to run an on-demand bug scan on the selected sites.

    The **Bug Scan** page appears. By default, bug scan is enabled for a site.

3. The **General** table displays all the sites. Select a site and click **Scan Now**.

    The **History** table displays bug scan job information such as site name, status, type, nodes, start and end time.

4. Click the job in the table for the side pane to display additional job details.
5. Click the ↗ icon to display **Bug Scan** status page.
6. (Optional) Select an In Progress job and click **Stop** to stop a job.

Export Data

The **Export Data** feature enables you to export the data collected by Nexus Dashboard Insights over Kafka and Email. Nexus Dashboard Insights produces data such as advisories, anomalies, audit logs, faults, statistical data, risk and conformance reports. When you import a Kafka broker, all the data is written as a topic. By default, the export data is collected every 30 seconds or at a less frequent duration. Starting with Nexus Dashboard Insights release 6.0.2, data can *also* be collected for specific resources (for CPU, memory, and interface utilization) every 10 seconds from the leaf and spine switches using a separate data pipeline. Additionally, CPU and memory data is collected for the controllers. The collected data is not stored in Elasticsearch by Nexus Dashboard Insights, but it is directly exported and pushed to your repository for consumption. Using the Kafka Export functionality, this data can then be exported to your Kafka Broker so that you can consume the data and push it into your data lake.

Additionally, you can configure an email scheduler to specify the data and the frequency with which you want to receive the information in an email.

Cisco Intersight is used for email notifications. See About Device Connector for more information.

Risk and Conformance Report

Starting from release 6.0.2, Risk and Conformance reports are scheduled to be generated everyday for each site, and you can subscribe to the latest reports by configuring an email scheduler. See Configure Email.

Risk and Conformance reports provides the status of the overall inventory for a site, including software release, hardware platform, and a combination of software and hardware conformance.

Risk and Conformance report contains the following information:

- Time stamp specified in the email scheduler
- Applicable site
- Frequency specified in the email scheduler
- Classification of devices into severities
- Node name
- Software and hardware conformance status
- Serial number
- IP address
- Software version
- Hardware model
- Software and hardware EOL date

The Risk and Conformance report also contains a detailed list of software and hardware components. For hardware components, modules such as switch, line card, fan, and power supply unit are also listed.

In a Risk and Conformance report, devices are classified into the following 3 severities based on the software release or hardware platform EOL dates. The severities include:

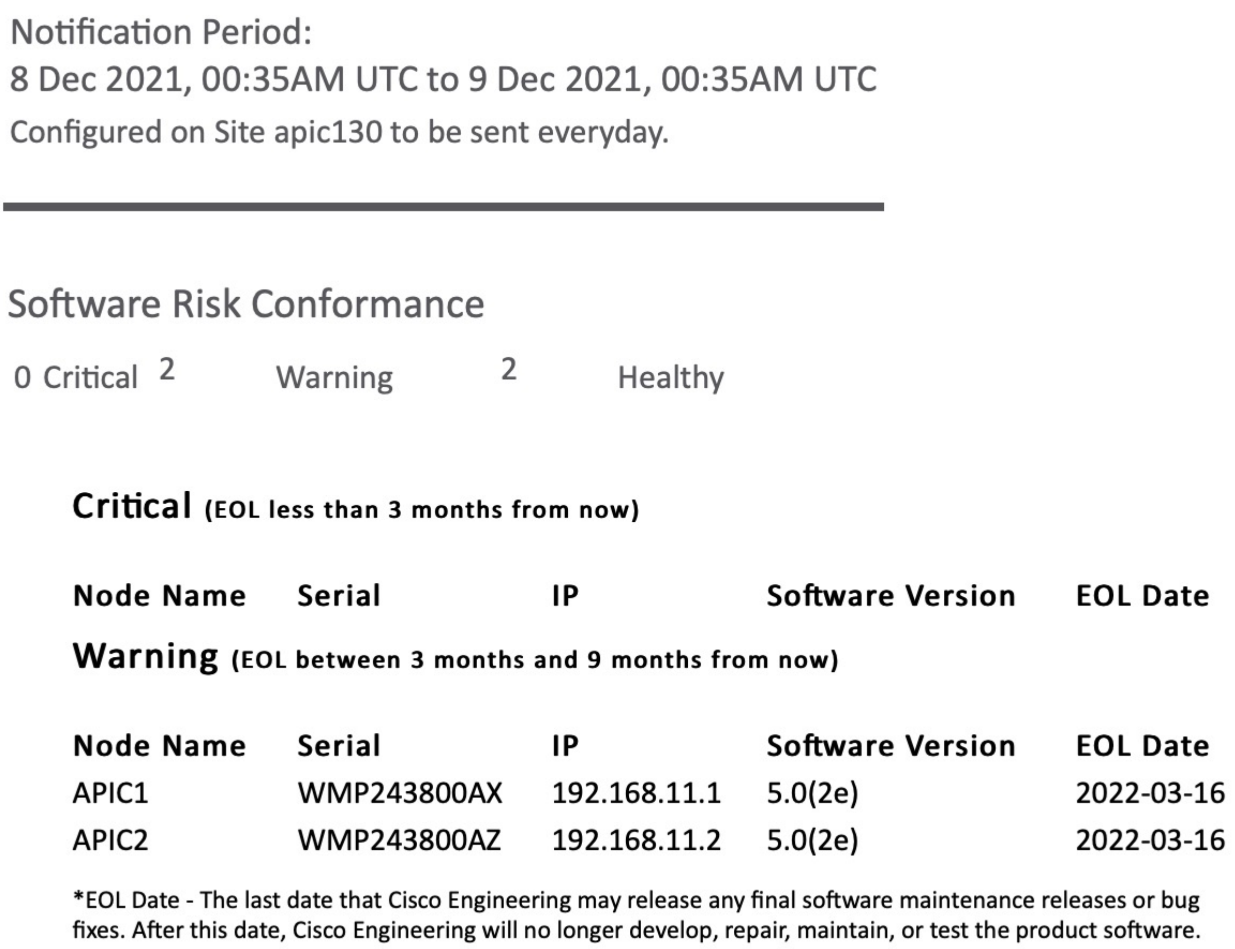
- Critical: EOL date is less than 3 months from today

- Warning: EOL date is between 3 months and 9 months from today
- Healthy: EOL date is more than 9 months from today or EOL is not announced

The **End of SW Maintenance Releases Date** in the *End-of-Sale and End-of-Life Announcement* is used as reference milestone to classify the inventory into a category of Critical, Warning, or Healthy.

Intersight connectivity is required to receive the reports via email.

Example of Risk and Conformance report for software



Notification Period:
8 Dec 2021, 00:35AM UTC to 9 Dec 2021, 00:35AM UTC
Configured on Site apic130 to be sent everyday.

Software Risk Conformance

0 Critical 2 Warning 2 Healthy

Critical **(EOL less than 3 months from now)**

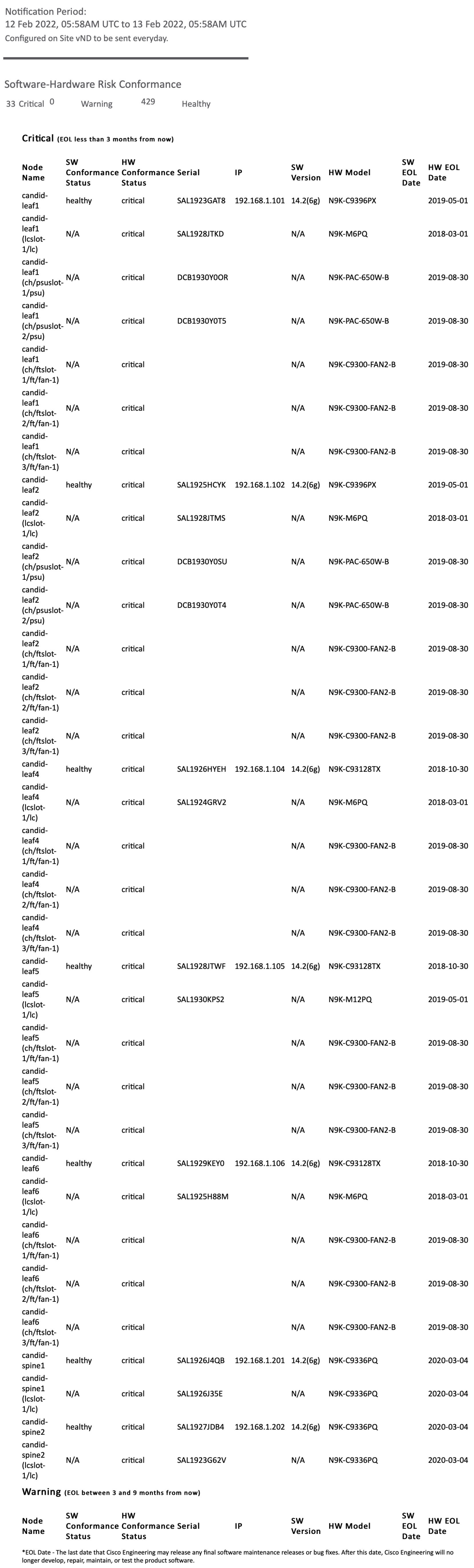
Node Name	Serial	IP	Software Version	EOL Date

Warning **(EOL between 3 months and 9 months from now)**

Node Name	Serial	IP	Software Version	EOL Date
APIC1	WMP243800AX	192.168.11.1	5.0(2e)	2022-03-16
APIC2	WMP243800AZ	192.168.11.2	5.0(2e)	2022-03-16

*EOL Date - The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.

Example of Risk and Conformance report for hardware



Notification Period:
12 Feb 2022, 05:58AM UTC to 13 Feb 2022, 05:58AM UTC
Configured on Site vND to be sent everyday.

Software-Hardware Risk Conformance

33 Critical 0 Warning 429 Healthy

Critical **(EOL less than 3 months from now)**

Node Name	SW Conformance Status	HW Conformance Status	Serial	IP	SW Version	HW Model	SW EOL Date	HW EOL Date
candid-leaf1	healthy	critical	SAL1923GAT8	192.168.1.101	14.2(6g)	N9K-C9396PX		2019-05-01
candid-leaf1 (lcslot-1/lc)	N/A	critical	SAL1928JTKD		N/A	N9K-M6PQ		2018-03-01
candid-leaf1 (ch/psuslot-1/psu)	N/A	critical	DCB1930Y0OR		N/A	N9K-PAC-650W-B		2019-08-30
candid-leaf1 (ch/psuslot-2/psu)	N/A	critical	DCB1930Y0T5		N/A	N9K-PAC-650W-B		2019-08-30
candid-leaf1 (ch/ftslot-1/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf1 (ch/ftslot-2/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf1 (ch/ftslot-3/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf2	healthy	critical	SAL1925HCYK	192.168.1.102	14.2(6g)	N9K-C9396PX		2019-05-01
candid-leaf2 (lcslot-1/lc)	N/A	critical	SAL1928JTMS		N/A	N9K-M6PQ		2018-03-01
candid-leaf2 (ch/psuslot-1/psu)	N/A	critical	DCB1930Y0SU		N/A	N9K-PAC-650W-B		2019-08-30
candid-leaf2 (ch/psuslot-2/psu)	N/A	critical	DCB1930Y0T4		N/A	N9K-PAC-650W-B		2019-08-30
candid-leaf2 (ch/ftslot-1/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf2 (ch/ftslot-2/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf2 (ch/ftslot-3/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf4	healthy	critical	SAL1926HYEH	192.168.1.104	14.2(6g)	N9K-C93128TX		2018-10-30
candid-leaf4 (lcslot-1/lc)	N/A	critical	SAL1924GRV2		N/A	N9K-M6PQ		2018-03-01
candid-leaf4 (ch/ftslot-1/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf4 (ch/ftslot-2/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf4 (ch/ftslot-3/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf5	healthy	critical	SAL1928JTWF	192.168.1.105	14.2(6g)	N9K-C93128TX		2018-10-30
candid-leaf5 (lcslot-1/lc)	N/A	critical	SAL1930KPS2		N/A	N9K-M12PQ		2019-05-01
candid-leaf5 (ch/ftslot-1/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf5 (ch/ftslot-2/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf5 (ch/ftslot-3/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf6	healthy	critical	SAL1929KEY0	192.168.1.106	14.2(6g)	N9K-C93128TX		2018-10-30
candid-leaf6 (lcslot-1/lc)	N/A	critical	SAL1925H88M		N/A	N9K-M6PQ		2018-03-01
candid-leaf6 (ch/ftslot-1/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf6 (ch/ftslot-2/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-leaf6 (ch/ftslot-3/ft/fan-1)	N/A	critical			N/A	N9K-C9300-FAN2-B		2019-08-30
candid-spine1	healthy	critical	SAL1926J4QB	192.168.1.201	14.2(6g)	N9K-C9336PQ		2020-03-04
candid-spine1 (lcslot-1/lc)	N/A	critical	SAL1926J35E		N/A	N9K-C9336PQ		2020-03-04
candid-spine2	healthy	critical	SAL1927JDB4	192.168.1.202	14.2(6g)	N9K-C9336PQ		2020-03-04
candid-spine2 (lcslot-1/lc)	N/A	critical	SAL1923G62V		N/A	N9K-C9336PQ		2020-03-04

Warning **(EOL between 3 and 9 months from now)**

Node Name	SW Conformance Status	HW Conformance Status	Serial	IP	SW Version	HW Model	SW EOL Date	HW EOL Date

*EOL Date - The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.

Guidelines and Limitations for Export Data

- You can configure up to 10 emails per day for periodic job configurations.
- Before configuring your Kafka Export, you must add the external Kafka IP address as a known route in your Nexus Dashboard cluster configuration.
- The following categories will be included for Anomalies in the Kafka and Email messages: Resources, Environmental, Statistics, Endpoints, Flows, Bugs.
- The following categories will not be included for Anomalies in the Kafka and Email messages: Security, Forwarding, Change Analysis, Compliance, System.
- Export data is not supported for Data Collection Type **Upload File**. See [Upload a File to a Site Group and Configure Assurance Analysis].
- A maximum of 5 exporters for Kafka Export for **Usage** will be supported in addition to the currently supported 5 Kafka exporters for **Alerts and Events**.
- You must provide unique names for each export, and they may not be repeated between Kafka Export for **Alerts and Events** and Kafka Export for **Usage**.
- You can configure separate Kafka Export sessions with each of the options: **Alerts and Events** and **Usage**.

Configure Kafka Exporter for Collection Type - Alerts and Events

Use the following procedure to configure the Kafka exporter:

1. In the **Overview** screen, at the top, choose your Site Group.
2. Click the Actions menu next to it and choose **Configure Site Group** and click the **Export Data** tab.
3. In the **Message Bus Configuration** area, click **Add New** and perform the following tasks.
   a. In the **Add New Message Bus Configuration** page, **Credentials** area, **Site Name** field, select the appropriate site.
   b. In the **IP Address** and **Port** fields, enter the appropriate IP address and port.
   c. In the **Mode** field, select the security mode. The supported modes are **Unsecured**, **Secured SSL** and **SASLPLAIN**. The default value is **Unsecured**.
   d. In the **Collection Type** area, choose **Alerts and Events**.
   e. In the **Collection Settings** area, select the Basic or Advanced mode. The Kafka export details for the anomalies and advisories are displayed.
4. In the **Collection Settings** area for each category, choose the severity level for anomalies and advisories.
5. Click **Save**.

This configuration sends immediate notification when the selected anomalies or advisories occur. To configure an email scheduler, see the procedure Configure Email.

Configure Kafka Exporter for Collection Type - Usage

Use the following procedure to configure the Kafka exporter:

1. In the **Overview** screen, at the top, choose your Site Group.
2. Click the Actions menu next to it and choose **Configure Site Group** and click the **Export Data** tab.
3. In the **Message Bus Configuration** area, click **Add New** and perform the following tasks.
   a. In the **Add New Message Bus Configuration** page, **Credentials** area, **Site Name** field, select the appropriate site.
   b. In the **IP Address** and **Port** fields, enter the appropriate IP address and port.
   c. In the **Mode** field, select the security mode. The supported modes are **Unsecured**, **Secured SSL** and **SASLPLAIN**. The default value is **Unsecured**.
   d. In the **Collection Type** area, choose **Usage**. The default value is **Alerts and Events**. Depending upon the Collection Type you choose, the options displayed in this area will change.
4. In the **Collection Settings** area, under **Data**, the **Category** and **Resources** for the collection settings are displayed.

   By default, the data for CPU, Memory, and Interface Utilization will be collected and exported. You cannot choose to export a subset of these resources.

5. Click **Save**.

The Kafka Export for Usage is enabled.

In the **Configure Site Group** page, in the **Export Data** tab, in the **Message Bus Configuration** area, the details of your export job are listed. Details such as the Site name, IP address/port, Topic Name, Collection Type, and Categories are listed in this area. The status of your Kafka Export displays here as **Enabled** or **Failed**.

Configure Email

Use the following procedure to configure an email scheduler that sends the summary of the data collected from Nexus Dashboard Insights:

1. In the **Overview** screen, at the top, choose your Site Group.
2. Click the Actions menu next to it, choose **Configure Site Group**, and click the **Export Data** tab.
3. In the **Email** area, click **Add New**, and perform the following actions:
   a. In the **General Settings** area, in the **Site Name** field, choose the site name.
   b. In the **Name** field, enter the name.
   c. In the **Email** field, enter the email address. For multiple email addresses, use commas as separators.
   d. In the **Format** field, choose Text or HTML format for email.

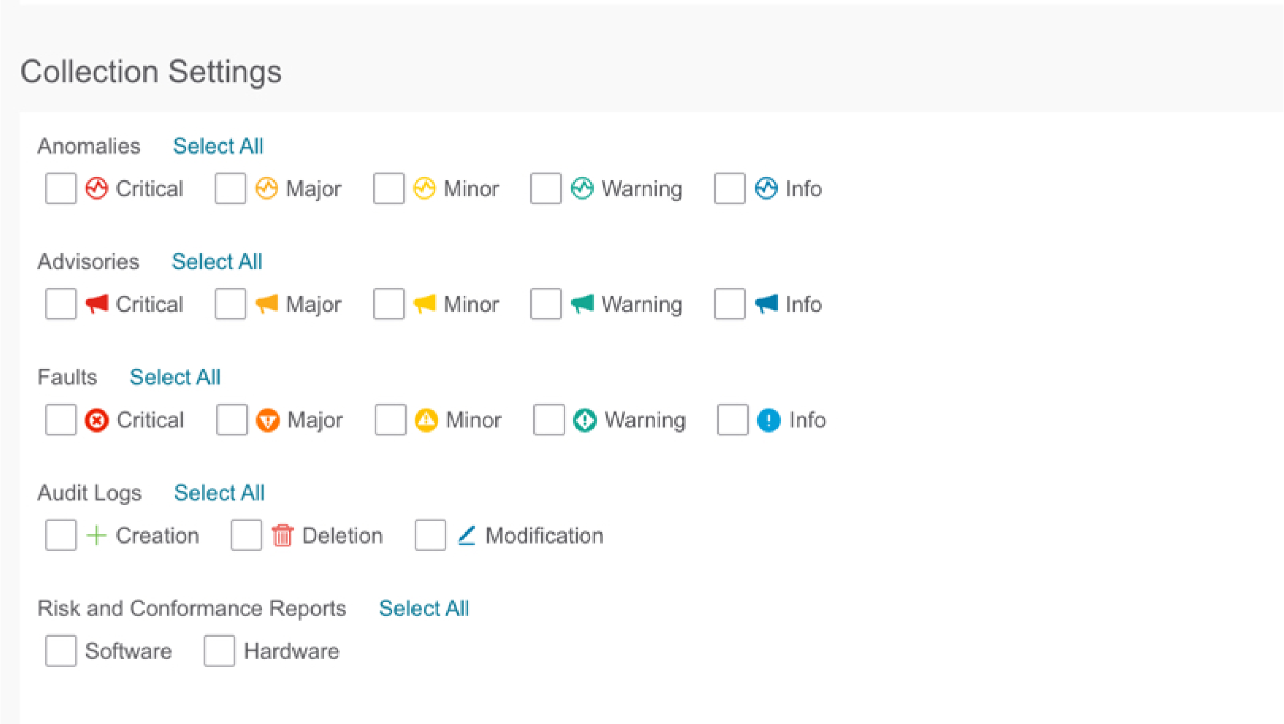
e. In the **Start Date** field, enter the start date.

f. In the **Collect Every** field, specify the frequency in days or weeks.

g. In the **Mode** field, select Basic or Advanced.

In the Basic mode, the severity for anomalies, advisories, and faults are displayed in the **Collection Settings** area. In the Advanced mode, the categories and severity for anomalies and advisories, are displayed in the **Collection Settings** area.

4. In the **Collection Settings** area for each category select the severity level for anomalies, advisories, and faults. Select all that apply. For **Audit Logs** select creation, deletion, and modification options. For **Risk and Conformance Reports**, select **Software** for software release, **Hardware** for hardware platform, and both for combination of software and hardware conformance.



Collection Settings

Anomalies Select All

□ Critical □ Major □ Minor □ Warning □ Info

Advisories Select All

□ Critical □ Major □ Minor □ Warning □ Info

Faults Select All

□ Critical □ Major □ Minor □ Warning □ Info

Audit Logs Select All

□ + Creation □ 🗑 Deletion □ ✎ Modification

Risk and Conformance Reports Select All

□ Software □ Hardware

5. Click **Save**. The configured email schedulers are displayed in the **Email** area.

You will receive an email about the scheduled job on the provided *Start Date* and at the time provided in *Collect Every*. The subsequent emails follow after *Collect Every* frequency expires. If the time provided is in the past, you will receive an email immediately and the next email is triggered after the expiry of the duration from the start time provided.

6. (Optional) In the edit area, perform the following steps:

a. Click ✎ to edit an email scheduler.

b. Click the 🗑 to delete an email scheduler.

Collection Status

In the **Overview** screen, at the top, choose your Site Group. Click the Actions menu next to it and choose **Configure Site Group** and click the **Collection Status** tab.

The summary pane displays the node capabilities and the features supported and unsupported for each node. Nodes from different releases are supported and their specific details by categories such as resources, flows, and endpoints are displayed.

Application Menu

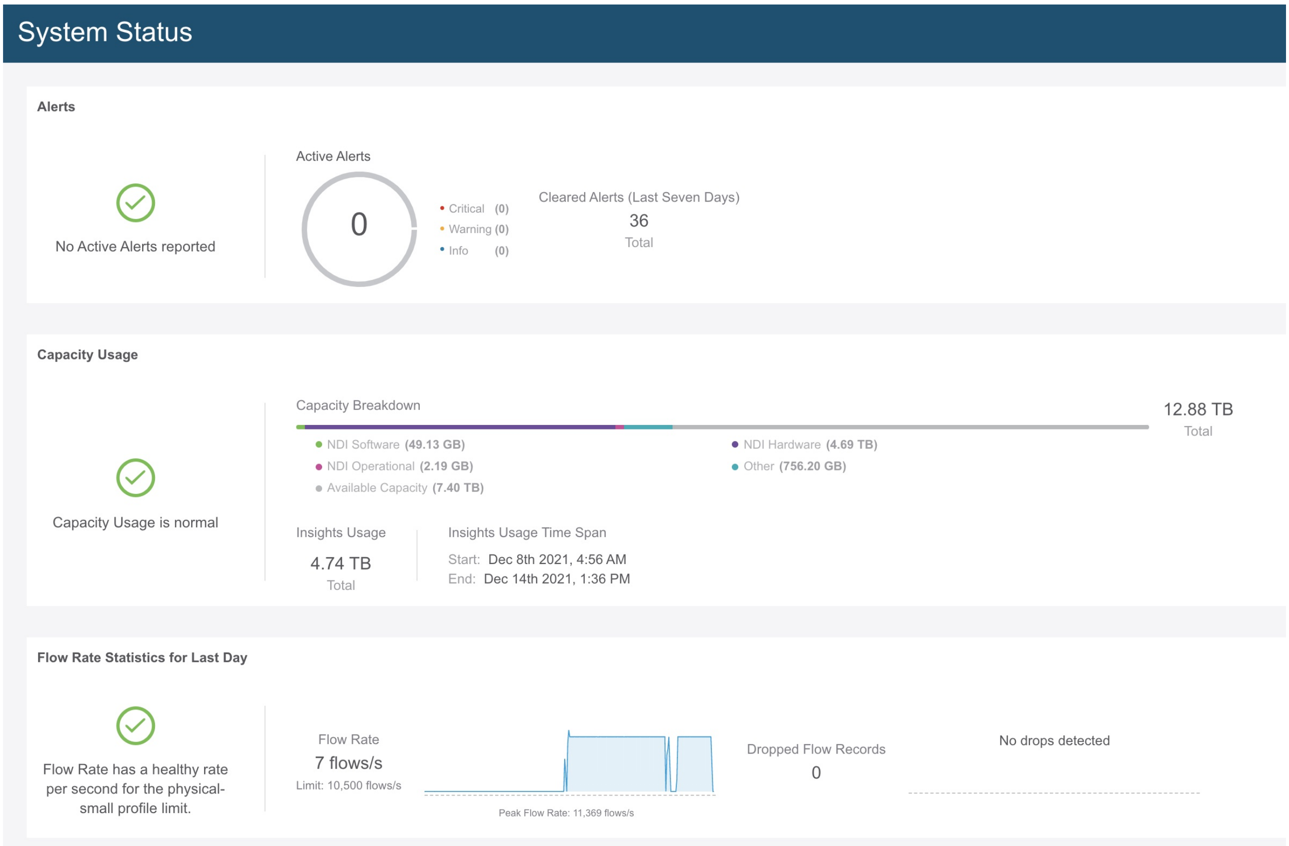
System Status

The System Status page displays Alerts, Capacity Usage, and Flow Rate Statistics for Nexus Dashboard Insights.

Nexus Dashboard Insights gathers resource utilization and shows the utilization, trends, and alerts when thresholds are exceeded or a sudden change from normal behavior is observed.

1. From the Settings icon, click **Application** > **Status**.

   The System Status page displays Alerts, Capacity Usage, and Flow Rate Statistics.

   System Status

   Alerts

   No Active Alerts reported

   Active Alerts

   0

   ● Critical (0)
   ● Warning (0)
   ● Info (0)

   Cleared Alerts (Last Seven Days)
   36
   Total

   Capacity Usage

   Capacity Usage is normal

   Capacity Breakdown

   12.88 TB
   Total

   ● NDI Software (49.13 GB)
   ● NDI Operational (2.19 GB)
   ● Available Capacity (7.40 TB)
   ● NDI Hardware (4.69 TB)
   ● Other (756.20 GB)

   Insights Usage
   4.74 TB
   Total

   Insights Usage Time Span
   Start: Dec 8th 2021, 4:56 AM
   End: Dec 14th 2021, 1:36 PM

   Flow Rate Statistics for Last Day

   Flow Rate has a healthy rate per second for the physical-small profile limit.

   Flow Rate
   7 flows/s
   Limit: 10,500 flows/s

   Peak Flow Rate: 11,369 flows/s

   Dropped Flow Records
   0

   No drops detected

   The Alerts area displays the active and alerts cleared in the last 7 days. The Capacity Usage area displays the capacity usage status, capacity breakdown, and timespan. The Flow Rate Statistics area displays the flow rates and tracks the number of dropped flows.

2. Click **Show All Alerts** to view all the alerts.
3. Use the filter bar to filter the alerts.

Alerts

The alert table lists the alerts raised for Nexus Dashboard Insights with details such as severity set to either warning or critical, status, start and end time, description, and recommendation. Statistics are collected from flow collector and flow correlator. The health container periodically monitors the statistics and raises alerts when it detects abnormalities. The following alerts 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 alert is raised and when the upper threshold is crossed then a critical alert is raised.

  Service Level Thresholds

System Anomalies	Description
Flow Collector Level	The following are flow thresholds: • Lower Threshold—18000 • Global Lower Threshold—54000 • Upper Threshold—20000 • Global Upper Threshold—60000
Flow Correlator Level	The following are flow thresholds: • Lower Threshold—54000 • Upper Threshold—60000

Capacity Usage

The Capacity Usage area displays the capacity usage status, capacity breakdown, and timespan.

Flow Rate Statistics

Nexus Dashboard Insights tracks flow rates per switch in the fabric and tracks the number of dropped flows, and displays the flow rate statistics in the system dashboard. Details such as Flow Rate, Dropped Flow Records, and Nodes Flow Rate are displayed and they apply to Flow Telemetry and Netflow. As a user, you can figure out the incoming flow rate for your specific setup by viewing the incoming pipeline rates for the fabric and at the per-switch level.

The **Flow Rate Statistics** area visually displays the **Flow Rate** and **Dropped Flow Records** as aggregated flow records. The flow rate is the total number of ingested flows to the pipeline that changes depending upon your platform. Based on the flow rate limit, there is a threshold. The visual cues on this page inform you that the system is reaching its maximum rate. The dropped flow records are tracked and they visually display the drops and the unpredictable behavior in the pipeline. Based on this information and after checking the system anomalies, you can adjust the filters to prevent dropped flows. For more details about anomalies, see Analyze Anomalies.

Click **Show More** in the **Flow Rate Statistics** area to expand and display the **Node Flow Rate** and the **Flows** details. In the **Node Flow Rate** area, you can view the scale of flow records per second by each individual node. The **Flows** area displays the flow collection details by individual site. For more details about configuring Flows, see Configure Flows.

Import and Export of Configurations

The import and export of configurations feature enables you import and export the following configurations in Nexus Dashboard Insights:

- Site Groups
  - Sites
  - Flow Settings
  - Microburst
  - Jobs such as analysis, bug scan, best practices
- Alert Rules
- Compliance
- Export Settings
- Flow Rules
- User Preferences

Only an administrator can manage all operations for configuration import and export.

Guidelines and Limitations

- You must be an administrator user to import or export a configuration.
- Site Groups and sites for **Upload File** data collection type are not supported.
- Running more than one import job simultaneously could yield unpredictable results and is not supported. Perform only one import job at a time.
- Importing a configuration appends the existing configuration in Nexus Dashboard Insights.
- The Site Group import process is ignored if the Site Group name is the same in the source and destination.
- Importing a configuration does not affect existing anomalies, and existing assurance analyses.
  - Existing anomalies continue to exist after importing a configuration.
- Host passwords from the imported configurations are not valid and must be re-entered to enable the imported Site Groups configurations to work properly. We recommend that you create a backup configuration by exporting the existing configuration before importing a configuration. The NAT configuration is ignored and not exported with the Site Groups configuration.
- The site must be onboarded on the Cisco Nexus Dashboard instance before importing a Site Group containing that site.
  - Import of site configurations will fail if the site is not present.
  - Import of site configurations will fail if the site name on the Site Group is different from the site name on Cisco Nexus Dashboard.
- Site Group import will fail if any of the sites are in a different Site Group. For example, if you

have a Site Group “IG1” with “Site1” as an existing site, and then you import “IG2” with “Site1”, then the import of IG2 will fail and the configurations for “Site1” will not be updated.

- In this release, import and export of the Site Group is disabled for Export Kafka Data feature using the **Message Bus Configuration** dialog box in the GUI.
- Import and export of configuration is not supported for Multi-cluster Connectivity feature in Nexus Dashboard. Only the configurations local to Nexus Dashboard cluster is exported, and the configurations of remote Nexus Dashboard cluster is not exported.
- Import and export of configurations are not supported for integrations as well as for Template Based Compliance.

Exporting a Configuration

Use the following procedure to export a configuration.

Procedure

1. Choose **Settings** > **Application** > **Import Export Configuration**.
2. Click **New Import/Export**.
3. In the **New Import/Export** page, click **Export**.
4. Click **Start** All the configurations available in Nexus Dashboard Insights are exported. All the existing configurations on the host, which includes, Site Groups, Alert Rules, Compliance, Export Settings, Flow Rules, and User Preferences are exported.
5. The **Import/Export** table displays information of the exported files such as status, type, and content.
6. Click ··· and choose **Download** once the export job status has moved to **Completed**. The exported configuration is downloaded as a compressed file.
7. Click ··· and choose **Delete** to delete the configuration.

Importing a Configuration

Use the following procedure to import a configuration.

Procedure

1. Choose **Settings** > **Application** > **Import Export Configuration**.
2. Click **New Import/Export**.
3. In the **New Import/Export** page, click **Import**.
4. Select the downloaded compressed tar.gz configuration file and click **Start**. The import job details are displayed in the **Import/Export** table.
5. Click ··· and choose **Apply** once the import job status has moved to **Validated**.
6. Select the configurations to import and click **Apply** The **Import/Export** table displays the details of the imported configuration.

When the status of the import job status is `Partially Failed`, some of the configurations would be added and some would be skipped due to failures. To view the reasons for the failure hover the mouse over the status column.

Central Dashboard

Central Dashboard

In Cisco Nexus Dashboard, the **Multi-cluster Connectivity** tab allows you to connect multiple clusters together for a Single Pane of Glass (SPOG) view and administration of the clusters and their sites, services, and configurations. When you add a second cluster, a federation of clusters is formed. The cluster from which you create the federation becomes the "primary" cluster with a number of unique characteristics that do not apply to other clusters in the group.

See Cisco Nexus Dashboard User Guide for information on Multi-cluster Connectivity.

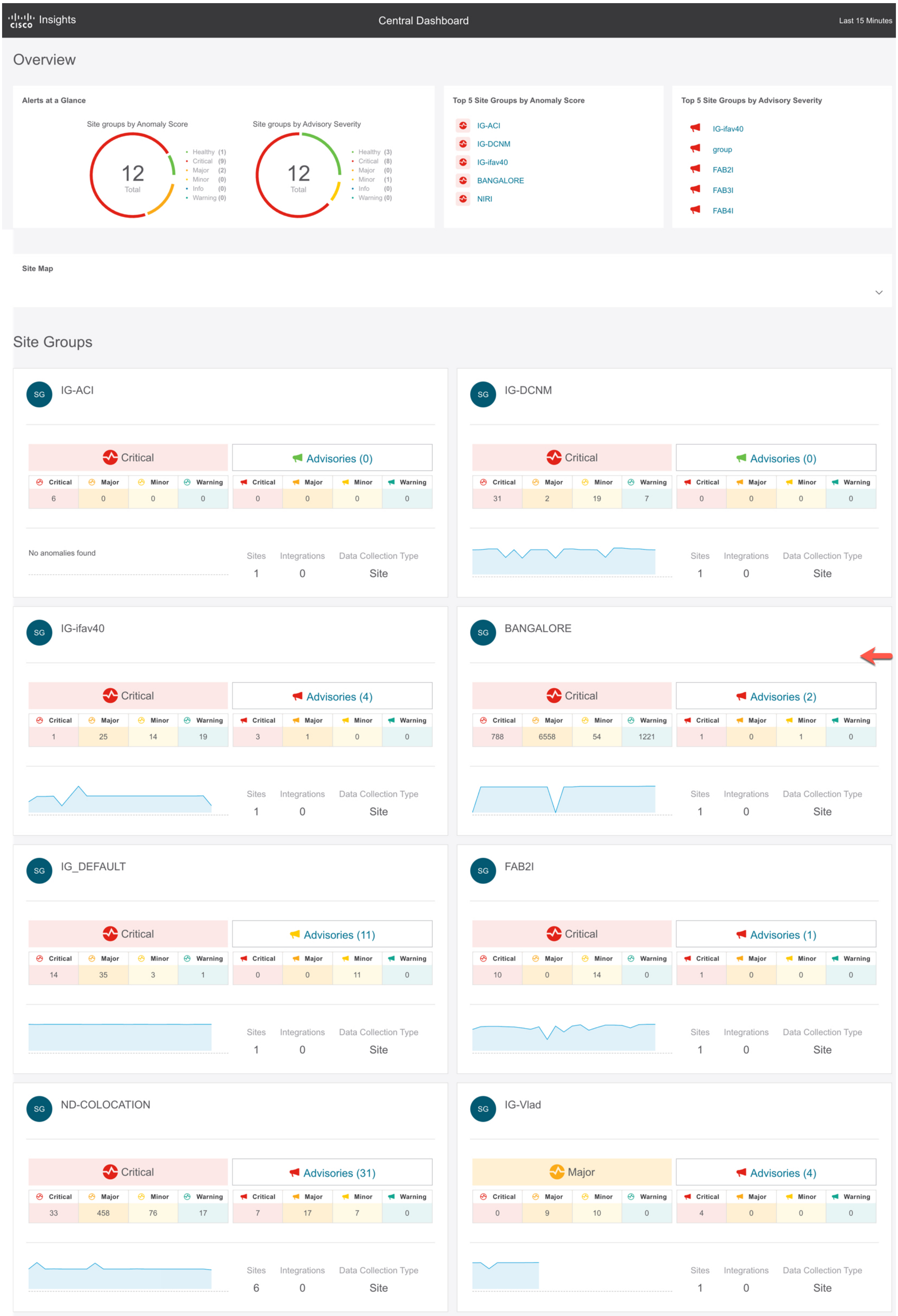
In Cisco Nexus Dashboard, the **Central Dashboard** provides an overview and status of the entire system with all clusters, sites, and services across the entire group of clusters you have created and allows you to quickly find obvious issues, such as connectivity loss to one of the clusters.

After configuring the clusters in Cisco Nexus Dashboard, you can access and perform all operations on the Site Group or site in Cisco Nexus Dashboard Insights. To add a new Site Group see Add a Site Group.

In Cisco Nexus Dashboard Insights, the **Central Dashboard** provides an overview of the Site Groups available in the multi-cluster setup, and the alerts (anomalies and advisories) associated with the Site Groups.

> The site name and Site Group name must be unique in a multi-cluster setup.

1. Click **Central Dashboard** in the top right of Nexus Dashboard Insights page.



Overview

Alerts at a Glance

Site groups by Anomaly Score

12 Total

Healthy	(1)
Critical	(9)
Major	(2)
Minor	(0)
Info	(0)
Warning	(0)

Site groups by Advisory Severity

12 Total

Healthy	(3)
Critical	(8)
Major	(0)
Minor	(1)
Info	(0)
Warning	(0)

Top 5 Site Groups by Anomaly Score

- IG-ACI
- IG-DCNM
- IG-ifav40
- BANGALORE
- NIRI

Top 5 Site Groups by Advisory Severity

- IG-ifav40
- group
- FAB2I
- FAB3I
- FAB4I

Site Map

Site Groups

SG IG-ACI

Critical				Advisories (0)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
6	0	0	0	0	0	0	0

No anomalies found

Sites	Integrations	Data Collection Type
1	0	Site

SG IG-DCNM

Critical				Advisories (0)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
31	2	19	7	0	0	0	0

Sites	Integrations	Data Collection Type
1	0	Site

SG IG-ifav40

Critical				Advisories (4)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
1	25	14	19	3	1	0	0

Sites	Integrations	Data Collection Type
1	0	Site

SG BANGALORE

Critical				Advisories (2)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
788	6558	54	1221	1	0	1	0

Sites	Integrations	Data Collection Type
1	0	Site

SG IG_DEFAULT

Critical				Advisories (11)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
14	35	3	1	0	0	11	0

Sites	Integrations	Data Collection Type
1	0	Site

SG FAB2I

Critical				Advisories (1)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
10	0	14	0	1	0	0	0

Sites	Integrations	Data Collection Type
1	0	Site

SG ND-COLOCATION

Critical				Advisories (31)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
33	458	76	17	7	17	7	0

Sites	Integrations	Data Collection Type
6	0	Site

SG IG-Vlad

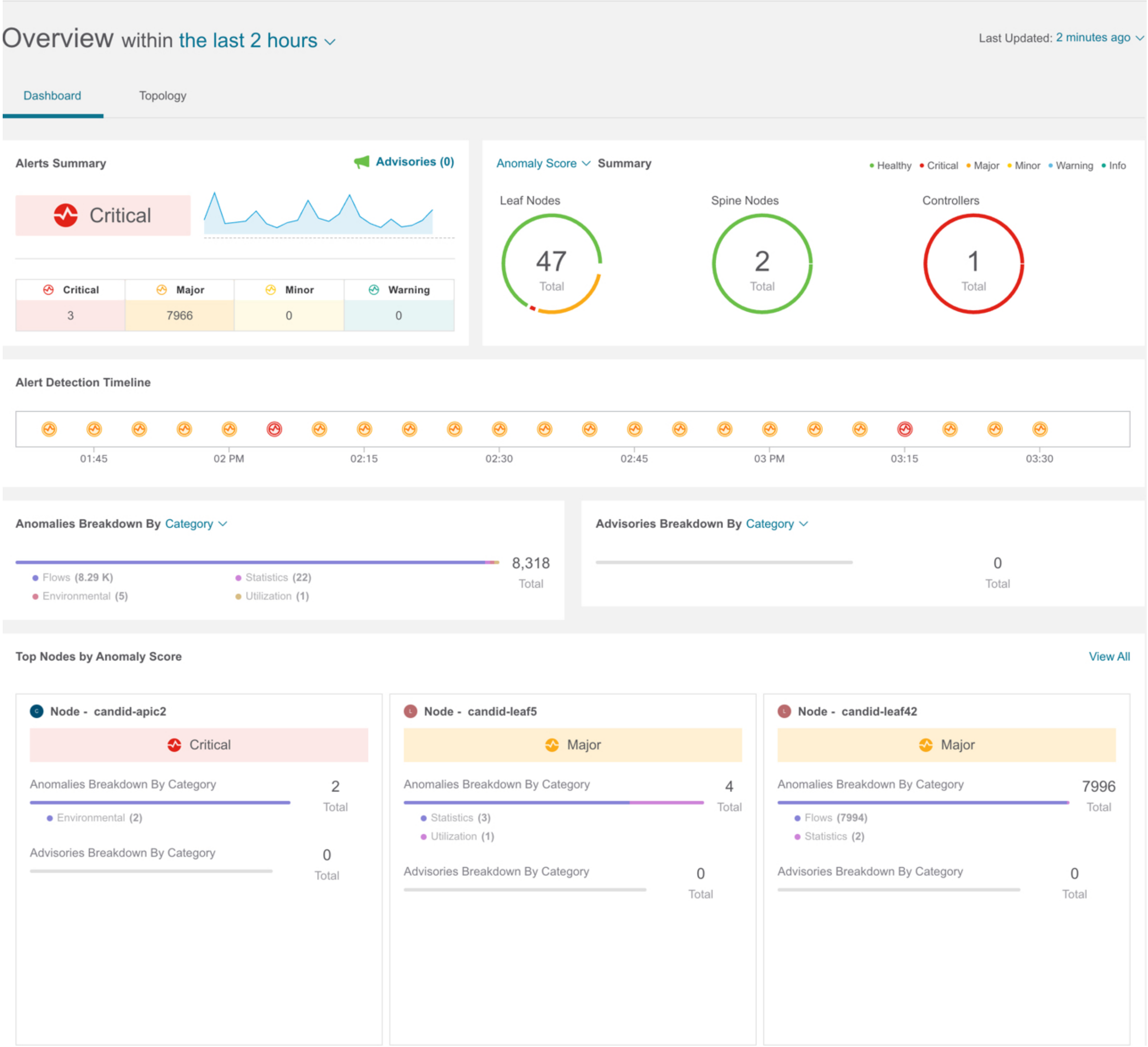
Major				Advisories (4)			
Critical	Major	Minor	Warning	Critical	Major	Minor	Warning
0	9	10	0	4	0	0	0

Sites	Integrations	Data Collection Type
1	0	Site

In the **Central Dashboard**, the Overview area displays the Site Groups by anomaly score and advisory severity and a site map specifies where the sites are located.

The Site Groups area displays information about individual Site Groups such as anomalies and advisories associated with the Site Group, number of sites, integrations, and data collection type.

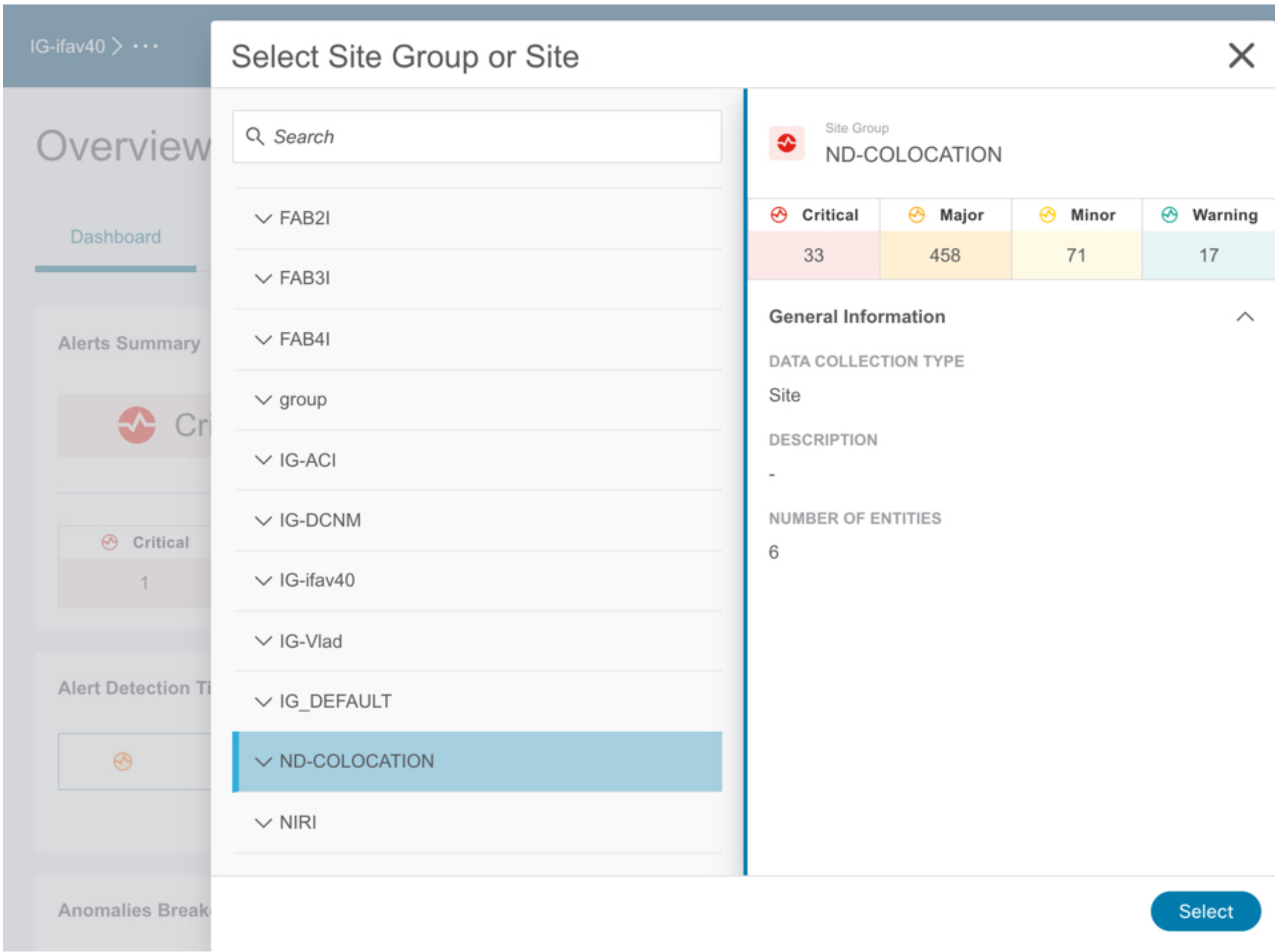
2. In the Overview area, click a Site Group to view specific information about the Site Group in the **Overview** page.



Critical	Major	Minor	Warning
3	7966	0	0

3. In the Site Groups area, click a Site Group to view specific information about the Site Group in the **Overview** page.

4. To navigate between Site Groups or sites in a Site Group, click the Site Group on the top. In the **Select Site Group or Site** dialog box, select the Site Group or site and click **Select**.



Select Site Group or Site

Search

- FAB2I
- FAB3I
- FAB4I
- group
- IG-ACI
- IG-DCNM
- IG-ifav40
- IG-Vlad
- IG_DEFAULT
- ND-COLOCATION
- NIRI

Site Group
ND-COLOCATION

Critical	Major	Minor	Warning
33	458	71	17

General Information

DATA COLLECTION TYPE
Site

DESCRIPTION
-

NUMBER OF ENTITIES
6

Select

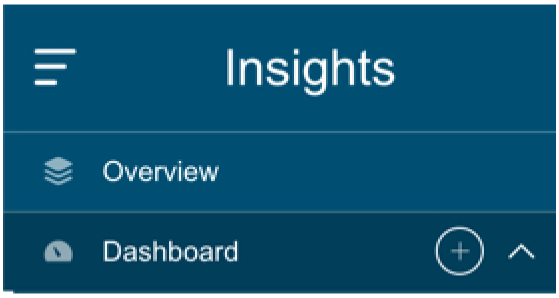
Dashboard

Custom Dashboard

The custom dashboard allows you to create a unique dashboard and add views on to the dashboard. The custom dashboard work pane displays the top level information about each view pinned to the dashboard. There is no limit for number of custom dashboards.

Create a Custom Dashboard

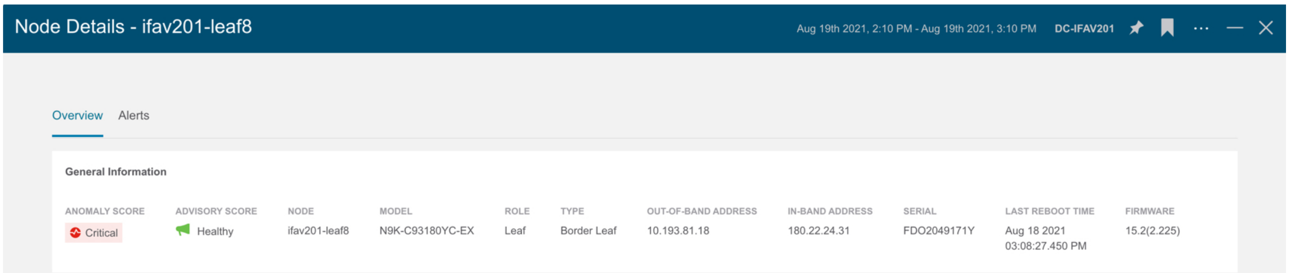
1. Click + icon to create a custom dashboard.



2. Enter a unique name. Click ✓ to save.
3. Select a time range. Click **Apply**.
4. (Optional) Click the edit icon next to the name to edit the name of the custom dashboard.
5. (Optional) Click the delete icon on the right to delete the custom dashboard.

Add Views to a Custom Dashboard

1. Click any category from the left navigation pane such as nodes, resources, flows, or endpoints.
2. Select a particular object and click ↗ to view the detail page.
3. Click the pin icon.



Node Details - ifav201-leaf8

Aug 19th 2021, 2:10 PM - Aug 19th 2021, 3:10 PM DC-IFAV201

General Information

ANOMALY SCORE	ADVISORY SCORE	NODE	MODEL	ROLE	TYPE	OUT-OF-BAND ADDRESS	IN-BAND ADDRESS	SERIAL	LAST REBOOT TIME	FIRMWARE
Critical	Healthy	ifav201-leaf8	N9K-C93180YC-EX	Leaf	Border Leaf	10.193.81.18	180.22.24.31	FDO2049171Y	Aug 18 2021 03:08:27.450 PM	15.2(2.225)

4. In the **Pin to Dashboards** dialog-box, complete the following:
   a. Select a custom dashboard to pin to an existing custom dashboard.
   b. Click **Add Dashboard** to pin to a new custom dashboard. Enter a unique name for the custom dashboard.
5. Click **Save**.

View a Custom Dashboard

1. Choose **Dashboard** > **Custom Dashboard**.
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 a Custom Dashboard

1. Choose **Dashboard** > **Custom Dashboard**.
2. Select any pinned view in the work pane. Click the pin icon to delete or unpin the view from the custom dashboard.

Explore

About Explore for ACI

The **Explore** feature analyzes a policy snapshot from the Cisco APIC to enable data center operators and architects to:

- Explore the ACI object models and associations
- Verify connectivity and segmentation between network assets

The **Explore** feature allows network operators to discover assets and their object associations in an easy-to-consume natural language query format. Operators can quickly get visibility into their infrastructure and connectivity or segmentation between assets. The **Explore** feature allows operators to easily discover associations between traditional networking constructs such as VRFs, EPs, and VLANs to the ACI object model.

The Explore feature is based on a natural language query interface. The types of queries supported by the feature include:

- **What Query**: Answers how the different networking entities are related to each other.

Examples for ACI:

1. What EPGS are associated with VRF: */uni/tn-secure/ctx-secure*
2. What EPs are associated with INF: *topology/pod-1/paths-101/pathep-[eth1/3]* or *VRF:uni/tn-secure/ctx-ctx1*
3. What EPGs are associated with BD: *uni/tn-secure/BD-BD1* and *LEAF: :topology/pod-1/node-103*

- **Can Query**: Answers whether the entities in the ACI policy can communicate with each other. Can queries can also be used to determine if the entities in the ACI policy can communicate using protocols such as TCP, UDP, or ICMP and the source and destination ports used for communication.

Example:

1. Can entity *A* talk to entity *B*.
2. Can EPG: *uni/tn-secure/ap-AP0/epg-B* talk to EPG: *uni/tn-secure/ap-AP0/epg-A* on tcp dport: *80* sport: *10*

- **How Query**: Provides details on the communication between the entities in the ACI policy.

Example: How does EPG *X* talk to EPG *Y*.

- **View Query**: Provides the visual indication of the interface status for any leaf switch in the Site Group.

Example: View interfaces on leaf *X*.

Use Cases

- **Design verification**: Ad-hoc query model enables operators to quickly understand and reason about their infrastructure. The natural language query model returns search results and associations in an easy to understand tabular format. In a single concise view, operators are able to answer design verification questions or discover deviations from organizational best practices.
- **Lightweight book-keeping**: Administration and maintenance teams can provide on demand visibility into the current state of their policy and networking infrastructure allowing inventory, book-keeping, and asset tracking procedures to be lightweight.
- **Connectivity and Segmentation**: Easily answer connectivity questions between a pair of assets or containers of assets. For example, if a group of EPGs needs to be quarantined, the **Can** query can quickly answer if policy has been correctly setup.

Workflow

The **Explore** page provides a consolidated view of all the security, forwarding, and endpoint issues based on the query.

It enables you to explore the connectivity between entities by creating a query. The Can query determines if the entities can communicate with each other and the health of the connectivity. The **How do they talk?** area displays the configuration used for communication between the entities and the health of the connectivity.

In the **Explore** page, you default to the first site in the selected Site Group that is found in the header. Choose the latest snapshot for the site, and generate a model. Assuming the model has enough data, you can then start a query by typing into the input box.

Can Query Results

The results of the Can query are displayed in the **Radial View**. The **Radial View** displays the association view and the connectivity view for a Can query. In the association view, you can use the inner and outer radial bands to explore the associations between the different objects. In the connectivity view, you can use the single radial band to view the prefixes or EPGs as entities.

The **View Controls** enables you to filter the information displayed in the radial view. The EPG view displays connectivity information between different EPGs as configured in the APIC policy. The prefix view displays connectivity information between prefixes as configured in the APIC policy or learnt prefixes. The object view displays the associations between the different objects such as tenants and VRFs. The health view displays the health of the connectivity. The connectivity can be healthy or unhealthy.

The default radial view displays the connectivity and the health of the EPGs.

The different components of the radial view represent different types of information.

- In the **View Controls**, if you select EPGs, Tenants, and Both, the outer ring represents the tenants, the inner ring represents the application profiles, and arced lines in the middle show the health of the contracts.

- In the **View Controls**, if you select EPGs, VRFs, and Both, the outer ring represents the VRFs, the inner ring represents the bridge domains, and arced lines in the middle show the health of the contracts.
- In the **View Controls**, if you select Prefixes and VRFs, and Both, the outer ring represents the VRFs, the inner ring represents the bridge domains or L3Outs, and arced lines in the middle show the health of the contracts.

The colors of the arced lines correspond to the severity of the anomalies. A red line indicates critical anomalies, orange indicates major anomalies, yellow indicates minor anomalies, and green indicates warning and info anomalies.

In **How do they talk?** area in the GUI, the results display in the **Connectivity Table**, **Prefix Table**, and **Anomalies** table.

The connectivity can be healthy or unhealthy. If the connectivity is healthy, using the **Connectivity Table** you can determine the health of the connectivity. If the connectivity is unhealthy, you can use the **Policy**, **Forwarding**, and **Endpoint** tabs to determine the possible cause. The possible causes for unhealthy connectivity include security violations, forwarding violations, and endpoint violations.

The color of the flow between the EPG pair indicates the maximum severity of anomalies across the **Policy**, **Forwarding**, and **Endpoints** tab.

- Red Color indicates critical anomalies
- Orange color indicates major anomalies
- Yellow color indicates minor anomalies
- Green color indicates warning and info anomalies

For example if the issues are related to security violations, you can use the **Connectivity Table**, **Prefix Table**, and **Anomalies** table to determine the anomalies associated with the security issue. In the **Prefix Table**, you can click **Subnet/Route** to see information regarding the prefixes. In the **Anomalies** table you can click the anomaly to determine the objects in your fabric that are affected by the issue, the Pass or Fail checks performed on the anomaly and suggested steps to resolve the issue.

For more details, see Creating a Can Query and Viewing the How Do They Talk? Area.

Guidelines and Limitations

- In the **Explore** page, four active snapshots to explore across all sites is supported. The snapshots can be used for exploration by either the same user or by multiple users. To explore additional snapshots, you must offload an existing snapshot before exploring. In the **Offload Snapshot From Explore** page you can select the snapshots to offload. This dialog box displays automatically when you load 4 snapshots in memory.
- The Explore feature is supported only for IPv4 prefixes.
- All queries created using the Explore feature are unidirectional.

- In the **Explore** page, if the analysis fails, the error message *Analysis has failed* is displayed. Download the tech support logs for **Explore** and contact Cisco TAC to resolve the issue.
    a. In Cisco Nexus Dashboard, choose **Operations** > **Tech Support** and choose **Actions** > **Collect Tech Support** > and choose the appropriate service for Cisco Nexus Dashboard Insights to download the tech support logs.
    b. Navigate to */data/services/app_logs/cisco-nir-logger/nae/nae/explorerService/* directory to locate the logs for the Explore feature. If there are multiple Explore instances running, the logs for each instance is located in a separate directory.

```
nae-policyexplorer-0/explorer.log
nae-policyexplorer-1/explorer.lo
nae-policyexplorer-2/explorer.log
nae-policyexplorer-3/explorer.log
```

- Prefixes configured under L3extSubnet without their learnt route will not be listed as part of the auto-suggestions when you enter a query in the Search bar.
- To explore the APIC resources successfully using the Explore feature, the APIC policy must contain either valid endpoints such as fv:CEp or valid EPGs.
- In the **Compliance** page, the policy intent based on contracts is used to determine the compliance.
- **Explore** has the following scale limits:
    - On virtual Nexus Dashboard we support snapshots with 100,000 logical rules and 350,000 (Vertices + Edges).
    - On physical Nexus Dashboard we support snapshots with 300,000 logical rules and 1000,000 (Vertices + Edges).

Creating a What Query

Use this procedure to create a What query using the Explore feature. This query helps answer the question, "What entities are associated with each other?""

Procedure

1. In the **Overview** page, choose the appropriate Site Group > Site.
2. In the left Navigation, click the **Explore** tab.
3. In the **Timeline** select a snapshot for analysis. When you select a snapshot, the data to explore is loaded on demand.
4. Generate a model and when there is enough data, you will be able to type in a query in the input field.
    a. In the query selector field, enter a **What** query. The query must include two groups of one or more entities available in the **Search** bar. See Supported Queries. By default, **What** endpoints are associated with the Any query view.

The Query results are displayed on the page, and you can drill further to see the associated entities. You can add to the source and destination list. (Can source talk to destination?)

In the **What entities can talk?** area, the radial is displayed with **View Controls** for additional filtering. Click inside the radial to get more information as required. Click an entity in the **Query Results** table to view details. Click a number in the results table to view details about the entity in the ACI policy.

See Analyze Alerts for details about anomalies and alerts.

Creating a Can Query and Viewing the How Do They Talk? Area

Use this procedure to create a query using the Explore feature. The can query will provide information that answers the question, can two entities communicate with each other?

Procedure

1. In the **Overview** page, choose the appropriate Site Group > Site.
2. In the left Navigation, click the **Explore** tab.
3. In the **Timeline** select a snapshot for analysis. When you select a snapshot, the data to explore is loaded on demand.
4. Generate a model and when there is enough data, perform the following actions.
    a. In the query selector field, enter a **Can** query. The query must include two groups of one or more entities from the ACI policy. For details, see Supported Queries.

> ℹ An automatic check is performed to see if the source entity can talk to the destination entity. You can click **Reverse Query** to reverse the source and destination entities for a query.

b. Use **View Controls** to choose different entities for more information.

A radial is rendered. You can drill down in the radial and get more detailed information as required. Below the radial, the **How do they talk?** area displays how the two entities communicate with each other. Related Policy, Forwarding, and Endpoint information is displayed in a table with associated anomalies

The color of the flow indicates the maximum severity of anomalies across the **Policy**, **Forwarding**, and **Endpoints** tab. The color of the icon in each tab indicates the individual severity of the anomalies included in the corresponding tab.

- Red color indicates critical anomalies
- Orange color indicates major anomalies
- Yellow color indicates minor anomalies
- Green color indicates warning and info events

- The **Policy** tab enables you to explore the security policy issues based on the query.
- The **Forwarding** tab enables you explore a prefix or pair of prefixes issues based on the query.
- The **Endpoints** tab allows you to explore the endpoint issues based on the query.

If the query results are large, the message “The query returned too much data to display” is displayed. Use the **View Controls** > **Advanced** > **From EPG** and **To EPG** Search bar to create a more specific query for the results to be displayed.

Can queries containing large associations such as vzAny may timeout. Use the **View Controls** > **Advanced** > **From EPG** and **To EPG** Search bar to create a more specific query.

For a query between prefixes, if the number of EPGs shared by the prefixes is greater than 25, the Endpoint table fails to load the data and displays an error message. Create an EPG to EPG query to display the results in the Endpoint table.

See Workflow for more details about the **Can** query and the **How do they talk?** area. See Viewing View Query Results for information about query results. See Analyze Alerts for details about anomalies and alerts.

Viewing View Query Results

A **View** query must include two groups of one or more entities from the ACI policy. See Supported Queries.

This is an example of how to perform an interface query that allows to view a specific interface on a leaf switch. The **Interface** page displays the physical interface health and provides the visual indication of the interface status for any leaf switch in the site based on the query. The **Interface** area displays information about one leaf switch at a time.

Procedure

1. In **Overview** page, choose the appropriate Site Group > Site.
2. In the left Navigation, click the **Explore** tab.
3. In the **Timeline** select a snapshot for analysis. When you select a snapshot, a model for your policy inspection is generated.
4. In the query selector field, type **View**, and choose the interface you want to view.
5. Toggle the appropriate options in **View Control** to filter the information you need, and the options in the **Anomalies** table will update.

A physical representation of the leaf allows you to toggle the different views to see the configurations and see the related anomalies below. You can drill further into the anomalies for more details. You can view anomalies by individual or aggregate data as desired. If an endpoint is attached to a particular interface, an image of the leaf switch is displayed as a two-dimensional image. The switch ports are color coded to display the status for each port. The color for each port matches its anomaly severity by color. Click one of the switch ports in the switch image, to view the details of the anomaly associated with that port, in the **Anomalies** table.

Some options that you can toggle in the **View Controls** area:

In the **Interface Usage** area, the interfaces are classified by their usage status:name: value

- Configured Interfaces: This interface is made available by the Site Group policy, and it is ready for use by the EPGs.
- Partially Configured Interfaces: This interface is available to be allocated for consumption by EPGs, and it is either in an unconfigured or a partially configured state.
- Used Interfaces: This interface is allocated by the Site Group policy, and it is consumed by the EPGs.

> ℹ The **Used Interfaces** tab is selected by default.

Under **Interface Operational Status**, the interfaces are classified by their operational status:

- Oper Down: This interface is operationally down due to issues such as link failure, error disabled, suspended state.
- Oper Up: This interface is operational with no known issues.
- Admin Down: The operator has administratively shut down this interface.

> ℹ Under **Interface Operational Status**, the tabs **Oper Down**, **Oper Up**, and **Admin Down** are selected by default.

See Analyze Alerts for details about anomalies and alerts.

Supported Queries

The following table lists the queries supported by the **Explore** feature for ACI.

Supported What Queries

Table 3. Supported What Queries

Query	Entity	Operator	Entity
What BDs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
What ENCAPs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
What EPGs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF

Query	Entity	Operator	Entity
What EPs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
What INFs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
What Inventory is associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF

Query	Entity	Operator	Entity
What Leafs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF
What VRFs are associated with	• ? • Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF	• And • Or	• Any • Any? • BD • ENCAP • EP • EPG • INF • LEAF • VRF

Supported Can Queries

Table 4. Supported Can Queries

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can BD `bd_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port
Can ENCAP `encap_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port
Can EP `ep_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can EPG `epg_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port
Can INF `inf_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port
Can LEAF `leaf_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can VRF `vrf_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port
Can Subnet `subnet_name` talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • Subnet • ANY*	On	• TCP • UDP • ICMP	• Port Number • Port Range • Well-known Port	• Port Number • Port Range • Well-known Port
Can ANY talk to	• BD • ENCAP • EP • EPG • INF • LEAF • VRF • ANY	—	—	—	—

The **Operator**, **Protocol**, **Destination Port**, and **Source Port** are not supported in CAN queries for these ANY entities.

Table 5. Supported View Queries

Query	Entity
View interfaces on	Leaf `leaf_name`

Nodes

Nodes

The *Nodes* pane displays the comparison chart with top nodes based on Resource Utilization, Environmental, Statistics, Endpoints, and Flows, which are various ways of viewing the behavior of the nodes. Based on the chosen top nodes by category, the summary pane displays the nodes with their anomaly score, firmware, serial, model, and type.

- Click the *Node* from the summary pane to display all the gathered information for the selected node.

  The *Node Overview* section displays the top five resources in each Nexus Dashboard Insights-Resource Utilization, Environmental, Statistics, Flows, Events, and Endpoints with the break down of the faults and events. The *Anomalies* section displays the anomalies that the system detects.

- Click the ⧉ on the right top corner of the summary pane to show the Node Details page.
- Click the **Overview** tab.

The Node Details page on the *Overview* tab displays General Information, Node Overview, and Anomalies. The *Node Overview* section displays the top five resources in Cisco Nexus Dashboard Insights-Resource Utilization, Environmental, Statistics, and Flows 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, Endpoints, Events, and Environmental Resources for the node.
- Click a category from the list to open browse work pane for that particular node.

The *Alerts* tab on the Node Details page displays the anomalies occurred on the nodes for the chosen top nodes by category.

- Click on the anomaly in the Node Details page to open the side pane with general details of the anomaly.
- Click **Analyze** for the anomaly details page to display the Lifespan, estimated impact, recommendations, mutual occurrences, and in-depth analysis of the anomaly.
- Hover over the anomalies, faults, events in the mutual occurrences graph. Click on them for detailed analysis of mutual occurrences of the anomaly.

Analyze Alerts

Analyze Alerts

Analyze Alerts provides a view into Anomalies and Advisories generated by Nexus Dashboard Insights. Nexus Dashboard Insights can proactively detect different types of anomalies throughout the network, root cause the anomalies, and identify remediation methods.

- The Anomalies Dashboard consists of anomalies raised for resource utilization, environmental issues, interface and routing protocol issues, flows, endpoints, events, assurance analysis, compliance, change analysis, and static analysis.
- The Advisories Dashboard consists of relevant impact due to field notice, EOL/EOS of software and hardware, PSIRTs at a node level and compliance.

PSIRTs are Product Security Incident Response Team notices that display three levels of advisory severity for node hardware and software in your network. It categorizes by severity and identifies software versions and hardware platforms to which the advisories apply.

Anomalies

The Anomalies Dashboard displays the graph with top nodes by anomaly score based on Type and Severity for a particular Site Group or site and based on the time range selected by the user.

The filter bar allows you to filters the anomalies. See Anomaly Filters for more information.

The page also displays individual or aggregated views of the anomalies in a tabular format.

- The individual view displays the individual anomalies raised for the site with details such severity, status, category, affected nodes, detection time, title, description, and user state.
- The aggregated view displays the aggregated views of the anomalies based on the anomaly title and displays the anomaly count for each title.

The Nexus Dashboard Insights uses the enhanced framework and workflow mappings on Cisco APIC and Cisco DCNM to recommend the enhanced anomaly diagnostics and impact. The Estimated Impact and Recommendations area in the Analyze Anomaly page describe the anomaly diagnostics impact and recommendations. To view more details about an individual anomaly see Analyze Anomalies.

You can configure the following properties on an anomaly.

- Assign an user
- Add tags
- Add a comment
- Set verification status
- Acknowledge an anomaly so that the acknowledged anomalies are not displayed in the Anomalies Table. To configure properties on an anomaly see Configuring Anomaly Properties.

You can acknowledge anomalies in the following ways:

- Manually acknowledge an anomaly. See Configuring Anomaly Properties.
- Manually acknowledge multiple anomalies. Configuring Anomaly Properties.
- Use alert rules to automatically acknowledge anomalies matching alert rules. See Creating Alert Rules.

Anomaly Filters

In the **Anomalies Dashboard**, you can use the following filters to refine the displayed anomalies:

- Acknowledgement - Display only anomalies with acknowledged status.
- Active - Display only anomalies with active status.
- Anomaly ID - Display only anomalies with a specified anomaly ID.
- Assignee - Display only anomalies assigned to a specified user.
- Category - Display only anomalies from a specific category.
- Comment - Display only anomalies with a specified comment.
- Description - Display only anomalies with a specified description.
- Detection Time - Display only anomalies with a specific detection time.
- Entity Name - Display only anomalies with a specified name.
- Last Seen Time - Display only anomalies with a specific time.
- Nodes - Display only anomalies for nodes.
- Severity - Display only anomalies of a specific severity.
- Sub-category - Display only anomalies from a specific sub-category.
- Tags - Display only anomalies with a specified tag.
- Title - Display only anomalies with a specified title.
- Verification status - Display only anomalies of a specific verification status.

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.

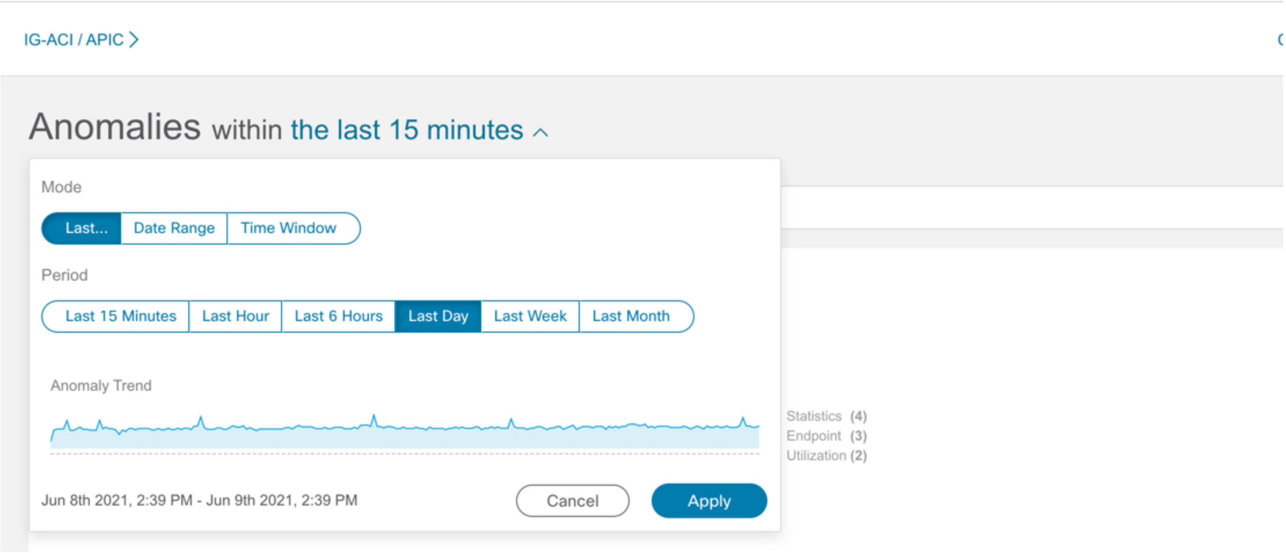
> - with the initial filter type, this operator, and a subsequent value, returns a match greater than the value.

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

Analyze Anomalies

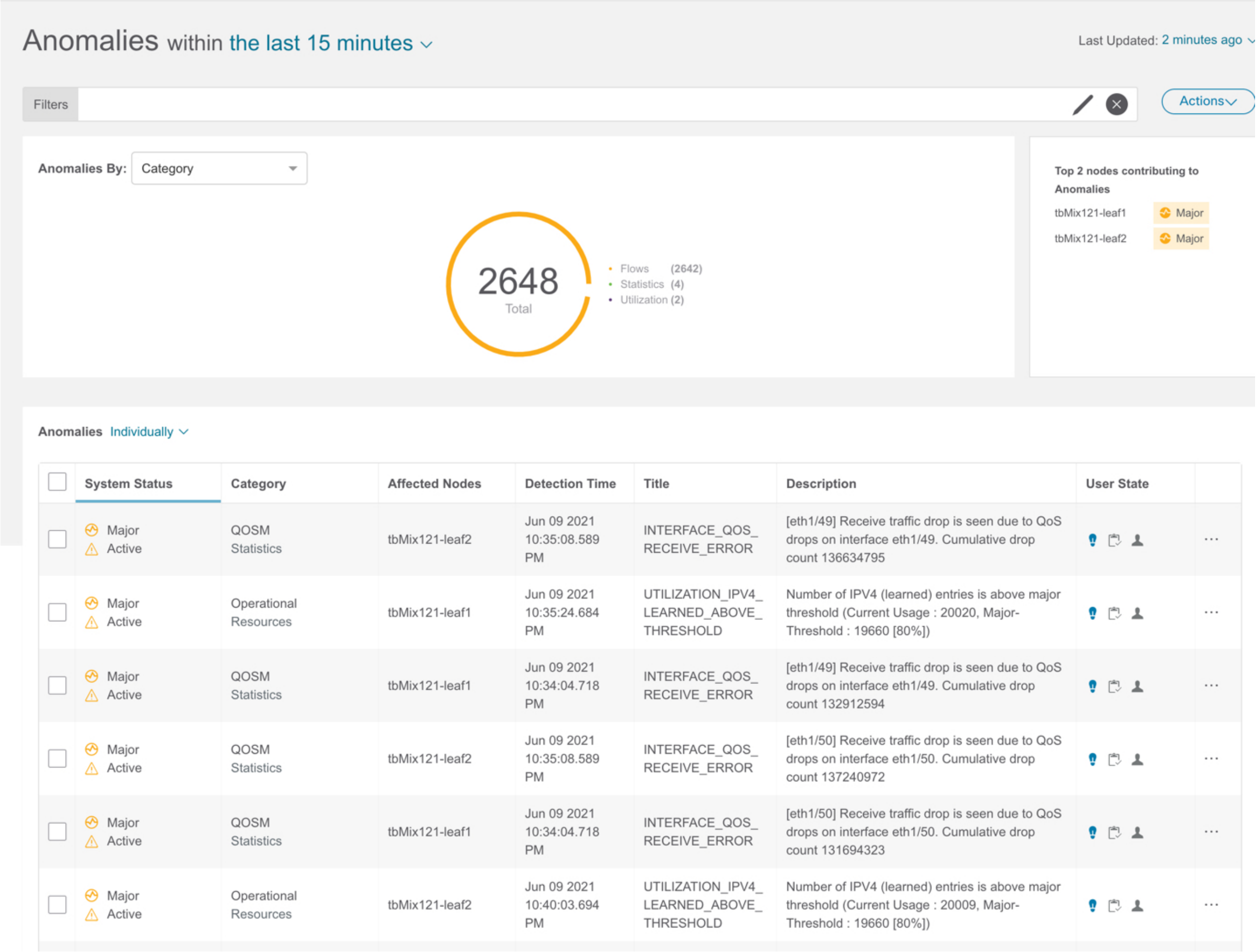
Use this procedure to analyze anomalies.

1. Choose **Analyze Alerts** > **Anomalies**.
2. In the **Anomalies** Dashboard, select a Site Group or site from the Site Group menu.
3. Select a time range from the drop-down menu.



In the time range, select at least **last 2 Hours** to view all the anomalies for the selected site.

The **Anomalies** table displays individual or aggregated anomalies based on the selected site and time range. The anomalies are sorted by System Status by default. The anomaly status include Active and Cleared. An active state indicates that the anomalous condition is present on your network. A cleared state indicates that the anomalous condition is not present on your network anymore and therefore the anomaly has been marked cleared.



Anomalies within the last 15 minutes

Last Updated: 2 minutes ago

Anomalies By: Category

2648 Total

- Flows (2642)
- Statistics (4)
- Utilization (2)

Top 2 nodes contributing to Anomalies

tbMix121-leaf1	Major
tbMix121-leaf2	Major

Anomalies Individually

□	System Status	Category	Affected Nodes	Detection Time	Title	Description	User State
□	Major Active	QOSM Statistics	tbMix121-leaf2	Jun 09 2021 10:35:08.589 PM	INTERFACE_QOS_RECEIVE_ERROR	[eth1/49] Receive traffic drop is seen due to QoS drops on interface eth1/49. Cumulative drop count 136634795	
□	Major Active	Operational Resources	tbMix121-leaf1	Jun 09 2021 10:35:24.684 PM	UTILIZATION_IPV4_LEARNED_ABOVE_THRESHOLD	Number of IPV4 (learned) entries is above major threshold (Current Usage : 20020, Major-Threshold : 19660 [80%])	
□	Major Active	QOSM Statistics	tbMix121-leaf1	Jun 09 2021 10:34:04.718 PM	INTERFACE_QOS_RECEIVE_ERROR	[eth1/49] Receive traffic drop is seen due to QoS drops on interface eth1/49. Cumulative drop count 132912594	
□	Major Active	QOSM Statistics	tbMix121-leaf2	Jun 09 2021 10:35:08.589 PM	INTERFACE_QOS_RECEIVE_ERROR	[eth1/50] Receive traffic drop is seen due to QoS drops on interface eth1/50. Cumulative drop count 137240972	
□	Major Active	QOSM Statistics	tbMix121-leaf1	Jun 09 2021 10:34:04.718 PM	INTERFACE_QOS_RECEIVE_ERROR	[eth1/50] Receive traffic drop is seen due to QoS drops on interface eth1/50. Cumulative drop count 131694323	
□	Major Active	Operational Resources	tbMix121-leaf2	Jun 09 2021 10:40:03.694 PM	UTILIZATION_IPV4_LEARNED_ABOVE_THRESHOLD	Number of IPV4 (learned) entries is above major threshold (Current Usage : 20009, Major-Threshold : 19660 [80%])	

4. Choose one of the following:

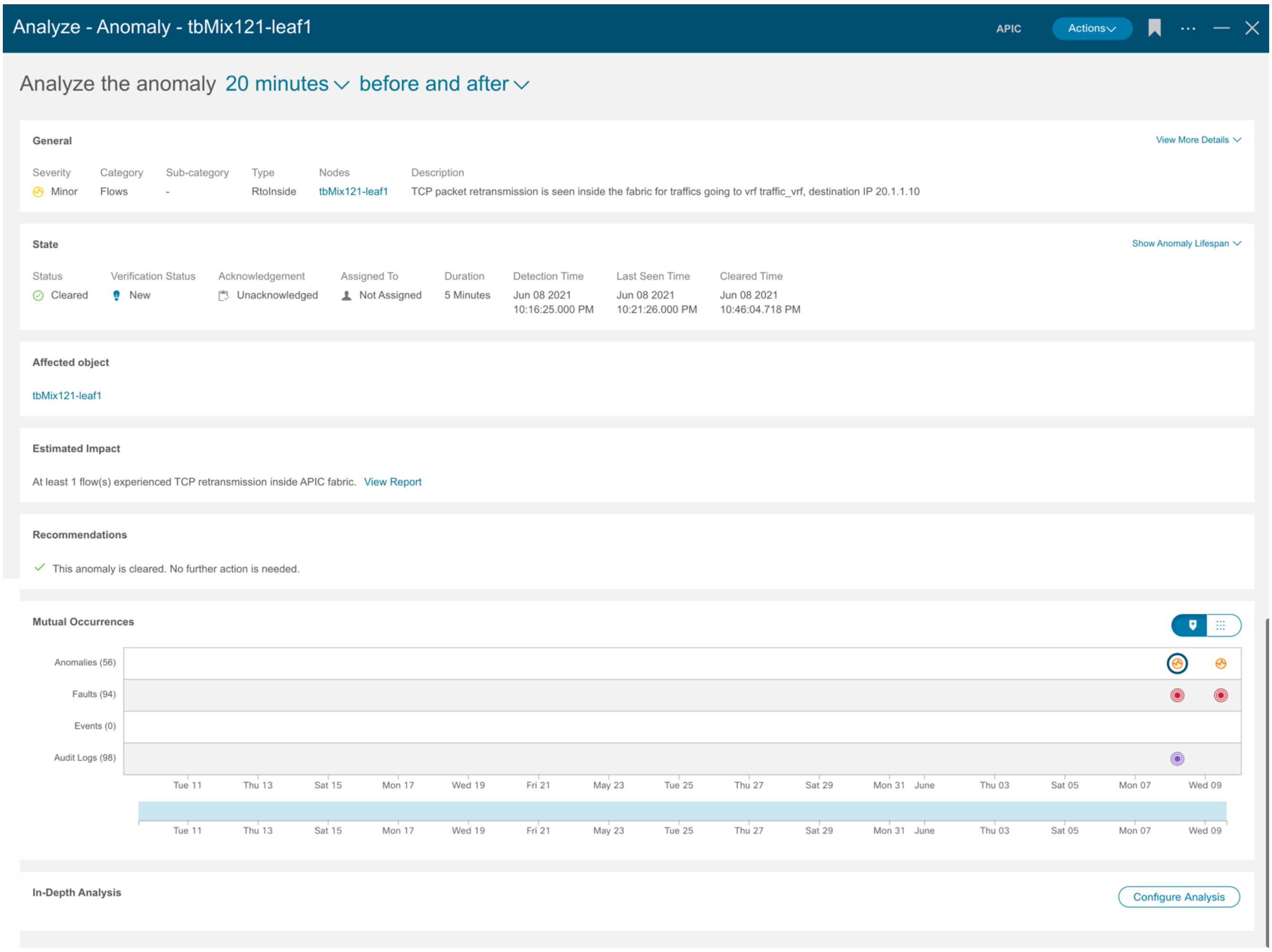
    a. Select **Individual** from the Anomalies drop-down list to view individual anomalies.

    b. Select **Aggregated** from the Anomalies drop-down list to view aggregated anomalies based on title.

5. Use the filter icon in each column to sort the anomalies. Filtering is not supported for the column **Affected Nodes**.

6. Click the anomaly in the **Anomalies** table for the side pane to display additional details about the anomaly. In the aggregated view, the side pane displays the list of individual anomalies. Click an anomaly to display additional details about the individual anomaly.

7. Click **Analyze**. The **Analyze Anomaly** page displays the general information of the anomaly, state, affected object, life span, estimated impact, recommendations, mutual occurrences, and in-depth analysis.



Analyze - Anomaly - tbMix121-leaf1

Analyze the anomaly 20 minutes before and after

General

View More Details

Severity	Category	Sub-category	Type	Nodes	Description
Minor	Flows	-	RtoInside	tbMix121-leaf1	TCP packet retransmission is seen inside the fabric for traffics going to vrf traffic_vrf, destination IP 20.1.1.10

State

Show Anomaly Lifespan

Status	Verification Status	Acknowledgement	Assigned To	Duration	Detection Time	Last Seen Time	Cleared Time
Cleared	New	Unacknowledged	Not Assigned	5 Minutes	Jun 08 2021 10:16:25.000 PM	Jun 08 2021 10:21:26.000 PM	Jun 08 2021 10:46:04.718 PM

Affected object

tbMix121-leaf1

Estimated Impact

At least 1 flow(s) experienced TCP retransmission inside APIC fabric. View Report

Recommendations

✓ This anomaly is cleared. No further action is needed.

Mutual Occurrences

In-Depth Analysis

Configure Analysis

a. In the **General** area, click nodes to view additional details.

b. The **State** area, displays the detection time and cleared time.

c. In the **Affected Object** area, click affected objects to view additional details.

d. In the **Estimated Impact** area, click **View Report** to view the details of the entities that were affected.

e. In the **Mutual Occurrences** area, hover over the anomalies, faults, and events. Click on them for detailed analysis of mutual occurrences of the anomaly.

f. Click **Configure Analysis** to analyze anomalies on nodes with a customizable graph.

   i. On the Object Selection Table, click **Add Objects**.

   ii. On the Chart Selection Table, select **Chart Type** and then select **Chart Name** from the drop-down list.

   iii. 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.

8. Click the ellipses ••• icon located on the top right of the page. Select a node from the list to open browse work pane for that particular node.

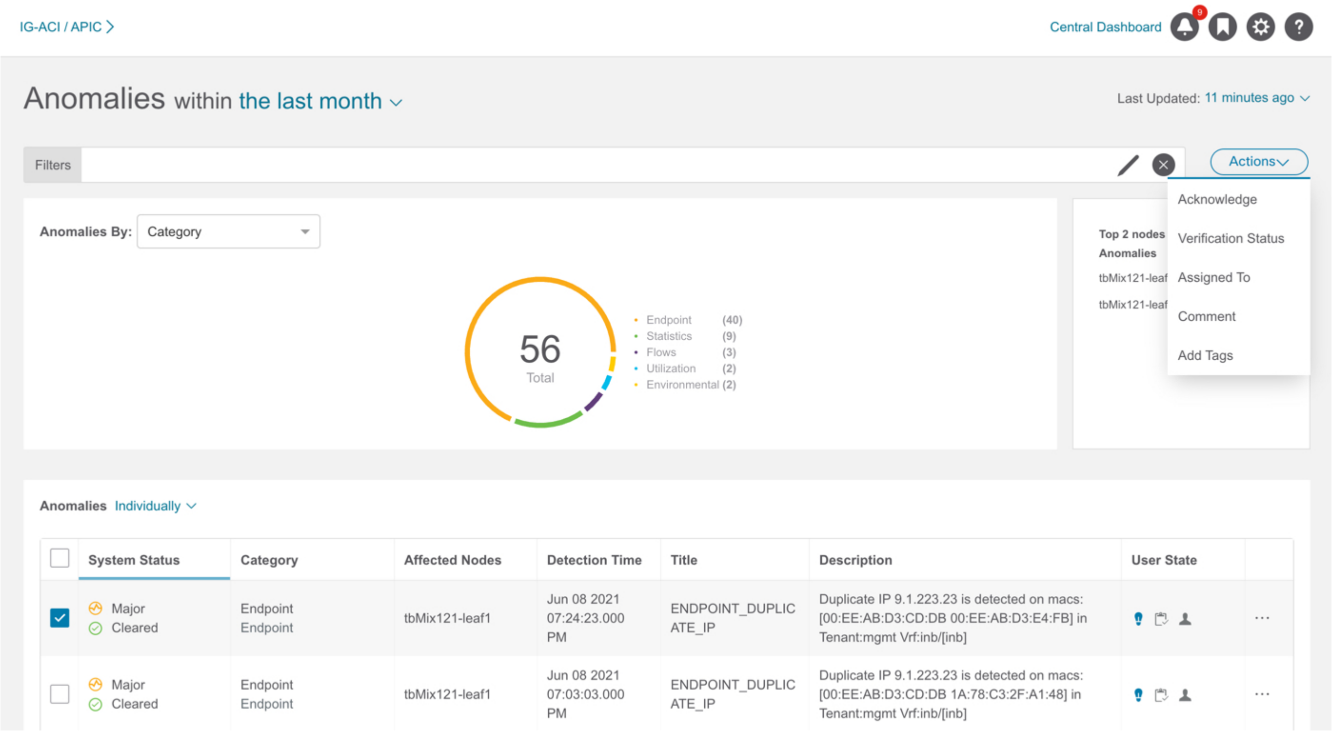
9. Click the icon to bookmark the page.

10. Click **Done**.

Configuring Anomaly Properties

Use the following procedure to configure properties on an anomaly.

1. Choose **Analyze Alerts** > **Anomalies**.
2. In the **Anomalies** Dashboard, select a Site Group or site from the Site Group menu.
3. Select a time range from the drop-down menu. The anomalies table displays individual or aggregated anomalies based on the selected site and time range.
4. Select **Individual** from the Anomalies drop-down list.
5. Select anomalies from the table and then select a property from the **Actions** menu.



□	System Status	Category	Affected Nodes	Detection Time	Title	Description	User State	
☑	Major Cleared	Endpoint Endpoint	tbMix121-leaf1	Jun 08 2021 07:24:23.000 PM	ENDPOINT_DUPLICATE_IP	Duplicate IP 9.1.223.23 is detected on macs: [00:EE:AB:D3:CD:DB 00:EE:AB:D3:E4:FB] in Tenant:mgmt Vrf:inb/[inb]		...
□	Major Cleared	Endpoint Endpoint	tbMix121-leaf1	Jun 08 2021 07:03:03.000 PM	ENDPOINT_DUPLICATE_IP	Duplicate IP 9.1.223.23 is detected on macs: [00:EE:AB:D3:CD:DB 1A:78:C3:2F:A1:48] in Tenant:mgmt Vrf:inb/[inb]		...

a. Select **Acknowledge** to manually acknowledge an anomaly. When you acknowledge an anomaly, it is not displayed in the **Anomaly Table**. To view the anomaly in the **Anomalies** table use the Acknowledgement=true filter.

> The default filter is Acknowledgement=false. The Acknowledgement=false filter is not applied when you select **Aggregated** from the anomalies drop-down list. It is applied when you select **Individually** from the anomalies drop-down list.

b. Select **Verification Status** to set a user defined status such a New, In Progress, or Closed to an anomaly. Click **Save**.

c. Select **Assigned To** to assign an anomaly to an user. Enter the username and click **Save**.

d. Select **Comment** to assign a comment to an anomaly. Enter a comment and click **Save**.

e. Select **Add Tags** to add user-defined tags to an anomaly. Enter the tag name and click **Save**. You can enter multiple tags. After entering the tag name, press Enter.

6. To configure a property on an individual anomaly, select an anomaly. Click the ⋯ icon and then choose a property from the drop-down list.
7. In the **Anomalies** table, the properties assigned to an anomaly are displayed in the User State column.

NOTE:

- When you configure properties on anomalies using the **Actions** menu, it will override any of the properties you have configured on an individual anomaly using the ⋯ icon in the **Anomalies** table.
- You must refresh the timeline range to view the configured properties on an anomaly.
- All the properties configured on an anomaly are only applicable to future analysis.
- To view an active anomaly for **Upload File** data collection type analysis, you must select the time range when the analysis was created.

One-Click Remediation

One-Click Remediation feature reduces MTTR by enabling you to remediate an anomaly based on recommendations.

Nexus Dashboard Insights uses the enhanced framework and workflow mappings on Cisco APIC to recommend the anomaly diagnostics and impact. The Estimated Impact and Recommendations area in the Analyze Anomaly page describe the anomaly diagnostics impact and recommendations. One-Click Remediation feature allows you to execute the proposed recommendation on the fabric.

In this release remediation is supported for following anomalies:

- ACCESS_ENTITY_PROFILE_NOT_ASSOCIATED_WITH_ANY_DOMAINS
- CONNECTED_EP_LEARNING_ERROR

Guidelines and Limitations

For CONNECTED_EP_LEARNING_ERRORR` anomaly, remediation is not supported for the following use cases:

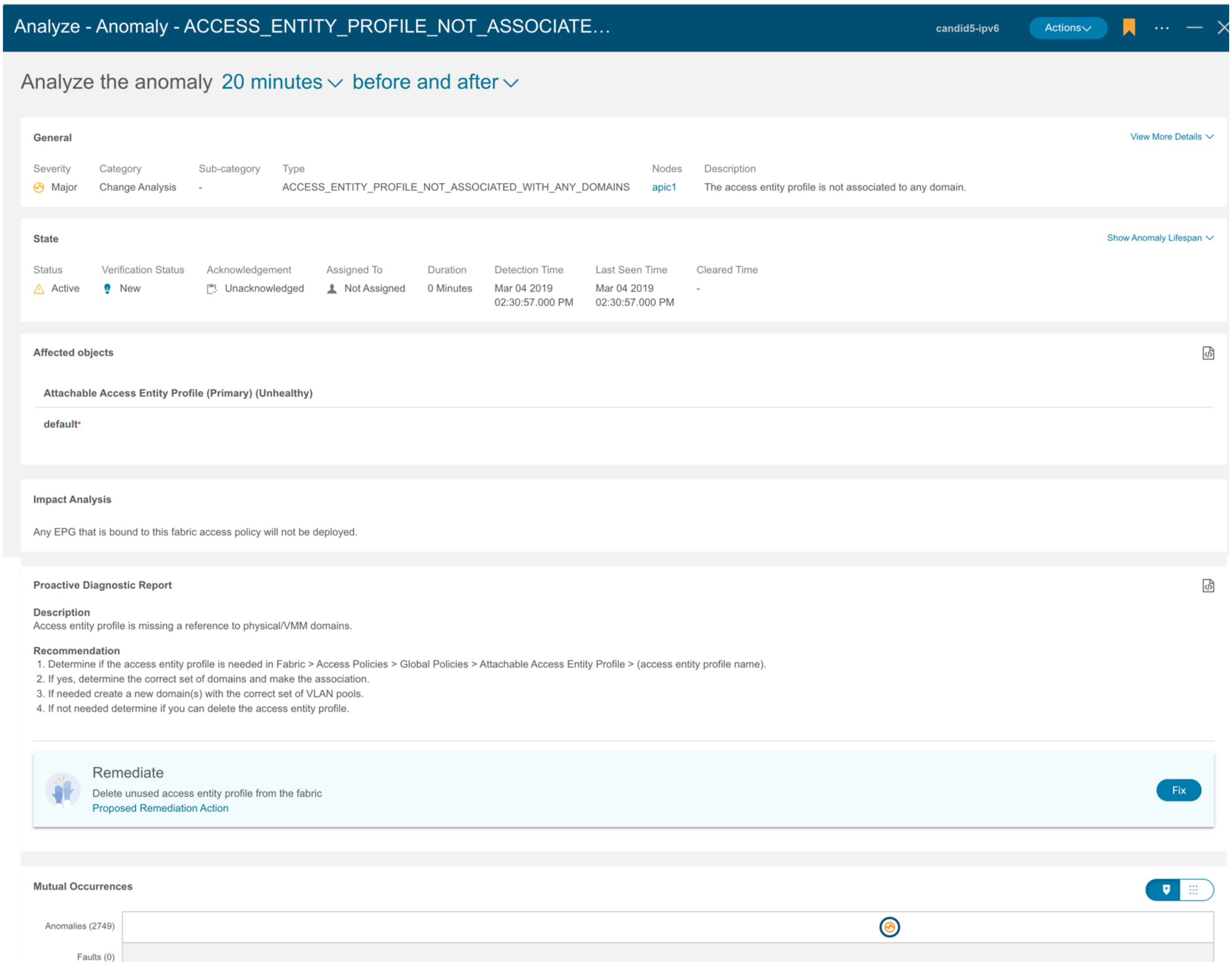
- A non-locally attached endpoints IP address or MAC is present in the global endpoint forwarding table of a leaf switch but is not present as a locally attached host in any of the other leaf switches in the fabric.
- Endpoint details in the global endpoint table are displaying incorrect NextHop Tunnel EndPoint (TEP) IP address.
- Endpoint found on spine switch is not marked as local on any of the leaf switches.
- Remediation is not supported for static endpoints.

Remediate an Anomaly

Use this procedure to remediate an anomaly.

1. Choose **Analyze Alerts** > **Anomalies**.
2. In the **Anomalies** Dashboard, select select a Site Group or site from the Site Group menu.
3. Select a time range from the drop-down menu.

   The **Anomalies** table displays individual or aggregated anomalies based on the selected site and time range.
4. Select **Individual** from the Anomalies drop-down list to view individual anomalies.
5. Click the anomaly in the **Anomalies** table for the side pane to display additional details.
6. Click **Analyze**. The **Analyze Anomaly** page displays the general information of the anomaly, state, affected object, estimated impact, proactive diagnostic report, mutual occurrences, and in-depth analysis.



Analyze - Anomaly - ACCESS_ENTITY_PROFILE_NOT_ASSOCIATE...

Analyze the anomaly 20 minutes before and after

General

Severity	Category	Sub-category	Type	Nodes	Description
Major	Change Analysis	-	ACCESS_ENTITY_PROFILE_NOT_ASSOCIATED_WITH_ANY_DOMAINS	apic1	The access entity profile is not associated to any domain.

State

Status	Verification Status	Acknowledgement	Assigned To	Duration	Detection Time	Last Seen Time	Cleared Time
Active	New	Unacknowledged	Not Assigned	0 Minutes	Mar 04 2019 02:30:57.000 PM	Mar 04 2019 02:30:57.000 PM	-

Affected objects

Attachable Access Entity Profile (Primary) (Unhealthy)

default*

Impact Analysis

Any EPG that is bound to this fabric access policy will not be deployed.

Proactive Diagnostic Report

Description
Access entity profile is missing a reference to physical/VMM domains.

Recommendation
1. Determine if the access entity profile is needed in Fabric > Access Policies > Global Policies > Attachable Access Entity Profile > (access entity profile name).
2. If yes, determine the correct set of domains and make the association.
3. If needed create a new domain(s) with the correct set of VLAN pools.
4. If not needed determine if you can delete the access entity profile.

Remediate
Delete unused access entity profile from the fabric
Proposed Remediation Action

Mutual Occurrences

7. The **Proactive Diagnostic Report** area displays the recommendations required to remediate the anomaly.
8. In the Remediate tile, click **Proposed Remediation Action** to view the actions required to remediate the anomaly.

9. Click **Fix** to execute the remediation action. The status of the remediation action is displayed as **In Progress**. Once the remediation action is completed, the status is displayed as **Completed** and the **Remediate** tile is no longer visible for the anomaly.

> In the **Proactive Diagnostic Report** area, the recommendation can contain multiple steps, but the **Proposed Remediation Action** may be applicable to only one of the steps.

Managing Anomalies

Use this procedure to manage anomalies.

Procedure

1. Choose **Analyze Alerts** > **Anomalies**.
2. In the **Anomalies** Dashboard, select a Site Group or site from the Site Group menu.
3. To unacknowledge anomalies, perform the following steps.
    a. In the filter bar, apply the filter `Acknowledgement == True`. The Anomaly table displays the acknowledged anomalies.
    b. Select **Individual** from the Anomalies drop-down list.
    c. Select the acknowledged anomalies and from the **Action** menu, select **Unacknowledge**
    d. To unacknowledge an individual anomaly, select an anomaly. Click the `···` icon and then choose **Unacknowledge** from the drop-down list.

Advisories

The Advisories dashboard displays the advisories by Type and Severity for a particular Site Group or site and based on the time range selected by the user.

- From the Advisories By drop-down list, select **Severity** to display the total number of advisories that are major, minor, and critical. The page summarizes the advisories with severity, detection time, resource type, affected nodes, and title.
- From the Advisories By drop-down list, select **Category** to display the total number of advisories by category such as PSIRT, Field Notice, HW EOL, SW EOL, and Compliance. The page summarizes the advisories with severity, detection time, resource type, affected nodes, and title.

Nexus Dashboard Insights uses metadata bundles to detect new bugs, PSIRTs, Field Notices, and End of Life Notices. Metadata packages are constantly updated by us and posted to the Cisco Intersight Cloud after validation. Nexus Dashboard Insights connects to the Cisco Intersight Cloud through a device connector that is embedded in the Nexus Dashboard platform and that pulls periodically updated metadata packages.

Choose **Settings** > **Application** > **About** to view the metadata version.

The filter bar allows you to filters the advisories.

Advisory Filters

In the **Advisories Dashboard**, you can use the following filters to refine the displayed anomalies:

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

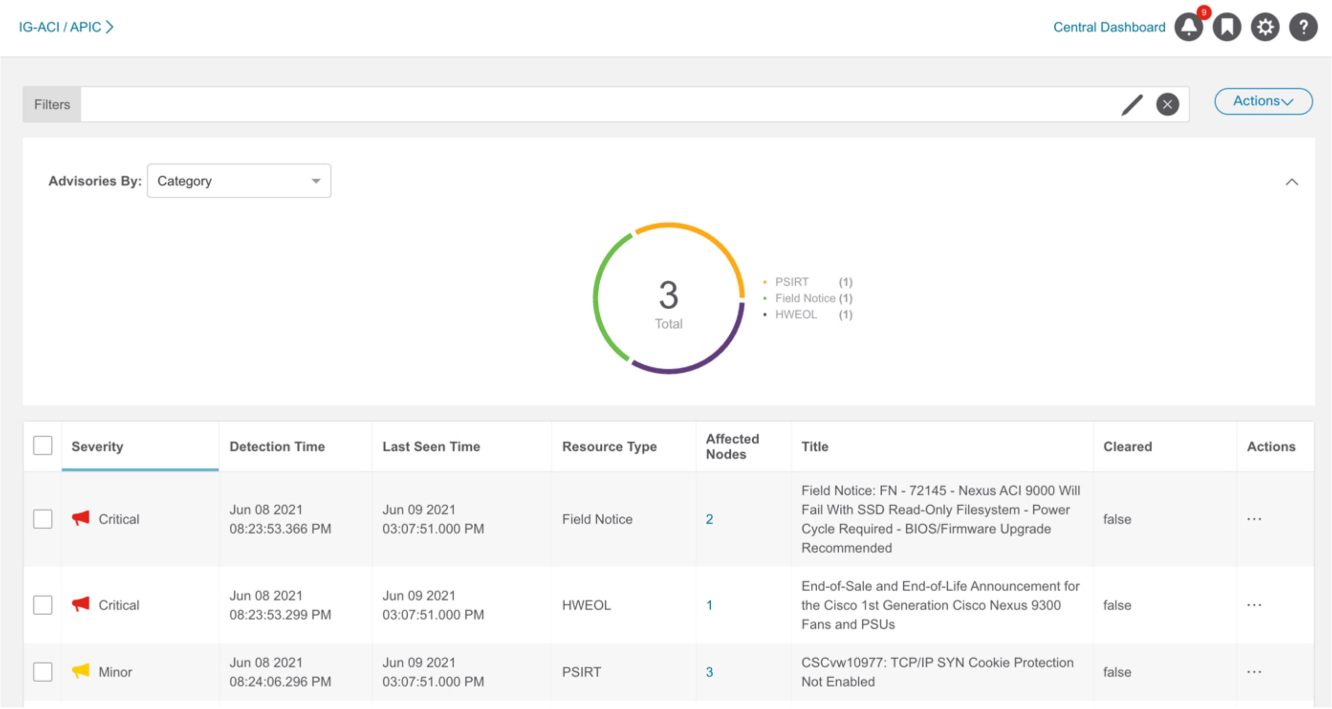
As a secondary filter refinement, use the following operators:

- `==` - 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.

Analyze Advisories

Use this procedure to analyze advisories.

1. Choose **Analyze Alerts** > **Advisories**.
2. In the **Advisories** Dashboard page, select a Site Group or site from the Site Group menu.
3. Select a time range from the drop-down menu.
4. The **Advisories** table displays individual advisories based on the selected site and time range. The advisories are sorted by Severity by default.


IG-ACI / APIC >

Central Dashboard

Filters

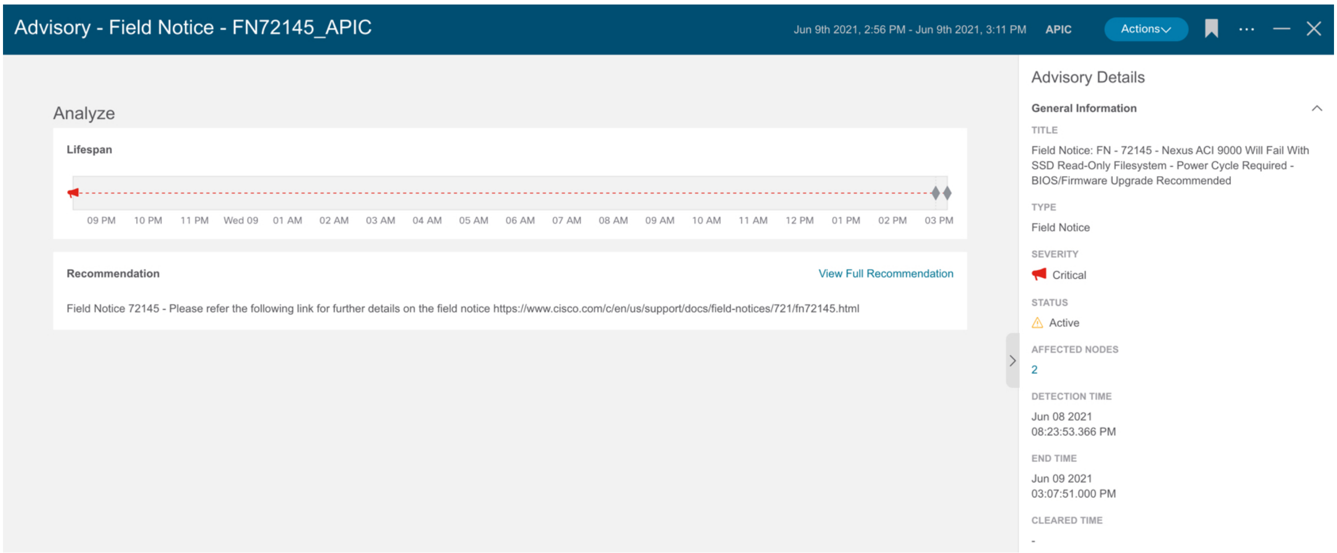
Actions

Advisories By: Category

□	Severity	Detection Time	Last Seen Time	Resource Type	Affected Nodes	Title	Cleared	Actions
□	Critical	Jun 08 2021 08:23:53.366 PM	Jun 09 2021 03:07:51.000 PM	Field Notice	2	Field Notice: FN - 72145 - Nexus ACI 9000 Will Fail With SSD Read-Only Filesystem - Power Cycle Required - BIOS/Firmware Upgrade Recommended	false	⋯
□	Critical	Jun 08 2021 08:23:53.299 PM	Jun 09 2021 03:07:51.000 PM	HWEOL	1	End-of-Sale and End-of-Life Announcement for the Cisco 1st Generation Cisco Nexus 9300 Fans and PSUs	false	⋯
□	Minor	Jun 08 2021 08:24:06.296 PM	Jun 09 2021 03:07:51.000 PM	PSIRT	3	CSCvw10977: TCP/IP SYN Cookie Protection Not Enabled	false	⋯

5. Click an advisory to view the additional details in the side pane.

6. Click **Analyze**. The **Analyze Advisory** page displays general information, lifespan, and recommendations.


Advisory - Field Notice - FN72145_APIC

Jun 9th 2021, 2:56 PM - Jun 9th 2021, 3:11 PM APIC Actions

Analyze

Lifespan

Recommendation

View Full Recommendation

Field Notice 72145 - Please refer the following link for further details on the field notice https://www.cisco.com/c/en/us/support/docs/field-notices/721/fn72145.html

Advisory Details

General Information

TITLE
Field Notice: FN - 72145 - Nexus ACI 9000 Will Fail With SSD Read-Only Filesystem - Power Cycle Required - BIOS/Firmware Upgrade Recommended

TYPE
Field Notice

SEVERITY
Critical

STATUS
Active

AFFECTED NODES
2

DETECTION TIME
Jun 08 2021
08:23:53.366 PM

END TIME
Jun 09 2021
03:07:51.000 PM

CLEARED TIME
-

a. In the **General Information** area, click affected nodes to view additional details.

b. In the **Recommendation** area, click **View Full Recommendation** to view additional details.

c. Click the ellipses ⋯ icon located on the top right of the page. Select a node from the list to open browse work pane for that particular node.

d. Click the 🔖k icon to bookmark the page.

e. Click Done.

7. Select advisories from the **Advisory** table and then select Acknowledge from the **Actions** menu to manually acknowledge advisories.

8. To filter advisories with the acknowledge status, in the **Filters** bar, select **Acknowledged** ==

True.

Alert Rules

Alert Rules

Alert rules feature enables you to acknowledge all new detected anomalies that match the criteria and adjust the anomaly score accordingly. You can also match an alert against an alert rule using the match criteria.

It also allows you to customize an anomaly by adding a custom message that will be displayed when an anomaly is raised based on the alert rule.

- An alert rule contains the match criteria required to match an alert against the rule and the action that should be applied on the matched alert.
- An alert rule can contain multiple match criteria.
- You can use attributes such as severity, category, subcategory, event name, and object match rule, to define the match criteria for the alert rule.
- A match criteria can contain one attribute or multiple attributes.
  - If a match criteria contains multiple attributes, then the alerts containing all the attributes will be matched. The **AND** operator will apply to the attributes.
  - If a match criteria contains multiple affected object match rules, then the alerts containing all of the affected object match rules will be matched.
- If an alert rule contains multiple match criteria, then the alerts containing the union of the match criteria will be matched. Any alerts that match any criteria will apply to the rule. The **OR** operator will apply to the criteria.
- Alert Rules using **Match Criteria** with **Object Match Rule** will only support the **Equals to** regex criteria.
- An alert rule can be enabled only if it contains at least one match criteria.

Guidelines and limitations

- Deleting or disabling an alert rule containing either **Acknowledge** or **Customize Anomaly** action will not delete or disable the alert rule from active anomalies. The alert rule will be applied to any new instance of the anomaly only.
- When you edit an alert rule containing either Acknowledge or Customize Anomaly action, the updates are not applied to active anomalies. The alert rule updates will be applied to any new instance of the anomaly only.
- If an alert rule contains both Acknowledge and Customize Anomaly action, and you edit the alert rule by removing either the Acknowledge and Customize Anomaly action, then the updates are not applied to active anomalies.
- When you delete or disable an alert rule containing **Customize Anomaly** action, the recommendations are still displayed in the Proactive Diagnostic Report area in the section **Rule Based Recommendation**.

- You can only manually unacknowledge anomalies, including those that are automatically acknowledged by an alert rule. You cannot automatically unacknowledge these anomalies by disabling or deleting the alert rules. See Managing Anomalies.

Creating Alert Rules

Use this procedure to create alert rules.

Procedure

1. Select the Site Group from the Site Group menu.
2. From the Actions menu next to the Site Group, choose **Configure Site Group** > **Alert Rules**.
3. Click **Create Alert Rule**.
4. Complete the following fields for **Create Alert Rule**.
   a. In the **Name** field, enter the name.
   b. In the **Description** field, enter the description.
   c. Choose the state to enable the rule to be active. If the state is enabled, the rule will be applied in the next analysis. If the state disabled, the rule will not be applied during the next analysis.
   d. Click **Add Match Criteria** to define the match criteria for the alert rule.
5. Complete the following fields for **Add Match Criteria**.
   a. From the **Site** drop-down list, select the site. A Site Group can have multiple sites. Make sure that you select the site belonging to the Site Group selected on step 1. Only the match criteria for the site running the analysis will be selected and matched with the alerts to perform the action.
   b. Select the attributes for the match criteria. You can use severity, category, subcategory, event title, and object match rule to define the attribute for the match criteria.
   c. Click **Add Object Match Rule** to define the primary affected objects for the match criteria.

> If multiple affected objects are included in the match criteria, then the alerts containing all the affected objects will be matched. If an alert rule contains multiple match criteria, then the alerts containing the union of the match criteria will be matched.

f. Click **Save**.

6. From the Actions tile, choose **Acknowledge** or **Customize Anomaly**. Acknowledge enables you to acknowledge all new detected anomalies that match the criteria and adjust the anomaly score accordingly. Customize Anomaly allows you to customize an anomaly by adding a custom message that will be displayed when an anomaly is raised based on the alert rule.
   a. Check the **Acknowledge** check-box. This option suppresses the alerts based on the alert rule but stores the alert in the database. You can view the alert in the **Anomalies** table using the Acknowledge=true filter.

        i. To filter anomalies with the acknowledge status, choose **Analyze Alerts** > **Anomalies**. In the **Filters** bar, select **Acknowledged** == **True**. The results are displayed in the **Anomalies** table.

        ii. Check **Apply to existing active anomalies** check-box to apply the alert rule to existing instance of the anomalies matching the alert rule. Uncheck the check-box to apply the alert rule to match to new instance of anomalies.

    b. Check the **Customize** check-box. Enter the recommendations to be displayed in the alert. You can create multiple rules based on different matching criteria to have more than one customized recommendation displayed in the alert. In the Analyze Anomaly page, the recommendations are displayed in the **Proactive Diagnostic Report** area in the section **Rule Based Recommendation**.

        i. Check **Apply to existing active anomalies** check-box to apply the alert rule to existing instance of the anomalies matching the alert rule. Uncheck the check-box to apply the alert rule to match to new instance of anomalies.

    c. Click **Add**

The new alert rule is displayed in the **Alert Rule** table.

Managing Alert Rules

Use this procedure to edit, enable, disable, and delete an alert rule.

Procedure

1. Select the Site Group from the Site Group menu.
2. From the Actions menu next to the Site Group, choose **Configure Site Group** > **Alert Rules**. The alert rules are displayed in the **Alert Rule** table.
3. Select an alert rule and click the `···` * icon.
    a. Choose **Edit** to edit the alert rule.

    b. Choose **Enable** to enable the alert rule. Before enabling an alert rule make sure that at least one match criteria is present in the alert rule.

    c. Choose **Disable** to disable the alert rule.

    > ℹ When the site(s) are disassociated from a Site Group, all the match criteria for those sites will be removed from the alert rule. If a match criteria is not found, the alert rule will be disabled.

    d. Choose **Delete** to delete the alert rule.

> ℹ When a Site Group is deleted, all alert rules associated with the Site Group are deleted.

Compliance

Compliance

ℹ Currently, this feature is supported for ACI Site Groups only.

The **Compliance** feature enables the user to accomplish compliance results. There are two Compliance Types and they are **Communication** and **Configuration** Compliance.

- **Communication Compliance** consists of the following Compliance Requirement Types:
  - Service Level Agreement (SLA) Compliance: You can set up rules for entities that must talk with other entities. You can use the Compliance feature to set up regulatory compliance rules.
  - Traffic Restriction Compliance: You can specify restrictions on protocols and ports for communication between objects.
  - Segmentation Compliance: You can establish walled areas around a set of entities that must not communicate with other entities.
- With **Configuration Compliance**, you can perform a configuration compliance check against a specified configuration.

In the UI, you specify your compliance requirements and Cisco Nexus Dashboard Insights will verify in the subsequent snapshots, whether the compliance requirements are satisfied by the policy that is configured on Cisco APIC. If satisfied, an event is raised stating that the compliance requirement is satisfied. One event per requirement per snapshot is raised. For example, if an assurance group runs a compliance analysis on a snapshot every 15 minutes, and there are two requirements associated with the snapshot, two anomalies will be raised.

The following examples provide you with information about the compliance **include** and **exclude** rules:

- Contains EPGs in Tenants with names that start with “a” or ending with “z”. EPGs in Tenants such as “abz” that satisfy both criteria are included only once.
- Contains EPGs in Tenants with names that start with “a” and are also in VRFs where the Tenant is “xyz” and the VRF name contains “c”. For example: When an EPG under Tenant “abc” that is in a VRF with DN uni/tn-xyz/ctx-abcde is selected, verify that both the Tenant and the VRF criteria match. An EPG under Tenant “abc” that is in a VRF with DN uni/tn-xyz1/ctx-abcde is not selected because the VRF Tenant does not match.
- Contains all EPGs under Tenants that begin with “a” except those that contain “d”. For example: An EPG under Tenant “abc” is selected. An EPG under Tenant “abcd” is not selected.
- Contains all EPGs under Tenants that begin with “a” except those EPGs that are also in the VRF with DN uni/tn-rrr/ctx-sss.

Compliance Requirement Guidelines and Limitations

- A single Compliance Requirement can be associated with multiple sites. However, traffic selectors and object selectors that are created for one Compliance Requirement cannot be reused by another Compliance Requirement. New selectors must be created each time you want to add a selector to a new Compliance Requirement.
- In the **Compliance Requirement Type** field, the **Configuration** and **Communication** tabs enable and enforce the configuration to meet best practices and business requirements that will be met only if you choose to run your changes through Cisco Nexus Dashboard Insights before you apply those changes on the controller. Otherwise, Cisco Nexus Dashboard Insights will not enforce the compliance but will report it as a violation. The **Configuration** tab enables and enforces the configuration to meet best practices and business requirements. The **Communication** tab enables communication or isolation between network objects that meet business and regulatory purposes.
- Compliance Requirements are created at the Site Group level, and the sites that you choose must be part of that Site Group.
- Compliance Requirements action rules are available within the Site Group where you define the compliance rules and actions.
- Per site, you can have a maximum of 30 active Communication Compliance requirements. If you exceed this limit, you cannot add more requirements in the **Manage Compliance** area.
- When a compliance job is in progress for one or more sites, do not start a bug scan for those sites.

Create a Compliance Requirement

Use this procedure to create a Requirement for compliance.

Before You Begin

At least one site in a Site Group must be created.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group > **Add** > **Compliance Requirement**.
3. In the **Create Compliance Requirement** dialog box, perform the following actions:
4. In the **Name** field, enter the **Requirement** name.

> Your Compliance Requirement name must be globally unique. Two different Site Groups cannot have the same Compliance Requirement name.

5. In the **Compliance Requirement Type** field, choose the **Communication** tab.
6. In the **Sites** area, click **Add Site**.

7. In the **Select Site** dialog box, choose the appropriate **Site Name**.

> When creating a Compliance Requirement, you can choose more than one site, but you must choose sites of the same type.

8. Click **Select**.
9. In the **Criteria** area, in the **Communication Type** field, choose the appropriate communication type. For example the options are **Must Talk To**, **Must Not Talk To**, **May Talk To**. For more details about which Compliance Requirement Type is configured based upon your selections, see the table that follows this procedure.
10. In the **Object Type** fields and the **Traffic Selector** area, choose the appropriate objects and traffic selector as appropriate.

    The Communication Types are applied between two different object groups. Select the appropriate criteria for both groups. After you define the criteria in the **Add Criteria** area, click the **View Selected Objects** link, and verify that the selected objects are appropriate. Based upon your selections of Communication Type and Traffic Selector Rules, the Compliance Requirement Type that you defined will be displayed.

11. After you complete defining the objects, criteria, traffic restrictions as appropriate for your site/s. click **Save** to complete the configuration.

The following table displays which Compliance Requirement Type is configured based upon your selections of Communication Type and Traffic Selector Rules.

> Additional descriptions about the Communication Types follow the table.

Table 6. Communication Type and Traffic Selector Rules Selections and the Resultant Compliance Requirement Type

Communication Type	Select a Traffic Selector Rule?	Objects You Can Select	Compliance Requirement Type
Must Talk To	Mandatory to select	EPG	Service Level Agreement (SLA)
Must Not Talk To	Not mandatory to select	• EPG • Tenant	• If you select a Traffic Selector Rule, the Compliance Rule is Traffic Restriction • If you do not select a Traffic Selector Rule, the Compliance Rule is Segmentation

Communication Type	Select a Traffic Selector Rule?	Objects You Can Select	Compliance Requirement Type
May Talk To	Mandatory to select	EPG	Traffic Restriction

Must Talk To: This allows you to configure objects where selector A **must talk to** objects selected by selector B under defined traffic restriction rules.

Must Not Talk To: Choose this configuration if your intention is that an object selected by object selector A must not talk to objects selected by object selector B using a defined type of traffic. The traffic restriction rule is optional in this configuration. Two different types of communication compliances can be configured using this option:

- Traffic Restriction compliance: You can specify a traffic selector rule that objects selected by selector A must not talk to objects selected by selector B, using a selected type of traffic that uses traffic restriction rules. This communication is restricted
- Segmentation compliance: By not defining a traffic selector rule, you can configure segmentation compliance where objects in selector A cannot talk to objects in selector B using any type of traffic. In this case, no traffic restriction rules are defined by you.

May Talk To: This allows you to create a traffic restriction compliance. Objects selected by selector A may talk to objects selected by selector B using only a specific type of traffic using traffic restriction rules. As an example, EPG A and EPG B are connected, but they can talk to each other using only the specific traffic types that are defined in the Cisco APIC contract using filters. As a Nexus Dashboard Insights user, to verify that EPG A can talk to EPG B using the traffic type TCP IP, configure the traffic restriction rule EPG A **May Talk To** EPG B using TCP IP.

View, Edit, Delete Compliance Requirements

To view, edit, or delete existing Compliance Requirements, perform the following actions:

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group, and click **Configure Site Group**.
3. In the **Configure Site Group** page, click the **Compliance Requirement** tab.
4. For the appropriate Compliance Requirement listed here, click **Actions**, and choose the appropriate action and complete the appropriate steps.

Configuration Compliance Check

Use this procedure to perform a configuration compliance check.

You can perform a configuration compliance check against a specified configuration. You specify a configuration file or snapshot, and Cisco Nexus Dashboard Insights continuously checks against it and enables you to identify changes for the objects and configurable attributes defined in Cisco APIC. If the configuration deviates from the specified configuration, then violations are raised. For each violation, there will be a separate violation anomaly displayed. Additionally, a single anomaly will be raised that includes every variable for every object of the Tenant that is not a violation.

To create a new Requirement for Configuration Compliance Check, see the following steps.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group > **Add** > **Compliance Requirement**.
3. In the **Create New Requirement** page, in the **Name** field, enter a name for the Configuration Compliance Requirement.
4. (Optional) In the **Description** field, enter a description.
5. In the **State** field, choose **Enabled** or **Disabled** as appropriate.
6. Under **Compliance Requirement Type**, choose **Configuration**.
7. In the **Sites** area, add the appropriate sites from the Site Group.
8. In the **Settings** area, in the **Base Configuration Settings** field, choose **Import Configuration** and drag and drop your file into the provided field to upload.

    > ℹ There are alternate options that you can choose instead of importing a file. Depending upon your choice for this field, different fields will become available in the **Settings** area for you to populate.

9. Click **Save**. In the **Management Compliance** page, the new Compliance Requirement is displayed.

> ℹ You cannot edit the configuration requirements when you upload a JSON/XML file. In such a case, after uploading a file, you can view or download it by navigating from the **Actions** tab.

Naming Compliance Requirement

Use this procedure to configure a naming compliance requirement.

You can configure a Naming Compliance requirement for certain objects such as BD, VRF, EPG, Contract, Subject, and Filter. All objects types are not supported.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group > **Add** > **Compliance Requirement**.
3. In the **Create New Requirement** page, in the **Name** field, enter a name for the Requirement.
4. (Optional) In the **Description** field, enter a description.
5. In the **State** field, choose **Enabled** or **Disabled** as appropriate.
6. Under **Compliance Requirement Type**, choose **Configuration**.
7. In the **Sites** area, add the appropriate sites from the Site Group.

8. In the **Settings** area, in the **Base Configuration Settings** field, choose **Manual Configuration**.
9. In the fields that display based on your choice, choose object types and add the criteria as appropriate
10. Click **Add Rule**, and in the **Add Rule** dialog box, choose the **Name** or the **Name Alias** option from the **Attribute** field drop-down list.
11. Click **Save**. Cisco Nexus Dashboard Insights starts performing a check based on the Naming compliance requirements that you specified.

In the **Manage Compliance** page, view the new requirement by choosing **View Requirement** from the **Actions** tab. To download the snapshot, click the **Download** link from the **Settings** tab.

BD to EPG Relationship Configuration

With this feature, you can specify a BD selector to have a fixed number of EPGs. By configuring a BD compliance rule, you can set the maximum number of EPGs with which a BD can be associated.

As a result of this compliance rule, when the requirement set is not satisfied, a violation anomaly will be raised. If the requirement is satisfied, it will raise an enforcement anomaly. Only when the BD selector is not resolved, a warning anomaly will be generated.

The user can configure a requirement to verify that a specified number of EPGs are being associated with a BD. The supported operators for this requirement are **At least** /**At most** /**Equal to**. As an example, if a requirement is configured that the BD must have at least 5 EPGs associated, violation events will be raised if the BD has less than 5 EPGs (0-4). However, if the BD has >= 5 events, then an enforcement anomaly will be raised.

Before You Begin

You must have a BD created before you begin this procedure.

To configure a BD to EPG relationship, perform the following steps.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group > **Add** > **Compliance Requirement**.
3. In the **Create New Requirement** page, in the **Name** field, enter a name for the BD to EPG relationship configuration.
4. (Optional) In the **Description** field, enter a description.
5. In the **State** field, choose **Enabled** or **Disabled** as appropriate.
6. Under **Compliance Requirement Type**, choose **Configuration**.
7. In the **Sites** area, add the appropriate sites from the Site Group.
8. In the **Settings** area, in the **Base Configuration Settings** field, choose **Manual Configuration**. As a result, additional fields are displayed.

9. In the additional fields, perform the following actions:
    a. In the **Object Type** field, choose BD.
    b. In the **Matching Criteria** field, click **Add Criteria** and choose the appropriate selection by name or by DN.
    c. In the **Configuration Compliance Rules** area, click **Add Rule**, to open the **Add Rule** dialog box.
    d. In the **Attribute** field, choose **EPG Association Count**.
    e. In the **Operator** field, choose your desired operator.
10. Click **Save**.

Compliance Requirement with Snapshot Selection

Use this procedure to perform a configuration compliance with snapshot selection.

> This is similar to the Configuration Compliance Check method but you also select a snapshot. With this method, you can make sure that certain attributes of objects are not changed when going from one snapshot to another snapshot.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group > **Add** > **Compliance Requirement**.
3. In the **Create New Requirement** page, in the **Name** field, enter a name for the Requirement.
4. (Optional) In the **Description** field, enter a description.
5. In the **State** field, choose **Enabled** or **Disabled** as appropriate.
6. Under **Compliance Requirement Type**, choose **Configuration**.
7. In the **Sites** area, add the appropriate sites from the Site Group.
8. In the **Settings** area, in the **Base Configuration Settings** field, choose **Snapshot Settings**.
9. In the **Time of Snapshot** field, choose the desired snapshot time, and click **Apply**.
10. In the **New Requirement** page, click **Save**. Cisco Nexus Dashboard Insights starts performing a check.

In the **Manage Compliance** page, view the new requirement by choosing **View Requirement** from the **Actions** tab. To download the snapshot, click the **Download** link from the **Settings** tab.

Template Based Compliance

With Template Based Compliance, you have the flexibility to select objects based on any attributes and provide different types of matching criteria that are not supported when you configure other compliance tasks.

Template-based compliance allows you to configure a template and specify types of queries to select objects and attributes that enforce specific conditions when enabled. The Template Query Language enables you to select any configurable object and define what attributes to apply to the compliance. **SELECT** allows you to choose a certain subset of objects that you want to specify, and **MATCH** defines the Compliance rule.

With other types of Compliance configurations releases you can upload a JSON/XML file and all the attributes in the file will be matched as is. Alternatively, you can also select a few specific objects based on name matches, and you can configure select attributes supported for those specific objects. This allows you to search for existing or future objects matching the names that are checked for compliance for the specified parameters.

Verified Scalability Limits for Template Based Compliance

- Number of Template Requirements are 5 for APIC with total configurable objects of 150,000.
- Each template selects 15,000 objects on an average.
- Number of tenants per template is 30 tenants, with each tenant selecting 500 objects on an average.
- You may create more than 5 templates (the upper limit is 30 total Requirements), if the total objects selected by all the templates are less than 5*15,000 and the total configurations in APIC are < 150,000 objects.

Template Guidelines

Follow these guidelines when defining a template:

- The JSON file format is supported for the template query. The XML format is *NOT* supported.
- The template follows the same structure as used in APIC files. It has objects, attributes, and children.
- The template file size that you upload can be up to 15 MB including whitespaces. Pretty JSON files will have whitespaces to support indentation. To reduce the file size, you can remove whitespaces and upload the file.

Template Syntax Guidelines

Follow these syntax examples and guidelines:

Template Syntax for SELECT

SELECT allows the user to choose a subset of objects based on the criteria defined using the KEYWORDS. In the following example, **SELECT** is followed by the attribute name which is an attribute of the object. You must use one of the following keywords:

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

Syntax:

SELECT(<attribute_name>): KEY_WORD(<value>) attribute_name any attribute of the object

KEY_WORDS→>

"STARTS_WITH(abc)” “ENDS_WITH(xzy)” “EXACT(abc)” “OR(abc, xyz)”

REGEX(<value>) - where the value must follow the standard regex expression syntax "SELECT(name)": "REGEX(Ctrct_[1-3])"

For more details about keyword regular expressions, see Summary of Regular-Expressions Constructs.

The following is a syntax example:

```
{
  "fvAEPg":
  {
    "attributes":
    {
      "dn": "EXACT(uni/tn-aepg_vzanycons_imd_ctx_pass_7/ap-CTX1_AP1/epg-
CTX1_BD1_AP1_EPG7)",
      "MATCH(isAttrBasedEPg)": "EXACT(no)"
    }
  }
}
```

If **SELECT** is not specified for an attribute, then **rn** and **dn** will be considered as **SELECT** by default.

Template Syntax for MATCH

The **MATCH** criteria is used to define the Compliance rule. These compliance rules will be applied on objects that are selected using the **SELECT** criteria. The keyword to match the attribute is MATCH, and the match is applied to all objects of the specified type. Specify the attributes and values that you want to match. The attributes are matched to all the objects of the specified type.

The values are not required to be exact matches. They can be as follows:

- STARTS_WITH

- ENDS_WITH
- EXACT
- OR
- REGEX

MATCH(<attribute_name>): KEY_WORD(<value>)

The following is a syntax example where you select all **vzBrCP** contract objects where the name is **Ctrct_1** or **Ctrct_2** or **Ctrct_3**. Then you define that the scope is context.

```
"vzBrCP": {
  "attributes": {
    "SELECT(name)": "REGEX(Ctrct_[1-3])",
    "MATCH(scope)": "EXACT(context)"
  }
}
```

The following is a syntax example where if the KEY_WORD is not defined, the default behavior is **EXACT**. When you use MATCH(dn) and MATCH(rn), they are defined as match criteria.

ℹ If an attribute (other than **dn** and **rn**) does not have **MATCH** or **SELECT** specified, it will be considered as **MATCH** by default.

```
{
  "fvAEPg": {
    "attributes": {
      "SELECT(dn)": "uni/tn-aepg_vzanycons_imd_ctx_pass_7/ap-CTX1_AP1/epg-
CTX1_BD1_AP1_EPG7",
      "MATCH(isAttrBasedEPg)": "EXACT(no)",
      "prio": "OR(unspecified, prio1)"
    }
  }
}
```

In the above example, by default, "prio" will be a **MATCH**.

The following is a syntax example of a generic template where the **KEY_WORD** is {}. You can use this template to customize your requirements, select attributes, regular expresssions.

The **KEY_WORD** values can be as follows:

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR

- REGEX

```
{
  "<MO type>": {
    "attributes": {
      "SELECT(<attribute>)": "KEY_WORD(<expression>)",
      "MATCH(<attribute>)": " KEY_WORD (<value>)"
    },
    "children": [
      {
        "<MO type>": {
          "attributes": {
            "SELECT(<attribute>)": " KEY_WORD (<value>)",
            "MATCH(<attribute>)": " KEY_WORD (<value>)"

          },
          "children": [
            {
              "<MO type>": {
                "attributes": {
                  "SELECT((<attribute>)": " KEY_WORD (<value>)",
                  "MATCH(<attribute>)": " KEY_WORD (<value>,<value>)"

                }
              }
            }
          ]
        }
      }
    ]
  }
}
```

The following is an example of a Template Based Configuration Compliance. In this example, choose all the contracts where **name** starts with **Ctrct_(1-3)**. Then, match **scope** which must be **context**. For **children** of the subjects of those contracts, select **name** as any (wildcard) and **nameAlias** must be ABC.

```
{
  "vzBrCP": {
    "attributes": {
      "SELECT(name)": "REGEX(Ctrct_[1-3])",
      "MATCH(scope)": "EXACT(context)"
    },
    "children": [
      {
        "vzSubj": {
          "attributes": {
            "SELECT(name)": "REGEX(.*)",
            "nameAlias": "ABC"
          },
          "children": [
            {
              "vzRsSubjFiltAtt": {
                "attributes": {
                  "SELECT(tnVzFilterName)": "ENDS_WITH(3_1_1)",
                  "MATCH(action)": "deny"
                }
              }
            }
          ]
        }
      }
    ]
  }
}
```

The following are examples of templates where the attribute value is null or empty.

```
"REGEX(^.{0}$)"
"EXACT()"
"OR(test, )" <- use space
```

```
{
  "fvTenant": {
    "attributes": {
      "MATCH(annotation)": "OR(orchestrator:msc, )",
      "SELECT(name)": "REGEX(aepg_aepg_imd_tnt_pass_[0-9]+)",
    }
  }
}
```

- In a template, defining **attributes** is mandatory because the Compliance is applied on the attribute.
- In a template, defining **children** is optional. If children are defined in the query, the selection is

applied to the real children of the selected objects.

- In a template, you can include the same object type only once per child array. This prevents the possibility of creating requirements that will result in conflicting compliance rules that result in violation anomalies.

  In the following *invalid* example, if there is a BD named **ABCXYZ**, it will be selected by both the child object templates snippets for **fvBD**, and one of them will be a violation because **type** can either be **regular** or **fc**.

  ```
  {
    "fvTenant": {
      "attributes": {
        "SELECT(name)": "EXACT(tenantABC)"
      },
      "children": [
        {
          "fvBD": {
            "attributes": {
              "MATCH(type)": "EXACT(regular)",
              "SELECT(name)": "REGEX(.*ABC.*)"
            }
          }
        },
              {
          "fvBD": {
            "attributes": {
              "MATCH(type)": "EXACT(fc)",
              "SELECT(name)": "REGEX(.*XYZ.*)"
            }
          }
        }
      ]
    }
  }
  ```

Configure Template Based Compliance

Use this procedure to configure object selectors for Naming Compliance using template based compliance.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.
2. Click the Actions menu next to the Site Group > **Add** > **Compliance Requirement**.
3. In the **Create New Requirement** page, in the **Name** field, enter a name for the Requirement.
4. (Optional) In the **Description** field, enter a description.
5. In the **State** field, choose **Enabled** or **Disabled** as appropriate.

6. Under **Compliance Requirement Type**, choose **Configuration**.
7. In the **Settings** area, click **Configuration** type.
8. In the **Base Configuration Settings** field, choose **Template Based Compliance**.
9. In the **Sites** area, add the appropriate sites from the Site Group.
10. In the **Choose a file or drag and drop to upload** area, upload your template based file. After the file upload is complete, you can click the View icon to review the contents of the file that you uploaded.

> A JSON file is currently supported. XML file is not supported. The template file size that you upload can be up to 15 MB. The view feature will not be available if the file size is greater than 5 MB. If the file size is greater than 5 MB, you can download the file and view the contents.

11. Click **Save**.
12. In the **Configure Site Group** page, under the **Compliance Requirements** tab, the new compliance requirement is displayed.

If the **Status** is **Enabled**, the compliance requirement is ready to be consumed in the next snapshot. If the status is **Disabled**, you can click the Actions menu for the row and click **Edit** to open the **Edit Compliance Requirement** page. In the **State** field, change the state to **Enabled** and click **Save**.

This completes the configuration.

Use a Template to Configure Object Selectors for Naming Compliance

When you use the Naming Compliance Requirement task to configure compliance, only a few specific object selectors are supported (such as BD, EPG, VRF). By using a template, you can configure *any* object for a Naming Compliance Requirement.

An object can be any managed object from APIC, and its selection is based on the Distinguished Name of the object. If you prefer to have a different attribute as the selection criteria, you can use any valid attribute of that object. The **SELECT** criteria can be defined using one of the following keywords.

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

The following is a syntax example:

```
{
   "<object>":{
      "attributes":{
         "SELECT(dn)":"<KEY_WORD>(<value>)",
         "MATCH(nameAlias/name)":"<KEY_WORD>(<value>)"
      }
   }
}
```

For Naming Compliance, the Compliance rules are on the name and nameAlias fields that are indicated by **MATCH**. The **MATCH** criteria can be again defined using the keywords provided earlier in this section.

Use the following example template to configure a Naming Compliance to match selected objects to **name** or **nameAlias**:

```
{
   "vzSubj":{
      "attributes":{
         "SELECT(dn)":"EXACT(subj1)",
         "MATCH(nameAlias)":"STARTS_WITH(ABC)"
      }
   }
}
```

> ℹ In the above template, you can use any object instead of "vzSubj", and you can use any attribute instead of "dn".

As the attribute **dn** is always considered as **SELECT** by default and any other attribute is always considered as **MATCH**, the above template can be simplified as displayed in the example below. Additionally, if the keyword is not defined, the default behavior is **EXACT**.

```
{
   "vzSubj":{
      "attributes":{
         "dn":"subj1""nameAlias":"STARTS_WITH(ABC)"
      }
   }
}
```

> ℹ In the above template, you can use any object instead of "vzSubj", and you can use any attribute instead of "dn".

For the procedure to configure Object Selectors for Naming Compliance using the above template, see Configure Template Based Compliance.

Use a Template to Configure Object Selectors Based on Tags and Annotations

As an APIC user, you can create tags on managed objects (MOs) that result in creating child objects of type **tagInst** or **tagAnnotation** (based on which APIC version is in use).

Therefore, if you select objects based on a tag created in APIC, you can follow the templates provided in this section to configure object selectors on tags and annotations.

The following is an example that displays the child object as type **tagInst**:

```
{
   "<object>":{
      "attributes":{
         "MATCH(<attribute_name>)":"<KEY_WORD(<value>)"
      },
      "children":[
         {
            "<tagInst>":{
               "attributes":{
                  "SELECT(<attribute_name>)":"<KEY_WORD(<value>)"
               }
            }
         }
      ]
   }
}
```

The following is an example that displays the child object as type **tagAnnotation**:

```
{
   "<object>":{
      "attributes":{
         "MATCH(<attribute_name>)":"<KEY_WORD(<value>)"
      },
      "children":[
         {
            "<tagAnnotation>":{
               "attributes":{
                  "SELECT(<key or value>)":"<KEY_WORD(<value>)"
               }
            }
         }
      ]
   }
}
```

An object can be any valid APIC object with **tagAnnotation** or **tagInst** as a child. Object selection is defined in the **tagInst** or **tagAnnotation** object using **SELECT** on the name in the case of **tagInst**, and **key or value** in the case of **tagAnnotation**. The selection criteria can be any of the following keywords:

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

Compliance rules are defined at the parent object level using **MATCH** and the criteria can be defined using any **KEY_WORD**. **tagInst** or **tagAnnotation** do not participate in Compliance rules as they only provide the selection criteria.

The following is an example template where you **SELECT** all the fVBDs where the tag is “BDs_in_cisco”, and those BDs must have name as **BD** or **app1BD**.

```
{
   "fvBD":{
      "attributes":{
         "MATCH(name)":"OR(BD, app1BD)"
      },
      "children":[
         {
            "tagInst":{
               "attributes":{
                  "SELECT(name)":"EXACT(BDs_in_cisco)"
               }
            }
         }
      ]
   }
}
```

For the procedure to configure object selectors based on Tags and Annotations using a template, see Configure Template Based Compliance.

When using the steps to Configure Template Based Compliance, to configure object selectors for tags and annotations, you must perform an additional step. Before you click **Save**, in the **Create New Requirement** page, you must check the checkbox for the field **Enable Object Selection Based on tagAnnotation/tagInst**. Therefore, if any object has a tag annotation or tagInst, the parent based on the selection criteria in these two objects will be selected.

Schedule a Compliance Analysis

Use this procedure to schedule a compliance analysis.

Before You Begin

At least one site in a Site Group must be created.

Procedure

1. In the **Overview** page, at the top, choose your Site Group for which you want to run the Compliance Analysis. If required expand the listed Site Groups to view the sites displayed, and choose a site.
2. Click the Actions menu next to the Site, and click **Configure Site Group**.
3. In the **Configure Site Group** page, click **Assurance Analysis** tab. Under the **General** area, details for the analysis that will be run on the selected site are listed based upon the default values. To perform a Scheduled Analysis, the default values are already populated.
4. To start the analysis, click the edit icon for your site.
5. In the **Configuration** dialog box, change the **State** from **Disabled** to **Enabled**.
6. Modify the **Start Time**, **Repeat Every**, and **End On** field values if required. Click **Save**.

The analysis will run based upon your scheduled selections.

In the **History** table in the same page, the analysis job appears and displays the status under **Start Time**. For example, you can see **Scheduled** or **In-Progress**. When the analysis is completed, the status displays **Completed**. The **End Time** and **Run Time** are also listed as they become available for an analysis.

Run an Instant Compliance Analysis

Use this procedure to run an instant compliance analysis.

Before You Begin

At least one site in a Site Group must be created.

Procedure

1. In the **Overview** page, choose you Site Group for which you want to run the Compliance Analysis. If required expand the listed Site Groups to view the sites displayed, and choose a site.
2. Click the Actions menu next to your Site Group > **Configure Site Group**.
3. In the **Configure Site Group** page, click **Assurance Analysis** tab. Under the **General** area, details for the analysis that will be run on the selected site are listed based upon the default values.
4. To run an instant analysis, click the **Run Now** button for your site. A message displays that the

Assurance Analysis has started for your site.

In the **History** table in the same page, the analysis job appears and displays the status under **Start Time**. For example, you can see **Scheduled** or **In-Progress**. When the analysis is completed, you will see "Completed". The **End Time** and **Run Time** are also listed as they become available for an analysis.

View a Compliance Analysis

Use this procedure to view details of a compliance analysis.

Before You Begin

At least one compliance analysis for a site must be complete.

Procedure

1. In the **Overview** page, in the left Navigation, click **Compliance**.
2. In the **Compliance Analysis** page, to view an event, choose the appropriate site and a snapshot.
3. At the top of the page, choose the appropriate site.
4. Click the drop-down link to display the time, to view the appropriate modes for which you want to see the analysis. Based upon the Mode you choose, additional fields may be available for you to choose.
5. When you are done selecting your choices, click **Apply**.

You can view analysis from the available modes, for any time period and snapshot selection for which an analysis was generated. You can also view the Anomalies that are generated for the site as a result of the compliance requirements that are set for it. The **Compliance summary** area displays the total anomalies by severity that are generated. The **Non-compliant resources** area displays the objects that have been affected by the defined requirements. The **Requirement Violations** area displays the percentage of compliance requirements that are fully satisfied. The **Requirement Type** area displays the number of each requirement type that is associated with this site. Click the drop-down arrow in this field to expand the view and view the requirement types that are associated along with details of violated, enforced, or verified.

See Analyze Alerts for details about anomalies and alerts.

Policy CAM

Policy CAM

The Policy CAM feature determines how and where resources in the fabric are used. Policy CAM provides information about the resource utilization in the network, and the amount of policy content-addressable memory (Policy CAM) utilization.

In Cisco Nexus Dashboard Insights **Overview** page, in the left Navigation, expand **Browse** > **Resource Utilization**. In the **Resource Utilization** Work pane, click the **Browse** tab to locate the "Policy CAM" tab.

View Policy CAM Analyzer Details for all Nodes in a Site Group

To view Policy CAM details for nodes in a Site Group follow these steps.

1. In Cisco Nexus Dashboard Insights **Overview** page, on the top, choose the choose the appropriate Site Group.
2. In the left Navigation, expand **Browse** > **Resource Utilization**.
3. In the Work pane, in time selector field, choose the appropriate snapshot of time within which to view the resource utilization, and click **Apply**.

   > Within the time range you selected, the last snapshot is considered for each of the site/s included in the Site Group. Therefore, you get the latest state of the application within the selected time range.

4. Click **Browse**, and in the **Top Nodes by** field, choose **Policy TCAM** from the drop-down list. A bar chart is displayed with a list of each node in the Site Group based on resource utilization, starting with the node that has the maximum utilization followed by the next lower TCAM utilization. When you hover on a specific bar in the graph, it displays the details for that node such as maximum capacity, hardware count, utilization percent.
5. In the following table, click the **Policy CAM** tab in the page to display details with anomaly scores for each node. The anomaly score displays the highest category of anomaly associated with that node. For example, if a node has one warning anomaly and one critical anomaly associated, the Anomaly Score for that node will display "Critical".
6. Click the **Launch Policy CAM Analyzer** button.
7. In the **Policy CAM Analyzer** page, in the **Analyze Site** area, choose the appropriate site and the snapshot, and click **Apply**. Details for all the nodes in the Site Group are displayed.
8. Toggle the icon on the top right of the page in order to change the presentation of the information in the page. When you toggle the icon to the left, an overview of the Policy CAM anomalies generated for the selected snapshot within the site is displayed. It displays anomaly counts based on severities. When you toggle to the right of the icon, the information is displayed in a tabular form.

You can view the rule utilization and anomalies that are generated for each node. You also see the associated anomaly score for each node. In the **Associated Policies** area, you can use the **Filter** column as a contract filter for a specific node. Each item in each column can be selected to show relevant associations and relationships between the tenants, contracts, and EPGs. The **Policy CAM Statistics** table displays all the nodes and associated rules, and you can drill into details for a specific node here. In the **Policy CAM Rules** table, you can view the listings for all of the nodes based on the selected snapshot. In the **Anomalies** table, you can view the anomalies that are generated in the selected snapshot of time, individually by nodes or as an aggregate.

See Analyze Alerts for details about anomalies and alerts.

View Policy CAM Analyzer Details for a Specific Node in a Site Group

To view Policy CAM details for a specific node in a Site Group follow these steps.

1. In Cisco Nexus Dashboard Insights **Overview** page, on the top, choose the choose the appropriate Site Group.
2. In the left Navigation, expand **Browse** > **Resource Utilization**.
3. In the Work pane, in the time selector field, choose the appropriate snapshot of time within which to view the resource utilization, and click **Apply**.

> Within the time range you selected, the last snapshot is considered for all the site/s included in the Site Group.

4. In the following table, click the **Policy CAM** tab in the page to display details with anomaly scores for each node. The anomaly score displays the highest category associated with that node.
5. Click a specific node in the **Node** column, and a sidebar displays the resource count details for that node. The anomalies generated for resource utilization for the specific node are also displayed with tags such as Critical, Major, Minor, Warning etc.
6. In the sidebar, click the Detail icon in the top right to view the **Resource Details** page for that node. In the **Policy CAM** section in the **Resource Details** page, details of the resource utilization count for a specific node are displayed.

Toggle the icon on the top right of the page in order to change the presentation of the information in the page. When you toggle the icon to the left, an overview of the Policy CAM anomalies generated for the selected snapshot for a specific node is displayed. It displays anomaly counts based on severities. When you toggle to the right of the icon, the information is displayed in a tabular form.

1. Click **Done** to close the **Resource Details** page.

When viewing the **Policy CAM** tab, if you click the **Launch Policy CAMM Analyzer** button, it will launch the Policy CAM analyzer filtering based on the selected node.

See Analyze Alerts for details about anomalies and alerts.

Troubleshoot

Delta Analysis

Nexus Dashboard Insights performs analysis of a Site Group at regular intervals and the data is collected in 15-minute intervals.

At each interval, Nexus Dashboard Insights captures a snapshot of the controller policies and the fabric run time state, performs analysis, and generates anomalies. The anomalies generated describe the health of the network at that snapshot.

Delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two snapshots. Delta analysis consists of the following workflow:

- **Create New Analysis**: Enables you to create a new delta analysis and manage existing analysis. See Creating Delta Analysis.
- **View Delta Analysis**: Enables you to view results of successful delta analysis such as health delta and policy delta. See Viewing Delta Analysis Results.

Health Delta

Health Delta analyses the difference in the health of the fabric across the two snapshots. The results are displayed in the following areas:

- **Anomaly Count**: Displays the difference in anomaly count per severity across the snapshots.
- **Health Delta by Resources**: Displays the count of resources by type that have seen a change in their health. The changes can either be issues resolved or new issues detected.
- **Anomalies**: The **Aggregated** view displays the delta status for aggregated anomalies across the two snapshots. The **Individual** view displays the delta status for each anomaly across the two snapshots.

Policy Delta

Policy Delta for ACI

Policy Delta analyzes the differences in the policy between the two snapshots and provides a co-related view of what has changed in the ACI Fabric.

The policy delta view enables you to:

- View the changed policy objects between the two snapshots.
- View the added, modified, and deleted policy configurations between the two snapshots.
- Export the policy configuration for the earlier snapshots policy and later snapshots policy.
- Search for text in added, modified, deleted, and unchanged areas in the policy delta.
- View the context around the modified areas in the policy delta.

- View the difference in the APIC audit logs across the two snapshots.

Policy Delta for DCNM

Policy Delta for DCNM Site Group analyzes the changed nodes or switches across two snapshots and obtains a co-related view of what has changed in the NX-OS switches.

The policy delta view enables you to:

- View the changed nodes or switches between the two snapshots.
- View the context around the modified areas in the policy delta.

Guidelines and Limitations

- The Delta Analysis functionality currently supports the local authentication domain only.
- While you are currently allowed to create more than one Delta Analyses at any given time, we recommend that you do not queue more than one Delta Analysis at any given time. In addition, we recommend that you wait for some time (approximately 10 minutes) between creating new analyses to avoid the risk of adversely impacting the run time of the concurrent online Site Group analysis.

  The interdependency arises because the Delta Analysis results in an increased load on the database. Sustained high-database load from multiple back-to-back Delta Analyses may affect the run-time of the online analysis.
- The **APIC Configuration Export Policy** must be of the same format (XML/JSON) for both the snapshots.
- The policy delta will not be performed if there are any APIC configuration export policy collection errors.

Creating Delta Analysis

Use this procedure to create a delta analysis.

Before You Begin

For ACI Assurance Group users, APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure the **APIC Configuration Export Policy**.

Procedure

1. Choose **Troubleshoot** > **Delta Analysis**.
2. From the Site Group menu, select a Site Group.
3. Click **New Delta Analysis**.
4. Complete the following fields for **Create Delta Analysis**.

   a. In the **Name** field, enter the name. The name must be unique across all the analyses.

   b. Click **Site** to select the site.

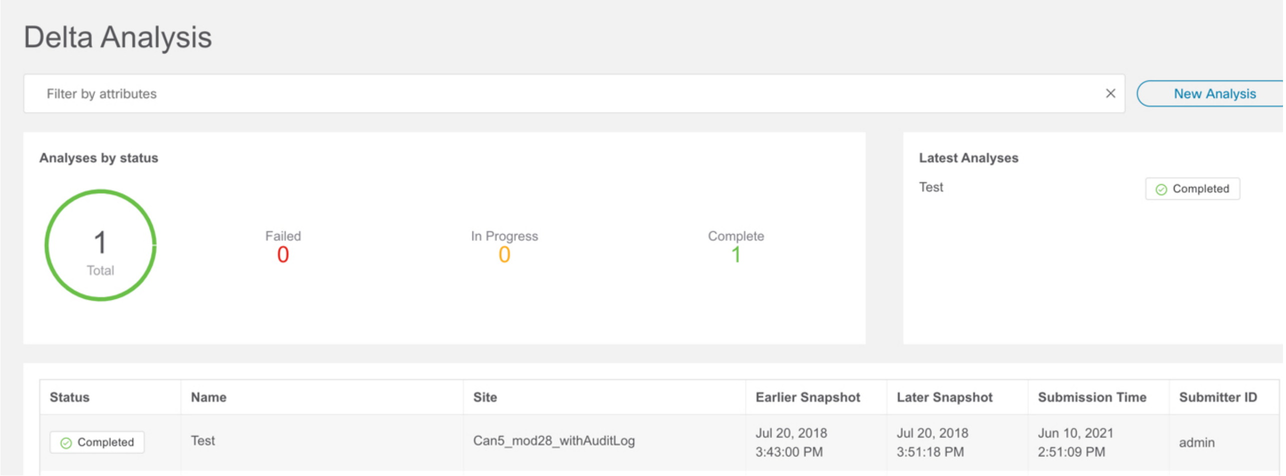
   c. Click **Select date and time** and choose the first snapshot for the delta analysis. Click **Apply**.

   d. Click **Select date and time** and choose the second snapshot for the delta analysis. Click **Apply**.

> The two snapshots selected for the delta analysis must belong to the same Site Group.

5. Click **Create**.

6. The status of the delta analysis is displayed in the **Delta Analysis** table.



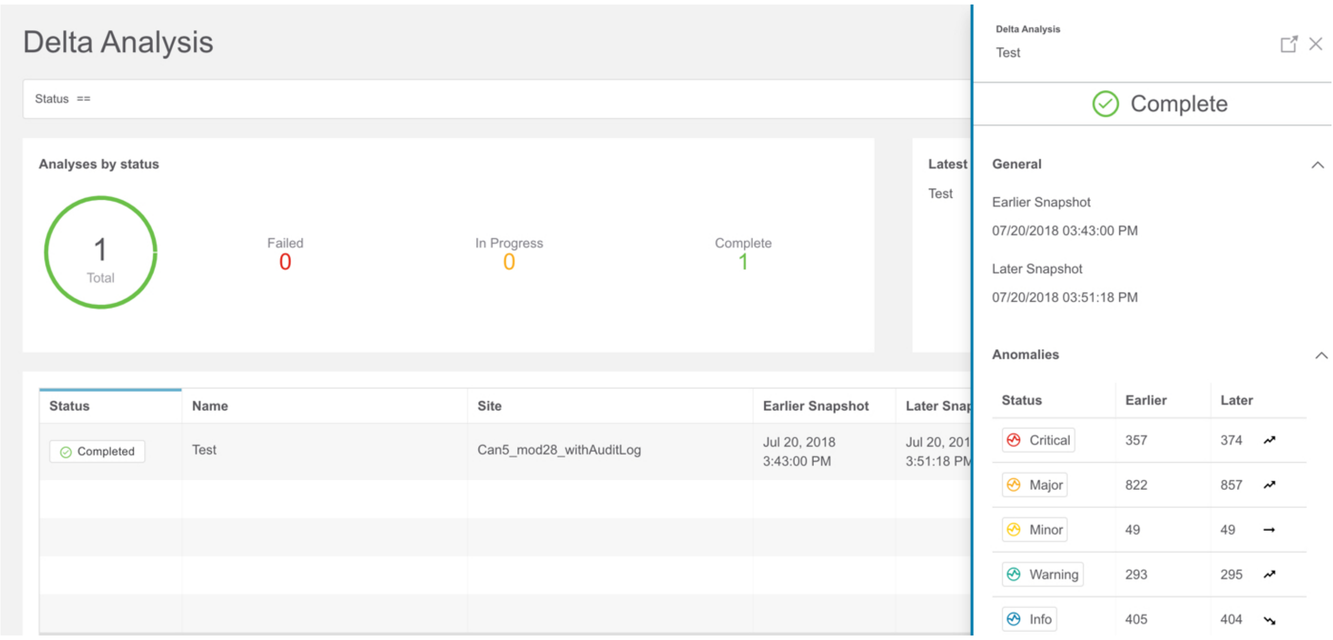
Status	Name	Site	Earlier Snapshot	Later Snapshot	Submission Time	Submitter ID
Completed	Test	Can5_mod28_withAuditLog	Jul 20, 2018 3:43:00 PM	Jul 20, 2018 3:51:18 PM	Jun 10, 2021 2:51:09 PM	admin

You can perform one delta analysis at a time. To perform another delta analysis, you must stop the current delta analysis and then start the another delta analysis.

7. (Optional) From the Status column, select an In Progress or Scheduled analysis and click **STOP** to stop the delta analysis.

8. To view the results of the delta analysis, select a delta analysis from the **Delta Analysis** table. The summary pane displays details such as general information and anomaly information.

9. Click the detail icon to view health and policy delta details.



Delta Analysis

Status ==

Analyses by status

1 Total

Failed 0

In Progress 0

Complete 1

Latest

Test

Status	Name	Site	Earlier Snapshot	Later Snap
Completed	Test	Can5_mod28_withAuditLog	Jul 20, 2018 3:43:00 PM	Jul 20, 201 3:51:18 PM

Delta Analysis

Test

Complete

General

Earlier Snapshot

07/20/2018 03:43:00 PM

Later Snapshot

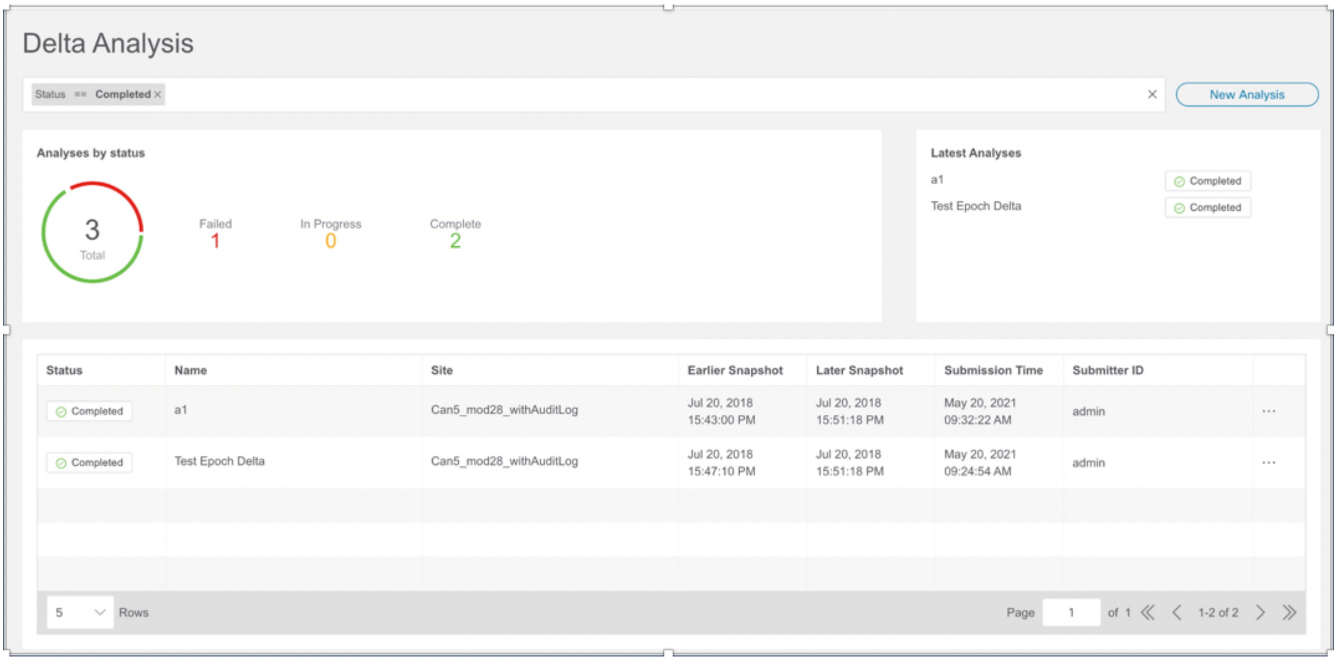
07/20/2018 03:51:18 PM

Anomalies

Status	Earlier	Later
Critical	357	374 ↗
Major	822	857 ↗
Minor	49	49 →
Warning	293	295 ↗
Info	405	404 ↘

Viewing Delta Analysis

The Delta Analysis Dashboard displays a graph of analyses by status for a particular Site Group or site and displays the latest analyses.



Delta Analysis

Status == Completed ×

Analyses by status

3 Total

Failed 1

In Progress 0

Complete 2

Latest Analyses

a1	Completed
Test Epoch Delta	Completed

Status	Name	Site	Earlier Snapshot	Later Snapshot	Submission Time	Submitter ID	
Completed	a1	Can5_mod28_withAuditLog	Jul 20, 2018 15:43:00 PM	Jul 20, 2018 15:51:18 PM	May 20, 2021 09:32:22 AM	admin	···
Completed	Test Epoch Delta	Can5_mod28_withAuditLog	Jul 20, 2018 15:47:10 PM	Jul 20, 2018 15:51:18 PM	May 20, 2021 09:24:54 AM	admin	···

5 Rows

Page 1 of 1 1-2 of 2

The filter bar allows you to filters the analysis by status, name, and submitter.

The page also displays the analysis in a tabular format. The analysis are sorted by status.

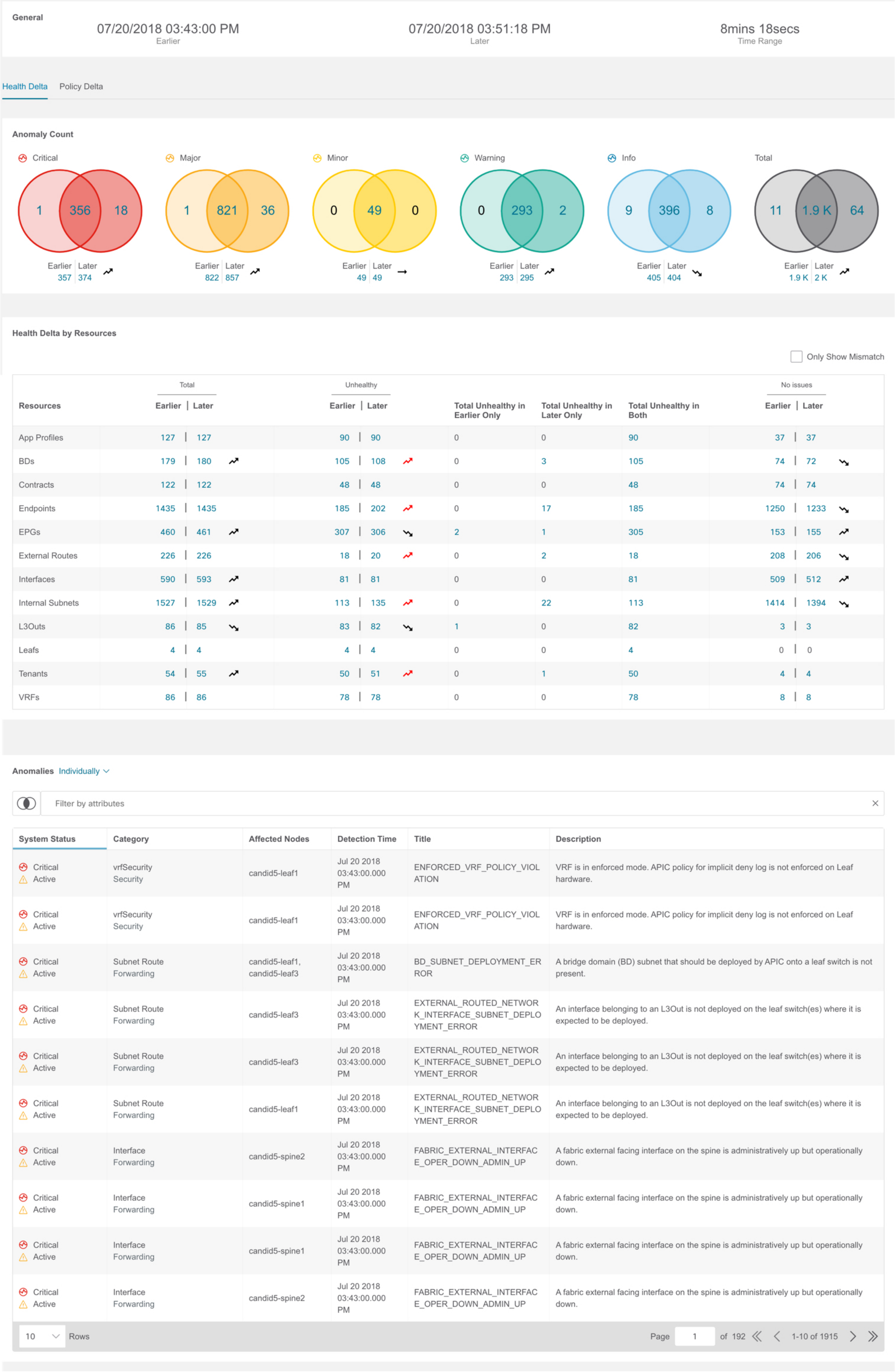
- To view the results of health delta analysis, see Viewing Health Delta Analysis.
- To view the results of policy delta analysis, see Viewing Policy Delta Analysis.
- To edit or delete a delta analysis, see Managing Delta Analysis.

Viewing Health Delta Analysis

Use this procedure to view the results of the health delta analysis.

Procedure

1. Choose **Troubleshoot** > **Delta Analysis**.
2. From the Site Group menu, select a Site Group.
3. Select a completed analysis from the Delta Analysis table. In the summary pane, click the detail icon to view health and policy delta details.
4. Click **Health Delta** to view the results of the health of the fabric.



General

07/20/2018 03:43:00 PM
Earlier

07/20/2018 03:51:18 PM
Later

8mins 18secs
Time Range

Health Delta   Policy Delta

Anomaly Count

	Critical	Major	Minor	Warning	Info	Total
Earlier only	1	1	0	0	9	11
Both	356	821	49	293	396	1.9 K
Later only	18	36	0	2	8	64
Earlier	357	822	49	293	405	1.9 K
Later	374	857	49	295	404	2 K
	↗	↗	→	↗	↘	↗

Health Delta by Resources

□ Only Show Mismatch

	Total			Unhealthy						No issues		
Resources	**Earlier**	**Later**		**Earlier**	**Later**		**Total Unhealthy in Earlier Only**	**Total Unhealthy in Later Only**	**Total Unhealthy in Both**	**Earlier**	**Later**	
App Profiles	127	127		90	90		0	0	90	37	37	
BDs	179	180	↗	105	108	↗	0	3	105	74	72	↘
Contracts	122	122		48	48		0	0	48	74	74	
Endpoints	1435	1435		185	202	↗	0	17	185	1250	1233	↘
EPGs	460	461	↗	307	306	↘	2	1	305	153	155	↗
External Routes	226	226		18	20	↗	0	2	18	208	206	↘
Interfaces	590	593	↗	81	81		0	0	81	509	512	↗
Internal Subnets	1527	1529	↗	113	135	↗	0	22	113	1414	1394	↘
L3Outs	86	85	↘	83	82	↘	1	0	82	3	3	
Leafs	4	4		4	4		0	0	4	0	0	
Tenants	54	55	↗	50	51	↗	0	1	50	4	4	
VRFs	86	86		78	78		0	0	78	8	8	

Anomalies Individually

Filter by attributes ×

System Status	Category	Affected Nodes	Detection Time	Title	Description
Critical Active	vrfSecurity Security	candid5-leaf1	Jul 20 2018 03:43:00.000 PM	ENFORCED_VRF_POLICY_VIOLATION	VRF is in enforced mode. APIC policy for implicit deny log is not enforced on Leaf hardware.
Critical Active	vrfSecurity Security	candid5-leaf1	Jul 20 2018 03:43:00.000 PM	ENFORCED_VRF_POLICY_VIOLATION	VRF is in enforced mode. APIC policy for implicit deny log is not enforced on Leaf hardware.
Critical Active	Subnet Route Forwarding	candid5-leaf1, candid5-leaf3	Jul 20 2018 03:43:00.000 PM	BD_SUBNET_DEPLOYMENT_ERROR	A bridge domain (BD) subnet that should be deployed by APIC onto a leaf switch is not present.
Critical Active	Subnet Route Forwarding	candid5-leaf3	Jul 20 2018 03:43:00.000 PM	EXTERNAL_ROUTED_NETWORK_INTERFACE_SUBNET_DEPLOYMENT_ERROR	An interface belonging to an L3Out is not deployed on the leaf switch(es) where it is expected to be deployed.
Critical Active	Subnet Route Forwarding	candid5-leaf3	Jul 20 2018 03:43:00.000 PM	EXTERNAL_ROUTED_NETWORK_INTERFACE_SUBNET_DEPLOYMENT_ERROR	An interface belonging to an L3Out is not deployed on the leaf switch(es) where it is expected to be deployed.
Critical Active	Subnet Route Forwarding	candid5-leaf1	Jul 20 2018 03:43:00.000 PM	EXTERNAL_ROUTED_NETWORK_INTERFACE_SUBNET_DEPLOYMENT_ERROR	An interface belonging to an L3Out is not deployed on the leaf switch(es) where it is expected to be deployed.
Critical Active	Interface Forwarding	candid5-spine2	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.
Critical Active	Interface Forwarding	candid5-spine1	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.
Critical Active	Interface Forwarding	candid5-spine1	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.
Critical Active	Interface Forwarding	candid5-spine2	Jul 20 2018 03:43:00.000 PM	FABRIC_EXTERNAL_INTERFACE_OPER_DOWN_ADMIN_UP	A fabric external facing interface on the spine is administratively up but operationally down.

10 Rows   Page 1 of 192   1-10 of 1915

5. The **Anomaly Count** displays the difference in the anomaly count per severity across the two snapshots. The first count represents the anomalies found only in the earlier snapshot. The second count represents the anomalies common in both the snapshots. The third count represents the anomalies found only in the later snapshot.
6. Click the anomaly count to view the anomaly details.
7. The **Health Delta By Resources** displays the health delta across various resource types. It also displays the count of the resources with issues, unhealthy resources, and the total resources.
    a. Click resource count to view the resources associated with the resource count.
    b. Click resource name to view the anomaly details for that resource.
    c. Check **Only Show Mismatch** check-box to view the changes across the two snapshots.
8. The **Anomalies** table displays the aggregated and individual view of the anomalies.
    a. Select **Aggregated** from the drop-down menu to view the aggregated anomalies across the two snapshots.
    b. Select **Individually** from the drop-down menu to view the individual anomaly across the two snapshots.
    c. Select an anomaly to view the anomaly details. See Analyze Anomalies for more information.
9. In the **Filter bar** use the multiple filters to search for anomalies.
    a. Click the snapshot icon to filter by the snapshots such as earlier snapshot, later snapshot, earlier snapshot only, later snapshot only, both snapshots, and consolidated used for the delta analysis.
    b. Use the Filter bar to filter by resources and then by resource name or DN.
    c. The results are displayed in the **Anomalies** table. Select an anomaly to view the anomaly details.

Viewing Policy Delta Analysis for ACI

Use this procedure to view the results of the policy delta analysis for the ACI Site Group.

Procedure

1. Choose **Troubleshoot** > **Delta Analysis**.
2. From the Site Group menu, select a Site Group.
3. Select a completed analysis from the Delta Analysis table. In the summary pane, click the detail icon to view health and policy delta details.
4. Click **Policy Delta** to view the policy changes across the two snapshots. Policy Delta includes 3 panels, Changed Policy Object, Policy Viewer, and Audit Log.
5. The **Changed Policy Object** panel, displays the changed policy object tree across the two snapshots.
    a. Drill down on a particular object to view the object types that have changed. The number indicates the number of changes to the object.

   b. Select the changed object type to view the anomalies that have changed.

   c. Click DN link to access the affected object type in APIC.

   d. Click **Show Changes** to view the changes in the Policy Viewer and Audit Log panels. The corresponding changes in the Policy Viewer and Audit Log panels are highlighted.

   e. Use the **Search** bar to perform a DN search.

6. The **Policy Viewer** panel displays the policy configuration across the earlier and later snapshots. The policy configuration for the earlier snapshot is called the earlier snapshot policy. The policy configuration for the later snapshot is called the later snapshot policy.

   a. Use the color coding to visualize the added, deleted, modified, and unchanged content across the two policies.

   b. Click **Show More Code Above** or **Show More Code Below** to display more content.

   c. Click the download icon to export the snapshot policy.

   d. Enter a value in the **Search** bar to perform a text search.

7. Cisco Nexus Insights collects audit logs from APIC and computes the difference in the audit logs between the two snapshots. The **Audit Log** panel then displays all the audit logs that were created between the two snapshots. A correlated view of what has change in the datacenter is displayed in the **Audit Log** panel. When you select a particular object in the **Changed Policy Objects** panel, the relevant difference is highlighted in the **Policy Viewer** panel and the relevant audit log is highlighted in the **Audit Log** panel. APIC audit logs are records of user-initiated events such as logins and logouts or configuration changes that are required to be auditable. For every snapshot, the audit log history is limited to last 24 hrs.

   a. Use the **Search** bar to perform a DN, User ID, or text search.

   b. Click **View More** on an audit log entry to view when the changes were made and who made the changes. The timestamp on the audit log entry corresponds to the the timestamp on the APIC audit log.

   c. Click Audit Log entry to access the affected object type in APIC.

Managing Delta analysis

Use this procedure to edit and delete a delta analysis.

Procedure

1. Choose **Troubleshoot** > **Delta Analysis**.
2. From the Site Group menu, select a Site Group.
3. Select a delta analysis from the **Delta Analysis** table.
4. Click the more icon and select Edit to edit the analysis.
5. Click the more icon and select Delete to edit the analysis. To delete a delta analysis that is in progress, you must stop the delta analysis before deleting.
6. From the Status column, select an In Progress or Scheduled analysis and click **STOP** to stop the delta analysis.

7. To view the results of the delta analysis, select a delta analysis from the **Delta Analysis** table. The summary pane displays details such as general information and anomaly information.
8. Click the detail icon to view health and policy delta details.

Log Collector

The Log Collector feature enables you to collect and upload the logs for the devices in your network to Cisco Intersight Cloud. It also enables Cisco TAC to trigger on-demand collection of logs for devices on the site and pulls the logs from Cisco Intersight Cloud.

The Log Collector has two modes:

- User initiated - The user collects the logs for devices on the site and then uploads the collected logs to Cisco Intersight Cloud after the log collection job is completed. Starting from this release, you can automatically upload the log files to Cisco Intersight Cloud after the log collection job is completed.
- TAC initiated - Cisco TAC triggers on-demand collection of logs for specified devices and pulls the logs from Cisco Intersight Cloud.

Device Connectivity Notifier for TAC Initiated Collector

Nexus Dashboard Insights uses the device connectivity issue notifier on Cisco Nexus Dashboard to communicate with the devices. The notifier checks for TAC triggered on-demand collection of logs. In case the fabric is not configured properly to communicate with the device, Nexus Dashboard Insights notifies the following:

- The device is not configured for node interaction.
- You can not run a Log Collector job on the device.
- Nexus Dashboard Insights cannot connect to the device.

If the node interaction is not healthy on the device, you cannot select the device for Log Collector to collect logs. In the GUI, the device is greyed out.

Log Collector Dashboard

The **Log Collector** Dashboard displays a graph of Logs by status for a particular Site Group or site and displays the latest log collections.

The filter bar allows you to filters the logs by status, name, type, start time, and end time.

The valid operators for the filter bar include:

- `==` - display logs with an exact match. This operator must be followed by text and/or symbols.
- `contains` - display logs containing entered text or symbols. This operator must be followed by text and/or symbols.

The page also displays the log collection jobs in a tabular format. The jobs are sorted by status.

1. Select the log collection job in the table for the side pane to display additional details.
2. Click the ↗ icon to view the **Log Collection** status page. The **Log Collection** status page displays information such as status, general information, and node details.

TAC Initiated Log Collector

The TAC initiated log collector enables Cisco TAC to trigger on-demand collection of logs for specified user devices in the Cisco Intersight Cloud to the Device Connector.

1. Click **Troubleshoot** > **Log Collector**.

   When the TAC assist job is complete, the new job appears in the **Log Collector** table.

2. Select the job in the table for the side pane to display additional job details.
3. Click the ↗ icon to view the **Log Collection** status page. The **Log Collection** status page displays information such as status, general information, and node details.

Uploading logs to Cisco Intersight Cloud

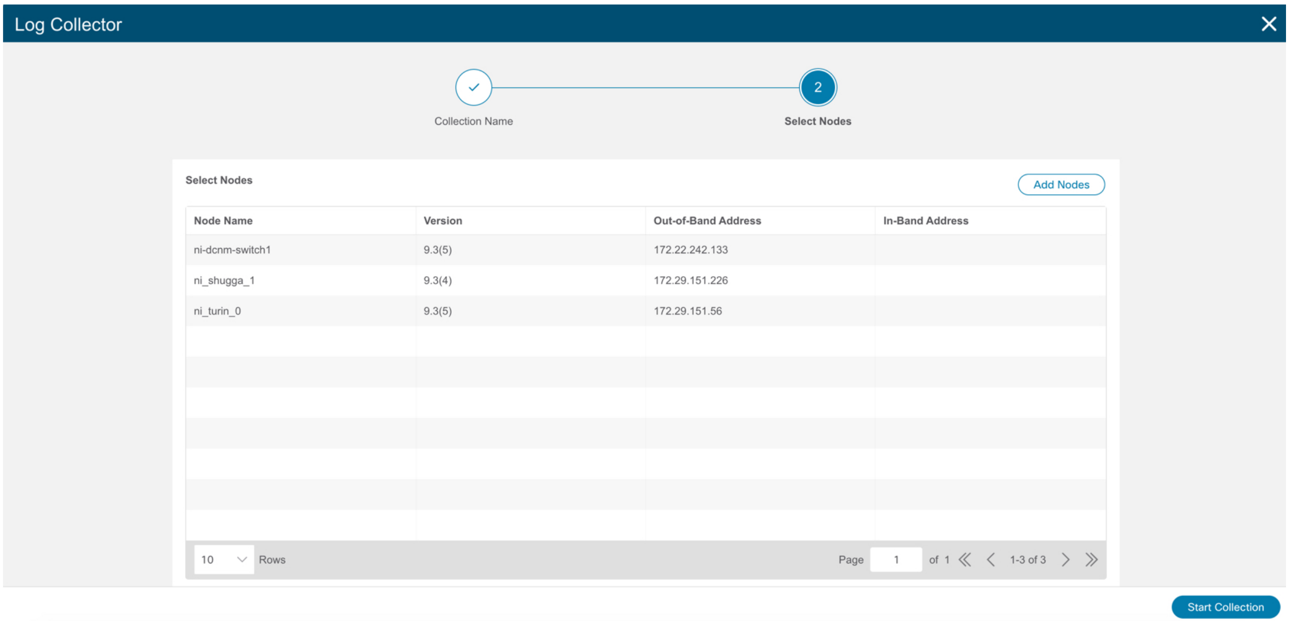
Use this procedure to upload the logs to Cisco Intersight Cloud.

Before you begin

- Ensure thatNexus Dashboard Insights is connected to Cisco Intersight Cloud.
- Ensure that Nexus Dashboard Insights is connected to Cisco Intersight Device Connector. See About Device Connector.

Procedure

1. Choose **Troubleshoot** > **Log Collector** > **New Log Collection**.
2. Enter the name.
3. Click **Select Site** to select a site.
4. (Optional) Check **Auto Upload Log Files** to automatically upload the log files to Cisco Intersight Cloud after the log collection job is completed.
5. Click **Next**
6. Click **Add Nodes** and then select the nodes from the **Select Nodes** menu.
7. Click **Add**. The nodes are displayed in the **Select Nodes** table.


Log Collector ✕

Select Nodes

Add Nodes

Node Name	Version	Out-of-Band Address	In-Band Address
ni-dcnm-switch1	9.3(5)	172.22.242.133	
ni_shugga_1	9.3(4)	172.29.151.226	
ni_turin_0	9.3(5)	172.29.151.56	

10 Rows — Page 1 of 1 — 1-3 of 3

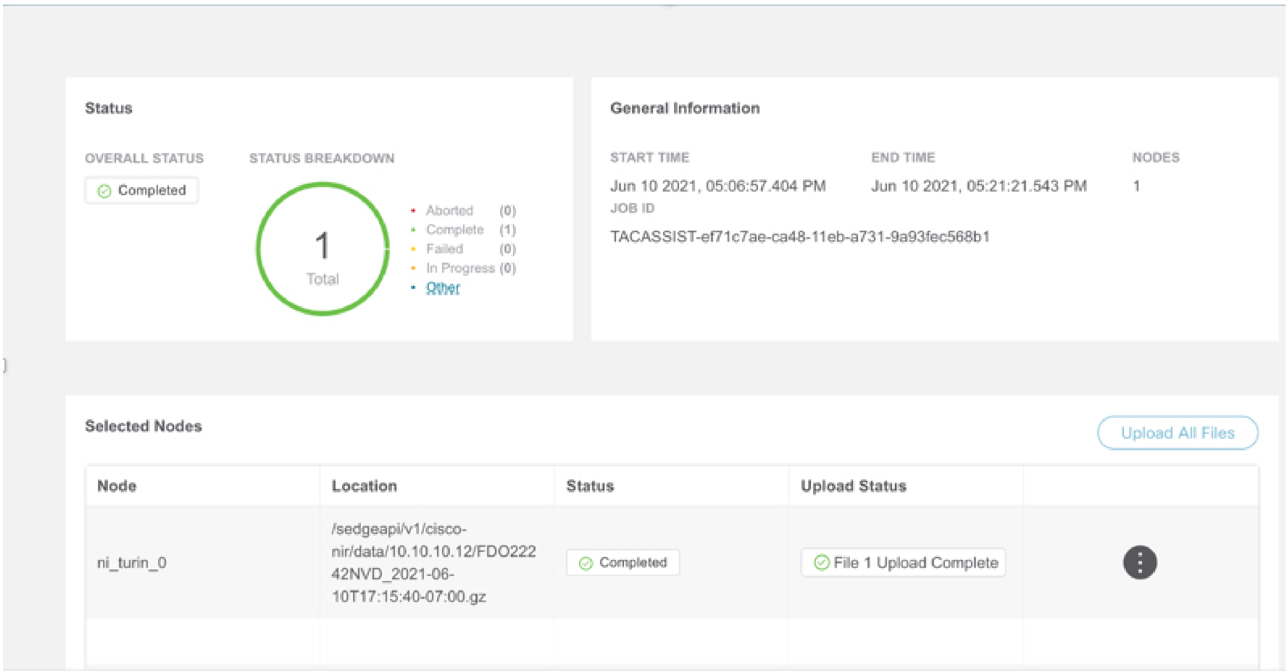
Start Collection

8. Click **Start Collection** to initiate the log collection process.

   When the job is complete, the new job appears in the **Log Collector** table.

9. Click the job in the table for the side pane to display additional job details.
10. Click the ↗ icon to display **Log Collection** status page.
11. Select the node and click ⋮ icon.
12. Click **Upload File to TAC Assist** to upload a single file for the selected node manually.
13. Click **Upload** to upload all the log files generated for the selected node manually.

    The status of the upload is displayed in the **Selected Nodes** table.


Status

OVERALL STATUS: ✓ Completed

STATUS BREAKDOWN

General Information

START TIME	END TIME	NODES
Jun 10 2021, 05:06:57.404 PM	Jun 10 2021, 05:21:21.543 PM	1

JOB ID

TACASSIST-ef71c7ae-ca48-11eb-a731-9a93fec568b1

Selected Nodes

Upload All Files

Node	Location	Status	Upload Status	
ni_turin_0	/sedgeapi/v1/cisco-nir/data/10.10.10.12/FDO22242NVD_2021-06-10T17:15:40-07:00.gz	✓ Completed	✓ File 1 Upload Complete	⋮

Guidelines and Limitations

- Log collection can be performed only on 5 nodes at a time.
- If the upload logs fails for some of the nodes and succeeds for the rest of the nodes, then in the **Selected Nodes** table, the status is displayed as Completed.
- If the collection fails for some of the nodes, then the collection will continue for other nodes. After the collection is completed, the upload will start. In the **Selected Nodes** table, the combined status is displayed in the Status column.
- If the collection succeeds for some of the nodes, but the upload fails, then in the **Selected Nodes** table, the status is displayed as Failed.
- **Auto Upload Log Files** can be performed only on one node at a time.

Browse

The Browse section of Nexus Dashboard Insights contains the following areas of statistical and analytical information:

- **Resources** —Displays utilization, rate of change, trends, and resource anomalies over time for operational, configuration and hardware resources.
- **Environmental** —Displays switch environmental resources such as fan, power, CPU, and memory.
- **Flows** —Displays telemetry information collected from various devices in the site.
- **Endpoints** —Displays endpoint for the nodes collected across the entire site.
- **Interfaces** —Displays switch nodes interface usage.
- **Protocols** —Displays protocol statistics.
- **Events** —Displays charts for event occurrences over time.

Resources

Resources in Nexus Dashboard Insights contains areas of data collection that are available in the Work pane under the **Dashboard** tab and the **Browse** tab.

Dashboard Tab

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

Click a node card in **Top Nodes by Utilization** to display the *Resource Details* page. The details include general information, resource trends for resource utilization properties, and anomalies for the resources.

Browse Tab

View, sort, and filter statistics using the **Filters** field in the **Browse** tab. You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

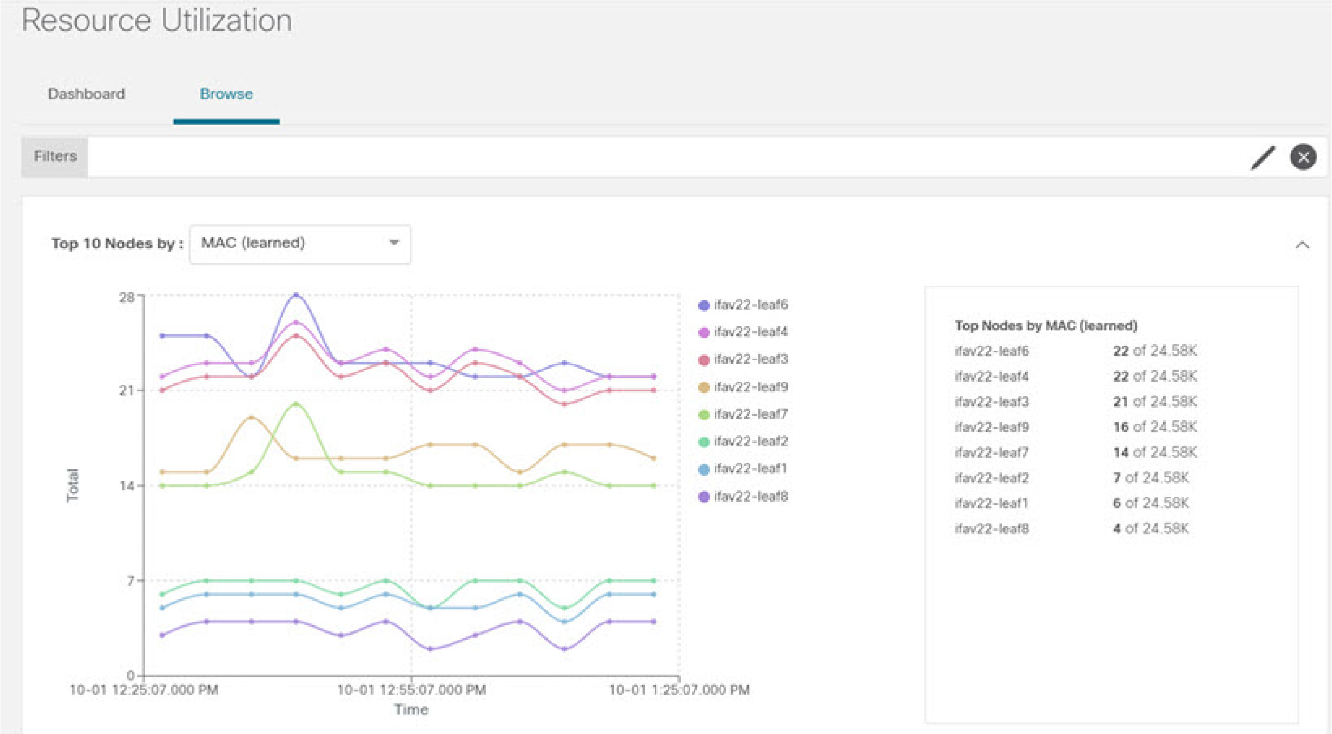
A filter refinement lets you select the filter, operator, and value. You can use the following operators:

- `==` - 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.

The following items are displayed following the **Filters** field.

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

Property	Description
Operational Resources	Displays a list of operational resources based on resource utilization. List information includes: • Anomaly Score • Node • MAC (learned) • IPv4 (learned) • IPv6 (learned) • IPv4 Host Routes • IPv6 Host Routes • Multicast Routes
Configuration Resources	Displays a list of configuration resources based on resource utilization. List information includes: • Anomaly Score • Node • VRF • BD • EPG • VLAN
Hardware Resources	Displays a list of configuration resources based on resource utilization. List information includes: • Anomaly Score • Node • Port Usage • Port Bandwidth • LPM • Policy TCAM



Top Nodes by MAC (learned)

ifav22-leaf6	**22** of 24.58K
ifav22-leaf4	**22** of 24.58K
ifav22-leaf3	**21** of 24.58K
ifav22-leaf9	**16** of 24.58K
ifav22-leaf7	**14** of 24.58K
ifav22-leaf2	**7** of 24.58K
ifav22-leaf1	**6** of 24.58K
ifav22-leaf8	**4** of 24.58K

- Click the node in the summary pane for the side pane to display additional details of the node.
- On the side summary pane, click the ⧉ icon on the right top corner to open the *Resource Details* page.
- Click the **Overview** tab.

  The Node Details page on the Overview tab displays General Information, Anomaly Score, Node Overview, and Resource Trends for resource utilization properties.

- 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, Endpoints, Events, and Environmental Resources, and Node Details for the node.

  Click a category from the list to open browse work pane for that particular node.

- The **Alerts** tab on the Node Details page displays the anomalies occurred on the node.

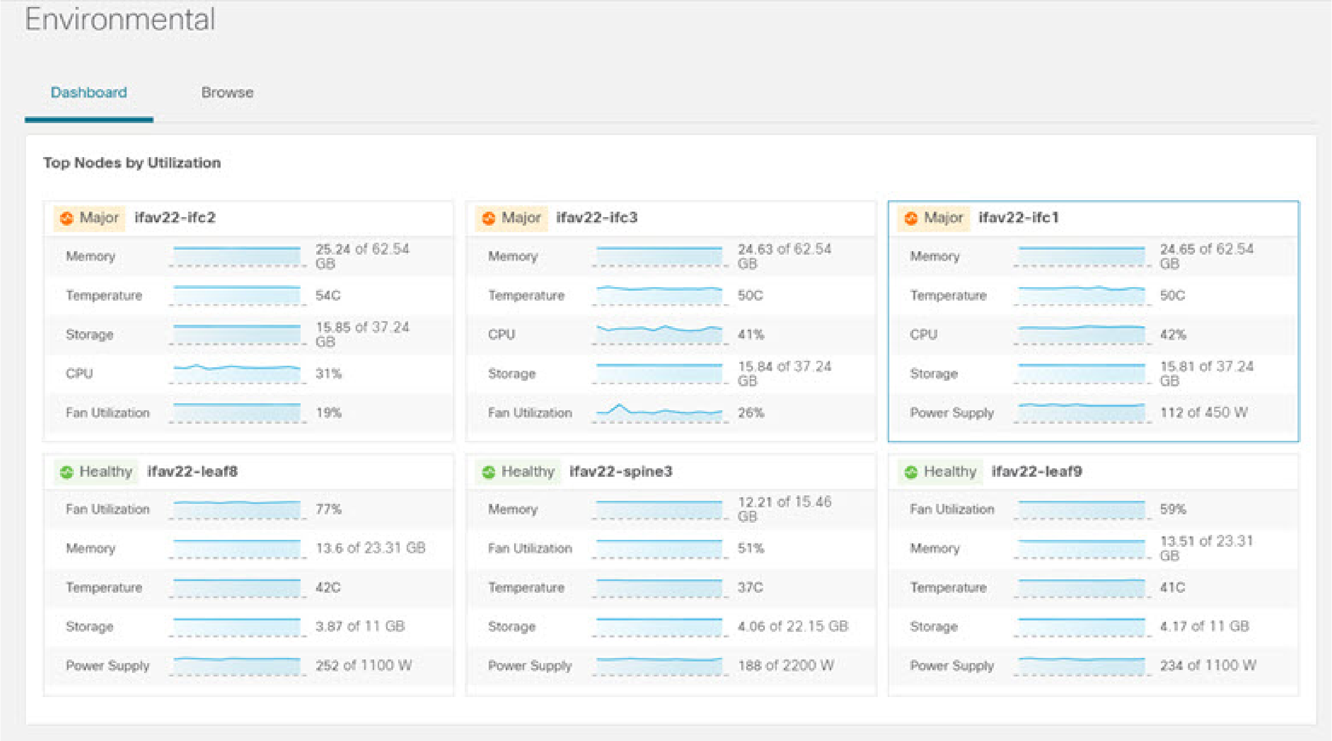
Environmental

Environmental in Nexus Dashboard Insights contains two areas of data collection that are available in the Work pane under the **Dashboard** tab and the **Browse** tab.

Dashboard Tab

The Environmental Dashboard displays utilization, rate of change, trends, and anomalies over time for switch environmental resources such as fans, power, CPU, and memory.

Property	Description
Top Nodes by Utilization	Displays the percentage utilized per component: • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage



Top Nodes by Utilization

Major ifav22-ifc2

Memory	25.24 of 62.54 GB
Temperature	54C
Storage	15.85 of 37.24 GB
CPU	31%
Fan Utilization	19%

Major ifav22-ifc3

Memory	24.63 of 62.54 GB
Temperature	50C
CPU	41%
Storage	15.84 of 37.24 GB
Fan Utilization	26%

Major ifav22-ifc1

Memory	24.65 of 62.54 GB
Temperature	50C
CPU	42%
Storage	15.81 of 37.24 GB
Power Supply	112 of 450 W

Healthy ifav22-leaf8

Fan Utilization	77%
Memory	13.6 of 23.31 GB
Temperature	42C
Storage	3.87 of 11 GB
Power Supply	252 of 1100 W

Healthy ifav22-spine3

Memory	12.21 of 15.46 GB
Fan Utilization	51%
Temperature	37C
Storage	4.06 of 22.15 GB
Power Supply	188 of 2200 W

Healthy ifav22-leaf9

Fan Utilization	59%
Memory	13.51 of 23.31 GB
Temperature	41C
Storage	4.17 of 11 GB
Power Supply	234 of 1100 W

Click a node card in **Top Nodes by Utilization** to display the *Environmental Details* page. The details include general information, resource trends for environmental properties, and anomalies for the environmental resources.

Browse Tab

View, sort, and filter statistics using the **Filters** field in the **Browse** tab. You can refine the displayed statistics by the following filters:

- Node - Display only nodes.

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

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

- `contains` - with the initial filter type, this operator, and a subsequent value, returns all that contain the value.
- `!contains` - with the initial filter type, this operator, and a subsequent value, returns all that do not contain the value.

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

- Click the node in the summary pane for the side pane to display additional details of the node.
- On the side summary pane, click the ↗ icon on the right top corner to open the *Environmental Details* page.
- Click the **Overview** tab.

  The Node Details page on the Overview tab displays General Information, Anomaly Score, Node Overview, and Resource Trends for environmental resource properties.

- 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, Endpoints, Events, and Environmental Resources, and Node Details for the node.

  Click a category from the list to open browse work pane for that particular node.

- The **Alerts** tab on the Node Details page displays the anomalies occurred on the node.

Interfaces

In the left Navigation pane, click **Browse** > **Interfaces** to view the **Interfaces** page in the Work pane.

At the top of the Work pane is the Site Group that is selected and there are 2 tabs available for viewing.

- **Dashboard** tab
- **Browse** tab

Dashboard tab

The **Dashboard** tab displays **Top Nodes by Interface Utilization** where charts are displayed based upon the nodes interface utilization.

The tab also displays **Top Nodes by Interface** where details for the top interfaces by anomalies for nodes that are of type - physical, port channel, virtual port channel (PC and vPC) interfaces, and Switch Virtual Interfaces (SVI).

The green dot next to an interface name represents the operational status and indicates that the interface is active. The red dot next to the interface name represents that the interface is inactive.

Browse tab

View, sort, and filter statistics using the **Filters** field in the **Browse** tab. 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 7. 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	The current severity level of the event. The levels are: • **Critical**—A service-affecting condition that requires immediate corrective action. For example, this severity could indicate that the managed object is out of service and its capability must be restored. • **Major**—Serious problems exist with one or more components. These issues should be researched and fixed immediately. • **Minor**—Problems exist with one or more components that might adversely affect system performance. These issues should be researched and fixed as soon as possible before they become a critical problem. • **Warning**—Potential problems exist with one or more components that might adversely affect system performance if they are allowed to continue. These issues should be researched and fixed as soon as possible before they become a critical problem. • **Info**—A basic notification or informational message, possibly independently insignificant. • **Cleared**—A notification that the condition that caused the fault has been resolved, and the fault has been cleared.
Code	The code that helps to categorize and identify different types of fault instance objects.
Last Transition	The day and time on which the severity last changed. If the severity has not changed, this field displays the original creation date.
Description	Additional descriptive information on the audit log, event or fault.

In the Work pane under the **Browse** tab, the top interfaces by different options such as Error, Transmit Utilization, Receive Utilization are displayed.

> If you choose an option from the following items: **Error**, **Transmit Utilization**, **Receive Utilization**, and if you have selected a snapshot older than 3 days and the time range is less than or equal to 1 hour, the **Top Interfaces** area in the **Browse** tab will not be populated.

The **Interfaces** table provides information such as Anomaly Score, Interface, Interface Type, Node, L2 Neighbors, Logical Neighbors, Receive Utilization, Transmit Utilization.

Single-click a row in the **Interface** page for the sidebar to display on the right with details about the specific interface.

Double-click each row in the **Interfaces** page to display the **Interface Details** page that has further details about the interface. This page has the following tabs:

- **Overview**:
- **Alerts**::
- **Protocols**:
- **Neighbors**:

Under the **Overview** tab, **General Information** area, you see the general information about your interface. In the **Trends** area, you see information about the traffic that is flowing over the interface and the usage. In the **Statistics** area, you can see various statistics for QoS, DOM, and Microbursts.

Under the **Alerts** tab in this page, the anomalies are displayed.

Under the **Protocols** tab, if a protocol is enabled on an interface, the details are displayed.

Under the **Neighbors** tab, there are two types of neighbors.

- L2 Neighbors: In this area, details are displayed such as Name, Peer Interface Name, Peer Device Type, Platform Information, Peer Management IP, Peer Node ID.
- Logical Neighbors: In this area, details are displayed such as Peer IP, Operational State, Protocol Name, VRF Name, Neighbors Type.

> An interface must be active for you to be able to view the neighbor details.

Supported Interface Types

Physical Interface: Double-click the type **Physical** to view the 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.

Port Channel 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 an additional set of objects that gives the admin-status, oper-status and list of member interfaces for both PC and vPC.

vPC Interface: The vPC is a logical interface that spans across two physical switches for fault tolerance. Double-click each row in the **Interfaces** page, to display the **Interface Details** page which summarizes the 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. For a vPC interface type, the **Logical Neighbors** information is also displayed. The categories that are supported are L3Out, IPN, ISN, L4-L7.

SVI Interface: An SVI is a virtual routed interface that connects a VLAN on the device to the Layer 3 router engine on the same device. Specific information such as Member Interfaces over which the SVI is deployed, VLAN ID, VLAN Type, Encap VLAN are displayed for the SVI interface.

Interface Limitations

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

Microburst Support for Interface Statistics

A burst of traffic impacts the output buffer of a physical interface port given the channel is already subscribed with line-rate flows.

These bursts are often hard to detect with just given queuing parameters, such as buffer cells used and buffer cells unused as there is a high variance of usage of these buffers.

The Cisco Nexus 9000 series switches provide a capability of detecting this by issuing an interrupt that is triggered when a queue occupancy rises above *x* bytes and falls below *y* bytes. This *x _& _y* bytes are configurable per queue per interface. You can configure up to 8 output queues per physical interface port.

When the UTR software collector receives a GRPC telemetry stream for the path `show queuing burst-detect detail`, according to the parser for the encoding path, data is formatted, and it's written to the telemetry output topic of Kafka.

Configuring and Monitoring Microburst

In Nexus Dashboard Insights, to configure Microburst, perform the following actions:

1. In the **Overview** page, choose the appropriate Site Group and click the Actions menu > **Configure Site Group**.
2. In the **Configure Site Group** page, in the **Microburst Configuration** area, for the appropriate Site Name, click the drop-down menu for **Microburst Sensitivity**. The default value is **Disable**. Choose the value appropriate that you want to configure. The other values are **Set High Sensitivity** and **Set Low Sensitivity**.

Based on the percentage of threshold, a microburst is either low, high, or medium. The percentage of threshold is inverse to sensitivity. When the number of microbursts are greater than 100 on a particular interface, an anomaly is raised. Nexus Dashboard Insights collects the microburst data for the selected sites. Microburst anomalies are raised on the interface of the node.

See also, Micro-Burst Monitoring for details.

Supported Platforms

See Supported Platforms for details.

Microburst Anomaly

Anomalies are raised in Nexus Dashboard Insights based on the number of microbursts at the interface level. Microburst anomaly jobs run every 5 minutes in a container environment, which checks for microburst records in microburst database. If the number of microbursts per interface is greater than `microburst count threshold` at any given point of time, then a minor anomaly is raised per interface in a node. At that point any anomaly record is written to Elasticsearch.

Nexus Dashboard Insights raises these anomalies in the **Browse** > **Interfaces** page.

1. The flows that are displayed in the summary table are gathered from Flow Telemetry data for a corresponding egress interface. Nexus Dashboard Insights matches the egress interface and egress queue to gather the corresponding microburst.
2. Based on the percentage of threshold, microburst is either low, high, or medium. The percentage of threshold is inverse to sensitivity. When the number of microbursts are greater than 100 on a particular interface, an anomaly is raised.
3. If flow telemetry is enabled and microburst is also enabled, then Nexus Dashboard Insights displays the estimated impact of flows for a particular microburst anomaly.
4. If the flow telemetry is disabled and microburst anomaly is enabled, then Nexus Dashboard Insights displays no **Estimated Impact** for that anomaly.
5. Flows that are contributing or impacted by microburst.

Browse Microburst Anomaly

To browse microburst anomalies, make sure flow telemetry is enabled and flow rules are configured on the site. The flows are available in the summary table when the flow rules are configured.

On the Interfaces summary pane:

1. Click the anomaly to display the side pane with additional details.
2. Click **Analyze**.
3. The detailed view page summarizes the flows that are impacted, mutual occurrences, lifespan, and recommendations.

> Starting from Nexus Dashboard Insights release 6.0, the content *The identified X flows are the top X with large max burst values, which may indicate heavier buffer usage by these flows* is not displayed in the Recommendations area.

a. Click the **Affected Object** in the side pane to display the *Interface Details* for the node. The page displays the interface details, number of bursts, time stamp, aggregated flow details, and top 25 microbursts by peak value.

b. Click **View Report** for top 100 flows contributing or impacted by microburst.

c. In the *Affected Entities* side view pane, select a flow and click ⧉ to display the flow details page.

Protocols

The Browse section of Nexus Dashboard Insights displays protocol information for the top interfaces by anomalies for nodes that are of type CDP, LLDP, LACP, BGP, PIM, IGMP, and IGMP Snoop protocols. This page also displays node name and *Count* which is 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 in the **Protocols** page for the sidebar to display additional details for that specific node.
- 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 interfaces, admin state, operational state, packets transmitted, packets received, neighbors, and errors.

Protocol Statistics Anomaly Detection

The protocol statistics counters are monitored for anomaly detection and are based upon the scheme mentioned below for how the respective anomalies are raised. The anomalies are raised on a counter that is specific to a source (for example interface) within a node. The anomaly detection algorithm works by calculating the Exponential Weighted Moving Average (EWMA) for every instance of the counter that is being monitored. Periodically, the EWMA is updated and the update is based on 90% weight to the existing EWMA + 10% weight to the new incoming value of the counter. The periodicity of the update is 1-minute. For the first 30-periods, the data is collected and EWMA is allowed to become stable. During this period anomaly is not generated. The stability period is when the service is started at which time the EWMA calculation begins for all counters. In addition, if a new node comes alive during operation of the fabric the counters of that node will go through the stability period to build EWMA. The EWMA calculation for that new node's counters is also 30-periods. The EWMA is compared with the incoming value to detect anomalies.

Two types of anomalies are processed on the protocol statistics counters.

Threshold-Based Anomaly. The utilization counters such as **InterfaceUtilizationIngress** and **InterfaceUtilizationEgress** are monitored for the utilization of the interface. A maximum utilization threshold is defined. If the utilization crosses a critical threshold, a threshold anomaly is raised. When the utilization falls below the threshold, the anomaly is cleared. Changed detection anomaly is based on EWMA. The EWMA for every counter is continuously updated every minute by the **predictor** service by querying the **statsdb** for the new value. The **change detection anomaly** is applied on the following counters.

Rate-of-Change Anomaly: If there is an increase or a decrease of bandwidth usage by more than 10% for 3-continuous detection periods (3 minutes, because the data is updated every minute), then a utilization **Rate-of-Change** anomaly is raised. The anomaly is cleared when the rate-of-change falls below 10%. The error-counter anomaly detection is used to flag detection of errors in any of the protocol counters. The list of error counters monitored are given in the table below. The error counters are monitored by the **predictor** service. If the error counter increases at least by a value of **1** for three continuous detection periods, then the corresponding error-anomaly will be raised. If the error is present for 5-periods, then the anomaly with **warning** will be raised. If the anomaly persists for 30-periods, then it will be changed to **major**. One period refers to 1-minute of wall clock time.

Table 8. Monitored Error Counters

Protocol Counter	Anomaly Detection Method	Thresholds	Severity	Anomaly Type
InterfaceUtilizationIngress InterfaceUtilizationEgress	Monitor whether the utilization crosses the specified threshold	is > 90%	Critical	high_threshold
InterfaceUtilizationIngress InterfaceUtilizationEgress	Monitor whether the new value is greater than or less than the EWMA by more than 10%.	rate of change > 10%	Warning	high_rate_of_change

Protocol Counter	Anomaly Detection Method	Thresholds	Severity	Anomaly Type
Protocol Errors. The specific protocol counters monitored for error are as follows: -interfaceForwardingDropIngress -interfaceAfdDropEgress -interfaceBufferDropIngress -interfaceBufferDropEgress -interfaceErrorDropIngress -interfaceErrorDropEgress -interfaceCrc -interfaceIngressError -interfaceEgressError -interfaceIngressDiscard -interfaceEgressDiscard -lldpFlaps -lacpFlaps	Monitor whether the counter value has increased in the last 5 minutes.	error-increase > 0	Major	error
interfaceStomped	Monitor whether the counter value is increasing and that none of the interfaceStomped counters are increasing in the neighbor node for this port.	error-increase > 0	Major	error

Anomaly Detection for Routing Protocols Received Paths

Nexus Dashboard Insights monitors changes in the BGP peer prefix received counts and calculates the percentage of variance in the last 5 minutes. If the percentage of variance is greater than 10%, Nexus Dashboard Insights generates an anomaly, and the anomaly type is **hige_rate_of_change**.

Multicast Protocols

The Browse Statistics dashboard displays protocols 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.

Flows

Flows 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.

The Flows section of Nexus Dashboard Insights displays the telemetry information collected from various devices in the site that were added to the site.

For details on Flow Telemetry support for Cisco Nexus series switches and line cards, see Nexus Dashboard Insights Release Notes, **Compatibility Information** section.

Flows in Nexus Dashboard Insights contains two areas of data collection that are available in the Work pane under the **Dashboard** tab and the **Browse** tab.

Flows Guidelines and Limitations

- Nexus Dashboard Insights 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.
- A maximum of 63 VRFs are supported on flow telemetry nodes.
- Flows is not supported for Endpoint Security Groups.
- Bridged and L3Out-to-L3Out flows are not reported from spine switch.
- For flows, if the time range you have selected is greater than 6 hours, the data may not get displayed. Select a time range that is less than or equal to 6 hours.

Limitations for Flows on **Cisco Nexus EX** switches.

For details on Flow Telemetry hardware support, see Nexus Dashboard Insights 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 Flows. This information is fetched from the software and not from the EX ASIC.
- For L3Out external EPGs; EPG names, Buffer drop anomaly, Forwarding drop anomaly, and QoS policing drop anomaly are not supported.
- Cisco Nexus 9300-EX platform switches do not support VRF based filtering. They support only bridge domain or subnet filtering of flow telemetry rules. Nexus Dashboard Insights gets the flows from the subnet if the subnet is across multiple VRFs.
- Tier-1 leaf switches do not export flow telemetry data from remote leaf switches to sub-leaf switches.

Limitations for Flows 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 Nexus Dashboard Insights flow path summary will be incomplete.
- Nexus Dashboard Insights 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), Nexus Dashboard Insights shows Ingress IP size of 1050 bytes and Egress IP size of 1108 bytes. For IPv4 intra-leaf traffic Nexus Dashboard Insights shows both Ingress and Egress IP size of 1050 bytes.
  - For IPv6 inter-leaf node traffic (with spine node), Nexus Dashboard Insights shows Ingress IP size of 1070 bytes and Egress IP size of 1128 bytes. For IPv4 intra-leaf traffic Nexus Dashboard Insights shows both Ingress and Egress IP size of 1070 bytes.

- Flow telemetry and flow telemetry events will not export `drop bit` if there is an egress ACL drop in the switch.
- Locally switched traffic in the same node, with shared services will not have information on the destination VRF or Tenant and EPG.
  - This is valid for both EPGs and ExtEPGs.
  - Shared services also encompasses the case of EPGs in the same VRF but different tenants.

Extending Flows to Cisco ACI Tier-3 Topologies in Nexus Dashboard Insights

Flows implements 3-tier topology where a second tier of leaf nodes are connected to first tier of leaf nodes. In the 3-tier topology when flow packet traverses from one host to the other using multiple tiers, before they reach the destination host, the packet becomes an iVXLAN packet when it traverses through a tier-1 leaf node.

Guidelines and Limitations

- The Cisco APIC Release 4.2(4o) does not support a leaf node exporting flow telemetry in case of iVXLAN packet, resulting in an incomplete flow path and inadequate information to stitch together all the flows.

Flows Dashboard

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

Property	Description
Top Nodes by	The flows 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.

Property	Description
Top Nodes by Flow Anomalies	Flow telemetry and analytics gives in-depth visibility of the data plane. Flows 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.

On the **Overview** tab, the *Aggregated Flow* section displays in-depth analysis of flow anomalies including source, destination, Ingress, and Egress details.

The *Path Summary* section describes the source IP and destination IP address for the node with anomaly.

On the **Alerts** tab, the *Anomalies* section summarizes the anomaly detection details.

On the **Trends** tab, The *Related Details* section displays anomaly analysis with the comparison charts for each flow property against time.

Browse Flows Records

The Browse Flows 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 flows properties recorded in the entire site. The node flows recorded for Top Sources and Top Destinations are also shown.

Property	Description
Filters	Display the node flow observations using the following filters: • Record Time • Nodes • Flow Type • Protocol • Source Address • Source Port • Destination Address • Destination Port • Ingress Node • Ingress Tenant • Ingress EPG • Egress Node • Egress Tenant • Egress EPG

Property	Description
Site Flows by	A time series plot for flows 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 **Top Sources** and **Top Destinations** are also shown. • **Anomaly Score**—The score is based on the number of detected anomalies logged in the database. • **Packet Drop Indicator**—The flow records are analyzed for drops. The primary method of detecting drops is based on the drop bit received from the switch (flow records). • **Latency**—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. • **Flow Move Indicator**—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.

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.

Flow Telemetry Events

Flow telemetry events are enabled implicitly when flow telemetry is enabled. The flow telemetry enables triggering events when a configured rule is met, where packets are exported to the collector for analysis.

Flow telemetry events enhance and complement current flows in Nexus Dashboard Insights. They enrich anomaly generation for flow telemetry and flow telemetry events.

It monitors security, performance, and troubleshooting. This is achieved using the periodic flow table event records exported every second.

The data export to Nexus Dashboard Insights is done directly from the hardware without control plane needing to handle the data. Statistics are assembled as a packet with a configurable MTU size and a defined header. These packets are sent as in-band traffic from Cisco ACI fabric. Headers are configured by software, and packets streamed are UDP packets.

When flow telemetry is available for a triggered flow telemetry event, then you can navigate to flow details page for aggregated information. These events are based on the following drop events:

- **Buffer Drop**—When the switch receives a frame and there are no buffer credits available for either ingress or egress interface, the frame is dropped with buffer. This typically hints at a congestion in the network. The link that is showing the fault could be full or the link containing the destination may be congested. In this case a buffer drop is reported in flow telemetry events.
- **Forward Drop**—The packets that are dropped on the LookUp block (LU) of the Cisco ASIC. In a LU block a packet forwarding decision is made based on the packet header information. If the packet is dropped, forward drop is counted. There may be a variety of reasons when forward drop is counted.
- **Policy Drop**—When a packet enters the fabric, the switch looks at the source and destination EPG to check for a contract that allows this communication. If the source and destination are in different EPG's, and there is no contract that allows this packet type between them, the switch drops the packet and labels it as SECURITY_GROUP_DENY. This increments the forward drop counter. In this case a policy drop is reported in flow telemetry events. A policy drop occurs because of missing contracts to allow the communication.
- **Policing Drop**—When packets are dropped due to policer configured at the EPG level or on the ingress interface, then a policing drop anomaly is reported in flow telemetry events.
- **IDS Drop**—The header errors we detected in parser for IDS such as header `cksum` error, IP length mismatch, `CFG_ft_ids_drop_mask`, `zero DMAC` and so on for both inner and outer headers if applicable. The IDS error codes are detected and translated, which are reported as IDS drop anomalies in flow telemetry events.
- **RTO Inside**—When a TCP retransmission happens for a flow due to a drop inside the fabric, an RTO inside anomaly is raised. This anomaly is aggregated across flows based on destination IP and egress VRF.
- **RTO Outside**—When a flow experiences TCP retransmission, but there is no drop inside the fabric for that flow, then an RTO outside anomaly is raised. This anomaly is aggregated across flows based on destination IP and egress VRF.

Flow Telemetry Events Vs Flow Telemetry

- The flow telemetry event packets are exported only when configured events occur, where as flow telemetry packets are streamed continuously.
- The flow telemetry events are captured for all traffic, where as flow telemetry is captured for filtered traffic.
- The total number of collectors between flow telemetry and flow telemetry events is 256.

Guidelines and Limitations for Flow Telemetry Events

- The flow telemetry events do not report policing drop anomalies in Nexus Dashboard Insights app, when the egress data plane policer is configured on front-panel ports and there is traffic drop.
- To export flow telemetry events on FX platform switches, you must configure flow telemetry

filters.

Browse Flow Telemetry Events

1. Click **Analyze Alerts** > **Anomalies** to browse anomalies.
2. Filter by Category == Flows
3. Click the anomaly with Resource Type **flowEvent**.
4. Click **Analyze** on the side pane to display additional details of the anomaly.
5. See the description of the anomaly for packet drop, TCP packet retransmission, policy drop, forward drop, and cumulative drop count.

   The *Analyze Anomaly* page displays the estimated impact, recommendations, and mutual occurrences. The estimated impact displays the flows affected.

   a. Click **View Report** for the side pane to display list of flows, number of packets dropped or impacted over time, affected interfaces, in-depth analysis of drop flow events per interface, and buffer drop anomalies. Every flow telemetry drop event shows the interface affected.
   b. The *Recommendations* section displays the flows that cause the buffer drop, flow details, and flow telemetry events at the node level.

Endpoints

The Endpoints section of Nexus Dashboard Insights contains endpoint information, charts, and history for the nodes with endpoint anomalies collected across the entire Cisco ACI site.

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

- The endpoints present on the leaf switches - browse Endpoints 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 and discover configuration and operational information of the endpoint.

The following anomalies are detected as part of Endpoints:

- Rapid endpoint moves across nodes, interface, and endpoint groups
- Missing endpoints that fail to get learnt after a node reboot
- Endpoints that have duplicate IP addresses
- Spurious endpoints

Endpoints in Nexus Dashboard Insights contains two areas of data collection that are available in the Work pane under the **Dashboard** tab and the **Browse** tab.

Endpoints Dashboard

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

Property	Description
Top Nodes by Number of Endpoints	Displays the top nodes based on the number of active endpoints.
Top Nodes by Endpoint Anomalies	Displays the 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.

Endpoints Browse Tab

Navigate to the **Browse** page as follows:

1. Choose the appropriate Site Group in the **Overview** page.
2. Choose the appropriate snapshot in the timeline.
3. In the left Navigation, click **Browse** > **Endpoints**.
4. In the Work pane, click the **Browse** tab in the **Endpoints** page.

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

- 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.
- Or, Click an endpoint in the summary table to display a sidebar with general information, configuration, and operational details of the endpoint.
- Click the ↗ Details icon on the right top corner of the sidebar to display the *Endpoint Details* page.

Endpoints Filters

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

View, sort, and filter statistics using the **Filters** field in the **Browse** tab. You can refine the displayed statistics by the filters.

Use the **Filter** field to refine the endpoints by choosing from 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.
- Search deleted IPs - Displays IP addresses that have been deleted.
- Interface - Display only interfaces.
- IP address/Hostname - Display nodes with IP address and hostname.

> Hostname support is a BETA feature. We recommend that you use features marked as ‘Beta’ in your test environments but not in production deployments.

- 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.

In the **Top 5** dropdown field, you can choose an option that models a graph based on your selection, and the graph displays the endpoints count with a timeline. You can also use the **Filter** field in the page to specify a particular item to search.

In the table in the **Endpoints** page, content is filtered based on your filtering. You can click items to view further details. For example, click a MAC address for an endpoint to open the sidebar that describes details about the specific endpoint. Click the Details icon in the sidebar to open the **Endpoint Details** page and view the details under **General Information** and **IP History** areas.

Endpoints Details

This page also lists the *Endpoint History*, *IP History*, and *Duplicate Endpoints*.

The *Endpoint History* lists in decreasing 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 *IP History* lists the history based on a given IP address. The **Routing Table** shows where the BDs in the fabric are deployed.

ℹ For the ACI site, when you click an IP address and then navigate to the IP Details page by clicking the Detail icon in the sidebar, there is a **Routing Table** available that displays the location of the subnets deployed on a particular node in the site.

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.

The *Alerts* tab displays the summary of the anomalies that occur on the nodes for the selected endpoint. Click an anomaly in the summary table to display a sidebar with anomaly details.

- Click **Analyze** for the anomaly details page to display the Lifespan, estimated impact, recommendations, mutual occurrences, and in-depth analysis of the anomaly.
- Hover over the anomalies, faults, events, and Audit Logs in the mutual occurrences graph. Click on them for detailed analysis of mutual occurrences of the anomaly.
- In the *In-Depth Analysis* section click **Configure Analysis**. See Analyze Anomalies for details.

Endpoints Guidelines and Limitations

- Endpoints is not supported for endpoint groups when `allow-micro-seg` and `useg epgs` 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.
- Endpoints is not supported for Policy Based Redirect graph deployed in your network.
- Endpoints is not supported for dot1Q tunnel.
- Endpoints is not supported for Endpoint Security Groups.
- Endpoint-streaming MOs (managed objects) will not be removed after a force disable of Cisco Nexus Dashboard Insights. To post new MOs, the workaround is to disable and then enable the site from Cisco Nexus Dashboard Insights.

Events

The Events section of Nexus Dashboard Insights displays charts for event occurrences information for top switch nodes.

Dashboard Tab

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

Property	Description
Events by time	Displays all audit logs, events, and faults over a timeline chart. To modify the timeline, go to Time Range at the top of the work pane.

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

Browse Tab

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.

As a filter refinement, use the following operators:

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

Property	Description
Audit Logs by Action	Displays audit logs by: • Deletion • Creation • Modification

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

Browse Audit Logs, Events and Faults

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

- Click the event in the summary pane for the side pane to display additional details of the event.
- Click the ↗ on the right top corner of the summary pane.
- The details page on the *General* tab displays general information, diagnostics, and change set.
- The *Timeline* tab displays a graph with faults, events, and audit logs that occurred for the chosen time interval. Hover over the dots in the graph for additional details. The summary table describes the faults, events, and audit logs for the chosen time interval.

Configure Flows

Flow Telemetry

Flow telemetry allows users to see the path taken by different flows in detail. It also allows you to identify the EPG and VRF of the source and destination. You can see the switches in the flow with the help of flow table exports from the nodes. The flow path is generated by stitching together all the exports in order of the flow.

Flow telemetry monitors the flow for each site separately, as there is no stitching across the sites in a sites group. Therefore, flow telemetry is for individual flows. For example, if there are two sites (site A and site B) within a sites group, and traffic is flowing between the two sites, they will be displayed as two separate flows. One flow will originate from Site A and display where the flow exits. And the other flow from Site B will display where it enters and where it exits.

Flow Telemetry Guidelines and Limitations

- Ensure that you have configured NTP and enabled PTP on Cisco APIC. See Cisco Nexus Dashboard Insights Deployment Guide for more information.
- Starting with Cisco Nexus Dashboard Insights release 6.0.1, all flows are monitored as a consolidated view in a unified pipeline for site types ACI and DCNM, and the flows are aggregated under the same umbrella.
- Even if a particular node (for example, a third party switch) is not supported for Flow Telemetry, Cisco Nexus Dashboard Insights will use LLDP information from the previous and next nodes in the path to identify the switch name and the ingress and egress interfaces.
- The toggle buttons can be enabled for Flow Telemetry and Netflow by the user if desired. It is recommended that you enable either one of the options.
- Flow telemetry supports the following:
    - 20,000 unique flows/s [physical standard]
    - 10,000 unique flows/s [physical small]
    - 2,500 unique flows/s [vND]
- Make sure you do not have any native or leaked default routes in the `mgmt:inb vrf` managed object because this can prevent the flow from being forwarded from the spine switch.
- The following Cisco Nexus 9000 ACI-Mode Switches versions are not supported with Nexus Dashboard Insights Flow Telemetry:
    - 14.2(4i)
    - 14.2(4k)
    - 15.0(1k)

    If you enable Flow Collection for a Site Group that contains 1 or more unsupported switches, the status of Flow is displayed as **Disabled**. After you upgrade the switches to a supported version, the the status of Flow is displayed as **Enabled**.

Configure Flow Telemetry

Configure Flow Telemetry as follows.

1. In the **Overview** screen, at the top, choose your Site Group.
2. Click the Actions menu next to it and choose **Configure Site Group**
3. In the **Configure Site Group** page, click **Flows**.
4. In the **General** tab, locate the appropriate site and click the Edit icon. (The **General** tab table displays the site name and whether the flow collection is enabled or disabled.)
5. In the **Edit Flow** page, in the **Flow Collection Modes** area, enable the **Flow Telemetry** button All the flows are disabled by default. The sFlow button will remain grayed out as it is not supported for ACI type.
6. Click **Save**.
7. In the **Flow Telemetry Rules** area, the filters are displayed.
8. To add a rule, click the **Add** link and choose the rule Name, Tenant, VRF details as desired, and click the checkmark.
9. Next in the **Rule Subnets** area, add the subnet.
10. In the **Rule Subnets** field, enter the source and destination IP addresses. If you have endpoints that are under the same endpoint groups, then you can provide a rule to monitor the subnet.)
11. Click **Save**

This enables the rule for the Flow Telemetry process to begin.

Monitoring the Subnet for Flow Telemetry

For Flow Telemetry, you monitor the subnet as follows.

In the following example, the configured rule for a flow monitors the specific subnet provided. The rule is pushed to the site which pushes it to the switches. So, when the switch sees traffic coming from a source IP or the destination IP, and if it matches the subnet, the information is captured in the TCAM and exported to the Cisco Nexus Dashboard Insights service. If there are 4 nodes (A, B, C, D), and the traffic moves from A > B > C > D, the rules are enabled on all 4 nodes and the information is captured by all the 4 nodes. Cisco Nexus Dashboard Insights stitches the flows together. Data such as the number of drops and the number of packets, anomalies in the flow, and the flow path are aggregated for the 4 nodes.

1. In the left Navigation, click **Browse** > **Flow Analytics**, and click the **Dashboard** tab.
2. Verify that your **Sites Group** and the **Snapshot** values are appropriate. The default snapshot value is 15 minutes. Your selection will monitor all the flows in the chosen Sites Group.
3. Click the **Browse** tab in the page, to view a summary of all the flows that are being captured based on the snapshot that you selected.

The related anomaly score, record time, the nodes sending the flow telemetry, flow type, ingress and egress nodes, and additional details are displayed in a table format. If you click a specific flow in the table, specific details are displayed in the sidebar for the particular flow telemetry. In the sidebar, if you click the Details icon, the details are displayed in a larger page. In this page, in addition to other details, the **Path Summary** is also displayed with specifics related to source and destination. If there are flows in the reverse direction, that will also be visible in this location.

For a bi-directional flow, there is an option to choose to reverse the flow and see the path summary displayed. If there are any packet drops that generate a flow event, they can be viewed in the Anomaly dashboard.

See Analyze Alerts for details about anomalies and alerts.

Netflow

Netflow is an industry standard where Cisco routers monitor and collect network traffic on an interface. Starting with Cisco Nexus Dashboard Insights release 6.0, Netflow version 9 is supported.

Netflow enables the network administrator to determine information such as source, destination, class of service, and causes of congestion. Netflow is configured on the interface to monitor every packet on the interface and provide telemetry data. You cannot filter on Netflow.

Netflow in Nexus series switches is based on intercepting the packet processing pipeline to capture summary information of network traffic.

The components of a flow monitoring setup are as follows:

- Exporter: Aggregates packets into flows and exports flow records towards one or more collectors
- Collector: Reception, storage, and pre-processing of flow data received from a flow exporter
- Analysis: Used for traffic profiling or network intrusion
- The following interfaces are supported for Netflow:

Table 9. Supported Interfaces for Netflow

Interfaces	5 Tuple	Nodes	Ingress	Egress	Path	Comments
Routed Interface/Port Channel	Yes	Yes	Yes	No	Yes	Ingress node is shown in path
Sub Interface/Logical (Switch Virtual Interface)	Yes	Yes	No	No	No	No

Netflow Types

Currently, Full Netflow type is supported with Cisco Nexus Dashboard Insights.

With Full Netflow, all packets on the configured interfaces are captured into flow records in a flow table. Flows are sent to the supervisor module. Records are aggregated over configurable intervals and exported to the collector. Except in the case of aliasing (multiple flows hashing to the same entry in the flow table), all flows can be monitored regardless of their packet rate.

Netflow Guidelines and Limitations

- For Cisco Nexus Dashboard Insights with ACI type, it is recommended that you enable Flow Telemetry. If that is not available for your configuration, use Netflow. However, you can determine which mode of flow to use based upon your fabric configuration

- Netflow, in Cisco Nexus 9000 series switches, supports a small subset of the published export fields in the RFC.
- Netflow is captured only on the ingress port of a flow as only the ingress switch exports the flow. Netflow cannot be captured on fabric ports.
- For Netflow, Cisco Nexus Dashboard requires the configuration of persistent IPs under cluster configuration, and 7 IPs in the same subnet as the data network are required.
- After you enable Netflow in Nexus Dashboard Insights, you must obtain the Netflow collector IP address and configure Cisco APIC with the collector IP address. See Cisco APIC and NetFlow.

  To obtain the Netflow collector IP address, click the Actions menu next to the Site Group in the **Overview** page and choose **Configure Site Group**. In the **Configure Site Group** page, click **Flows**. In the **Flows** page, click **View** in the **Collector List** column.

Configure Netflow

Configure Netflow as follows.

1. In the **Overview** screen, at the top, choose your Site Group.
2. Click the Actions menu next to it and choose **Configure Site Group**
3. In the **Configure Site Group** page, click **Flows**.
4. In the **General** tab, locate the appropriate site and click the Edit icon. (The **General** tab table displays the site name and whether the flow collection is enabled or disabled.)
5. In the **Edit Flow** page, in the **Flow Collection Modes** area, enable the **Netflow** button. All the flows are disabled by default. The sFlow button will remain grayed out as it is not supported for ACI type.
6. Click **Save**.

This enables the Netflow process to begin.

Firmware Update Analysis

Firmware Update Analysis

Before performing an upgrade there are multiple validations that need to be performed. Similarly after an upgrade process, multiple checks helps to determine the changes and the success of the upgrade procedure.

The Firmware Update Analysis feature suggests an upgrade path to a recommended software version and determines the potential impact of upgrade impact. It also helps with the pre-upgrade and post-upgrade validation checks.

The Firmware Update Analysis feature offers the following benefits:

- Assists in preparing and validating a successful upgrade of the network.
- Provides visibility on the pre-upgrade checks.
- Provides visibility on the post-upgrade checks and the status after the upgrade.
- Minimizes the impact to the production environment.
- Provides visibility if the upgrade process is a single step or multiple steps.
- Displays the bugs applicable to a specific firmware version.

Guidelines and Limitations

Before running a post-upgrade analysis, ensure that all the nodes are already upgraded.

Creating New Firmware Update Analysis

Use this procedure to create a new firmware update analysis.

Procedure

1. Choose **Change Management** > **Firmware Update Analysis**.
2. From the Site Group menu, select a Site Group or site.
3. Click **New Analysis**.

> You can also create an analysis from the Analyze Alerts page for PSIRTs Advisories. Choose **Analyze Alerts** > **Advisories**. Select a PSIRT advisory and click **Analyze**. In the Recommendations area click **Firmware Update Analysis**.

4. Enter the analysis name.
5. Select a site. Click **Next**.
6. Select the firmware. Cisco recommended release and the latest firmware release are displayed.
   a. Click **Release Notes** to view the release notes for the firmware release.

7. Click **Select Nodes**.
    a. Select the nodes. Only the nodes that are required to be updated are displayed. You can only select 10 nodes at a time per analysis.
    b. Click **Add**.
8. Click Save.
9. The firmware update analysis job is displayed in the **Firmware Update Analysis** Dashboard.
10. Click a completed analysis to view the details. The **Analysis Detail** page displays information such as analysis summary, site summary, node summary, and upgrade path for the firmware and node. The upgrade path for firmware and node is displayed separately if the firmware is selected on step 6.
11. Click **View Analysis Detail** to view the pre-update analysis and post update analysis for the firmware or node.
12. Click **Pre-Update Analysis** tab to view the details such as node status, validation results, potential affected objects, forecasted clear alerts after the upgrade, and potential release defects applicable after the upgrade.
    a. Click **Show All Validations** to view pre-update validation criteria and the issues detected for each criteria. See Pre-Validation Criteria for Cisco APIC.
    b. Click any object from the table to view additional details.
    c. Click **Rerun Analysis**. After fixing any of the issues highlighted in the **Validation Results** area, click **Rerun Analysis** to verify.
13. Click **Post-Update Analysis** tab to view the post-update analysis details.
    a. Perform the recommended firmware or node upgrade. The post-update summary displays the status of the upgrade.
    b. Click **Run Analysis** to view the post-update analysis details.
    c. Click **Health Delta** tab to view the difference in the anomalies between the pre-upgrade and post-upgrade analysis.
    d. Click **Operational Delta** tab to view the difference in the operational resources between the pre-upgrade and post-upgrade analysis.
    e. Click **Policy Delta** tab to view the difference in the polices between when the pre-upgrade and post-upgrade analysis were run. This is applicable only for ACI sites.
    f. Click **Rerun Analysis**.

Pre-Validation Criteria for Cisco APIC

Pre-Validation Criteria	Descriptioon	Release
Found inactive devices	This validation checks if all devices are active.	6.0.1

Pre-Validation Criteria	Descriptioon	Release
Select a compatible target version	This validation checks if the target firmware version is compatible with the current running version.	6.0.1
Remote leaf compatibility	This validation checks if remote leaf feature is supported in the target firmware version and if the fabric is using remote leaf feature.	6.0.1
Multi-Tier compatibility	This validation check if Multi-Tier topology is supported in the target firmware version and if the fabric has Tier-2 leaf nodes.	6.0.1
The fabric has 4 active critical configuration faults	This validation checks the presence of critical configuration faults or specific faults that may impact the firmware update.	6.0.1
Pod(s) have fewer than two route reflectors for infra MP-BGP	This validation checks if each pod has at least two spine nodes configured as route reflectors for infra MP-BGP.	6.0.1
Nodes are not in vPC	This validation checks if leaf nodes are configured with vPC to ensure the redundancy/high availability during the firmware update.	6.0.1
Nodes do not have out-of-band management IP	This validation checks the presence of nodes without OOB (Out-of-Band) management IP configuration to ensure that you always have access to all nodes.	6.0.1
NTP is not configured	This validation checks if Network Time Protocol (NTP) is configured for Cisco APICs.	6.0.1
Switch upgrade maintenance group check	This validation checks if APICs have maintenance and firmware groups.	6.0.1

Pre-Validation Criteria	Descriptioon	Release
Failed to validate rule	This validation checks if the target firmware version is compatible with current running CIMC versions.	6.0.1
Cisco APICs in cluster have different infra VLAN IDs	This validation checks if APICs in the cluster have same infra VLAN IDs	6.0.1
Cisco APIC cluster status is not fully-fit for all APIC nodes	This validation checks if the APIC cluster status is fully-fit for all APIC nodes.	6.0.1
Fabric recovery is in progress	This validation checks if there is any fabric recovery in progress.	6.0.1
The configured SNMPv3 user authorization and/or privacy types are not supported in the target Cisco APIC firmware version	This validation checks if configured SNMPv3 user authorization and/or privacy types are supported in the target APIC firmware version.	6.0.1
Endpoint network redundancy	This validation checks if nodes have non-redundant connected endpoints to avoid traffic loss during the reboot of nodes.	6.0.2

Viewing Defect Analysis

Use this procedure to views the digitized defects associated with the firmware version.

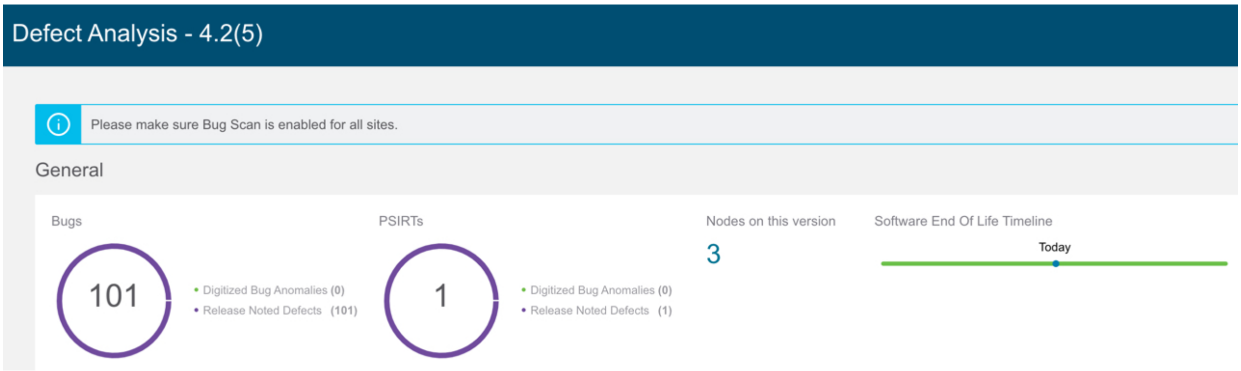
Before you Begin

Ensure that Bug Scan is enabled for all sites. See Bug Scan.

Procedure

1. Choose **Settings** > **Application** > **About**.
    a. Hover around **Metadata Version** to view the digitized defects for the metadata version in the current release.
2. In the **Overview** page, choose **Dashboard**.
    a. From the Anomaly Summary drop-down list, select **Firmware**.
    b. Hover around a firmware version of a controller and click **Release Notes** to view the release notes for the firmware version.
    c. Hover around a firmware version of a node or controller and click **Defect Analysis** to view the defects associated with the firmware version.
    d. In the **Defect Analysis** page, you can view the bugs, PSIRTs, nodes, and software EOL

timeline.



Defect Analysis - 4.2(5)

Please make sure Bug Scan is enabled for all sites.

General

Bugs

101

- Digitized Bug Anomalies (0)
- Release Noted Defects (101)

PSIRTs

1

- Digitized Bug Anomalies (0)
- Release Noted Defects (1)

Nodes on this version

3

Software End Of Life Timeline

Today

Digitized Bug Anomalies are digitized bugs that are also found as system anomalies in the Bug Scan feature. Release Noted Defects are bugs mentioned as Known Issues in the release notes for a specific firmware version. The software EOL timeline displays the EOL timeline for the firmware version and is color coded based on severity:

- Critical:Red - EOL is less than 90 days from today.
- Warning:Yellow - EOL is between 90 days and 249 days from today.
- Healthy:Green - EOL more than 250 days from today or EOL not yet available and product support is active.

e. Click **Digitized Bug Anomalies** or **Release Noted Defects** to view the details such as type, category, title, description in the table below.

f. Click **Nodes in this version** to view more information on the nodes associated with the firmware version.

You can also access the **Defect Analysis** page from the following areas in the GUI.

3. Choose **Nodes**.
   a. Hover around the firmware version of a node and click **Defect Analysis** to view the defects associated with the firmware version.
4. Choose **Change Management** > **Firmware Update Analysis**.
   a. From the Site Group menu, select a Site Group or site.
   b. Select the firmware version from the **Node Target Firmware** column.
   c. In the **Analysis Details**, page hover around node target firmware and click **Defect Analysis**

Pre-Change Analysis

Pre-Change Analysis

Currently this feature is supported for ACI Site Groups only.

You can access the Pre-Change Analysis page from the left Navigation column in the Cisco Nexus Dashboard Insights GUI. Navigate to **Change Management** > **Pre-Change Analysis**. When you want to change a configuration for a site, this feature in Cisco Nexus Dashboard Insights allows you to model the intended changes, perform a Pre-Change Analysis against an existing base snapshot in the site, and verify if the changes generate the desired results.

After you model the changes for a Pre-Change Analysis job, you can choose **Save** or **Save And Analyze**. By choosing **Save**, you can save the Pre-change Analysis job without having to start the analysis right away. You can return to the job later, edit the changes if required, and then run the analysis later. The **Save** option is supported only for a Pre-Change Analysis job with manual changes. If you choose **Save And Analyze**, the job gets scheduled and an analysis is provided.

When you choose **Save and Analyze** for the job, the changes are applied to the selected base snapshot, the analysis is performed, and results are generated. For every pre-change analysis job listed in the table, a delta analysis is performed between the base snapshot and the newly generated snapshot.

> In the Pre-Change Analysis page, to see the details of a completed Pre-Change Analysis job, click that job in the table. This opens a new page on the right that displays general information of the job. This includes the site name, snapshot details, type etc. Also included are the list of changes that were modeled for that job. As the job is complete, the severity area displays the anomalies that are generated for these changes.

If anomalies are raised in the analysis, make the required modifications based on the results and re-run the analysis until you obtain satisfactory results. The download option in a Pre-Change Analysis job allows you to download a JSON file that can be uploaded to Cisco APIC. However, if you choose the file upload approach, you can upload a JSON or an XML Cisco APIC configuration file to run a Pre-Change Analysis job.

Once the analysis starts, the status of the job will be shown as Running. During this time, the specified changes will be modeled on top of the base snapshot, and complete logical checks will be run, including Policy Analysis and Compliance. No switch software or TCAM checks will be performed. The status of the Pre-Change Analysis job is marked **Completed** when the entire analysis including Delta Analysis completes. The Delta Analysis is automatically triggered and the associated Pre-Change Analysis job is displayed as running during that time. The Delta Analysis is performed only on checks supported in Pre-Change Analysis job.

You can view changes applied by a user to a specific Pre-Change Analysis job by clicking the Pre-Change Analysis job in the Pre-Change Analysis table. The changes can be viewed in the sidebar by clicking a completed Pre-Change Analysis. Or you can click the View Analysis in the sidebar to view the changes under the Dashboard tab of the page that is displayed. If the changes in the Pre-Change

Analysis job is applied manually, you can view the different changes selected by the user. If the Pre-Change Analysis job is created using a JSON file, the Change Definition field displays the name of the JSON file from where the changes were imported.

Pre-Change Analysis Options

Currently this feature is supported for ACI Site Groups only.

The following list specifies the options you can choose to add to your pre-change analysis job. Only the objects listed are supported.

1. Add, modify, or remove Tenant.
2. Add, modify, remove App EPG (supported attributes: preferred group member, intra EPG isolation; relations for App EPG: BD, provided, consumed and taboo contracts; export/import of contracts is not supported.)
3. Add, modify, or remove a VRF (Supported attributes: policy control enforcement preference, policy control enforcement direction, BD enforcement status, preferred group member, description).
4. Add, modify, or remove a BD (Supported attributes: description, optimize WAN bandwidth, type, ARP flooding, IP learning, limit IP learning to subnet, L2 unknown unicast, unicast routing, multi-destination flooding, multicast allow, L3 unknown multicast flooding).
5. Add, modify, or remove a contract (Supported attributes: scope, description).
6. Add, modify, or remove a contract subject (Supported attributes: reverse filter ports, description, priority, target DSCP, filter name, forward filter name, reverse filter name).
7. Add, modify, or remove subnets (Supported attributes: scope, preferred, description, primary IP address, virtual IP address, subnet control).
8. Add, modify, or remove an App profile (priority, description).
9. Add, modify, or remove an L3Out (Supported attributes: description, VRF name, Target DSCP, route control enforcement).
10. Add, modify, or remove an L2Out (Supported attributes: description, BD name, encapsulation type, encapsulation ID).
11. Add, modify, or remove an L3 Ext EPG (Supported attributes: preferred group member, description, priority, and supported relations: VRF, provided contracts, consumed contracts, taboo, target DSCP).
12. Add, modify, or remove an L2 Ext EPG (Supported attributes: preferred group member, description, priority, target DSCP and provided contracts, supported contracts, taboo contracts).
13. Add, modify, or remove L3 Ext EPG Subnets (Supported attributes: description, scope).
14. Add, modify, or remove a Taboo Contract (Supported attributes: description).
15. Add, modify, or remove a Taboo Subject (Supported attributes: name, description, Supported relations: vzRsDenyRule).
16. Add, modify, or remove a Filter , Filter entries.

For Fabric Access Policies, you can choose to add the following to your pre-change analysis job:

1. Add, modify, or remove relationship between EPG and a physical domain.
2. Add, modify, or remove relationship between physical domain and a corresponding VLAN pool.
3. Add, modify, or remove relationship between physical domain and Attachable Entity Profile.
4. Add, modify, or remove a leaf interface profile.
5. Add, modify, or remove a port selector.
6. Add, modify, or remove a switch profile.
7. Add, modify, or remove a switch selector.
8. Add, modify, or remove an interface policy group.
9. Add, modify, or remove an interface policy for CDP and LLDP.

Pre-Change Analysis Guidelines and Limitations

When using Pre-Change Analysis follow these guidelines and limitations:

- Pre-change Analysis can be conducted for sites and uploaded files.
- More than one Pre-change Analysis can be run on the same base snapshot.
- Pre-Change Analysis cannot be run for a pre-change snapshot being used as a base snapshot.
- Only logical configuration anomalies are modeled and run in a Pre-Change Analysis. Switch software and TCAM changes are not modeled. After the analysis completes, a Delta Analysis will be automatically started to compare the snapshot, generated due to the Pre-Change Analysis, with the base snapshot. Delta Analysis is performed only on checks supported in the Pre-Change Analysis job.
- During a pre-change analysis, certain anomalies that exist in the base snapshot will not be analyzed in the pre-change analysis. As a result, these anomalies will not appear in the Pre-Change Analysis snapshot even though the violation continues to exist. The reason that such an event is not analyzed in a pre-change analysis is because these anomalies require not just logical data, but they also require switch software and TCAM data.
- Compliance Analysis displays the results of compliance checks in the Pre-Change Analysis snapshot.
- A local search of anomalies from a Pre-Change Analysis snapshot can be performed and viewed in the results section by navigating to specific tabs for **Dashboard**, **Delta Analysis**, **Compliance Analysis**, and **Explore**.
- Pre-Change Analysis does not support or analyze any service chain related changes or objects.
- The Delta Analysis tab does not allow a Pre-Change Analysis snapshot to be selected.
- If configuration data does not exist for a base snapshot, and you run a pre-change analysis job using this snapshot, new logical configuration files will not be generated. For such pre-change analysis jobs, the Download icon will be grayed out/disabled in the side panel. You will not be able to download a new logical configuration.

- The Pre-Change Analysis could go into a Failed state if an imported configuration has unsupported objects. Figure out the Cisco ACI objects that are unsupported by referring to the Pre-Change Analysis Options section, remove the unsupported objects, and import the configuration again before starting another Pre-Change Analysis job. If there is a failed Pre-Change Analysis, the error message for the failure is displayed in the Pre-Change Analysis table under **Analysis Status**.
- The Pre-change Analysis feature is supported in Cisco APIC release 3.2 or later. If you attempt to run a Pre-change Analysis with a Cisco APIC release earlier than release 3.2, an ERROR message indicates that Pre-Change verification is supported on APIC 3.2 or higher, and you cannot run the analysis.
- If there is an analysis that is currently running when you start a Pre-Change Analysis, that job is completed first. The new jobs are serviced in the order the jobs are scheduled. Cisco Nexus Dashboard Insights runs the jobs in the order that best suites the schedule and the available resources. All jobs, including the Pre-Change Analysis job are given the same priority.
- To prioritize or force a Pre-Change Analysis run, you can start the scheduler and assign a priority for your job. To do this, in the **Overview** page, at the top, choose your Site Group. Click the Actions menu next to it and choose > **Configure Site Group**. In the **Configure Site Group** page, choose the **Assurance Analysis** tab and you can stop a scheduled analysis here. At this location, you can disable all the Assurance Analysis jobs for all the sites.
- Currently, you can upload a JSON or an XML Cisco APIC configuration file to run a Pre-Change Analysis job. The maximum **change file size** supported are: 8 MB for vND and 15 MB for pND. The change file size is calculated as follows: The configuration file size of all the tenants impacted by the change + the configuration file size of the change.

Support for Multiple Objects in Pre-Change Analysis

In addition to multiple tenants, you can also add multiple infrastructure objects as part of a Pre-Change Analysis JSON or XML job. The Pre-Change Analysis upload path allows you to add, modify, and delete multiple objects across the policy universe. There are no additional configurations required to use this feature. Your Pre-Change Analysis job for multiple objects will run, based upon the file/s you upload.

The following file upload formats are accepted:

- A JSON or XML file with IMDATA of size 1.
- An IMDATA that contains a single subtree of the intended changes. The root of the subtree can be the UNI or any other Managed Object as long as the changes are represented as a single subtree.
- Use the file that you had uploaded from a JSON or XML path to perform a Pre-change Analysis. After the Pre-Change Analysis is complete, you can upload the same file to ACI to be used to make the changes.

Known Issues for Pre-Change Analysis

- When Pre-Change Analysis scale limits are exceeded, the analysis can fail with no error message.

- For Pre-Change Analysis jobs, you must not modify configurations where the total number of EPGs, BDs, VRFs are greater than 16,000.
- When creating a new Pre-Change Analysis, note the following:
    - If the JSON/XML file size being uploaded is less than 100 MB but greater than 15 MB, then the API validates the file and throws a validation error as follows: *Uploaded file size exceeds the 15MB(pND)/8MB(vND) maximum limit.* When users access Cisco Nexus Dashboard Insights, and try to create a Pre-Change Analysis job with a file size greater than 15MB(pND)/8MB(vND), the UI throws the following error: *File size cannot be larger than 15MB(pND)/8MB(vND).* Therefore, files larger than 15MB(pND)/8MB(vND) are not supported in Pre-Change Analysis.
    - If you upload a file with unsupported objects, Cisco Nexus Dashboard Insights will remove the unsupported object and run the job.
- A Pre-change Analysis job may fail or return incorrect results if the Cisco ACI configuration has features that are unsupported by Cisco Nexus Dashboard Insights.
- Pre-change Analysis is not supported in Cisco ACI configurations that contain service chains.
- Cisco Nexus Dashboard Insights performs a limited set of checks on the JSON file uploaded for pre-change analysis. Cisco ACI may reject this file.
- Pre-change Analysis may incorrectly report errors for attributes of subnets of external routed networks.
- Pre-change Analysis is supported in the following Cisco APIC releases:
    - For 3.2(x) release, 3.2(9h) and earlier are supported
    - For 4.0(x) release, 4.0(1h) and earlier are supported
    - For 4.1(x) release, 4.1(2x) and earlier are supported
    - For 4.2(x) release, 4.2(4o) and earlier are supported
    - For 5.0(x) release, 5.0(2e) and earlier are supported
    - For 5.1(x) release, 5.1(4c) and earlier are supported
    - For 5.2(x) release, 5.2(1g) and earlier are supported

Create Pre-Change Analysis Job

1. In the **Overview** page, at the top, choose your Site Group.
2. In the left Navigation, click **Change Management** > **Pre-Change Analysis**.
3. In the **Pre-Change Analysis** page, click **Actions** > **Create Pre-Change Analysis**. In the **Create Pre-Change Analysis** page, perform the following actions:
    a. In the **Pre-Change Analysis Name** field, enter a name.
    b. In the **Site** field, choose the appropriate site.
    c. In the **Snapshot** field, specify the appropriate snapshot.
    d. In the **Change Definition** field, choose the appropriate option. (**Import JSON/XML File** or

Manual Changes).

> ℹ Depending upon your selection, the relevant fields are displayed for you to populate. If you choose the file import option to upload a JSON or XML file upload, you must click **Save & Run** to start the Pre-Change Analysis operation. If you choose the manual changes option, you can either save & run the job, or save the job to start it at a later time by clicking **Actions** > **Edit Pre-Change Analysis** and clicking **Save & Run**. When in the **Edit** page, you can also change some of the fields if required.

e. Complete the selections as appropriate, and click **Save** or **Save & Run**.

After a Pre-Change Analysis job is completed, the **Pre-Change Analysis** table displays the status for the job as completed. Click the Pre-Change Analysis Name for which you want to view the details. In a sidebar to the right, the details are displayed in a column including the general information such as the name of the job, snapshot, and change definition type. The list of changes modeled for the job are also available. And if you are viewing a completed job, the anomalies that were generated as a result of the changes are displayed at the top of this page.

For completed jobs, click the icon on the top right of the sidebar to navigate to the results page. Further details about the job are available here under the specific tabs for **Dashboard**, **Delta Analysis**, **Compliance Analysis**, and **Explore**.

See Analyze Alerts for details about anomalies and alerts.

Clone Pre-Change Analysis Job

> ℹ You can clone Pre-Change Analysis jobs for manual changes only.

1. In the **Overview** page, at the top, choose your Site Group.
2. In the left Navigation, Click **Change Management** > **Pre-Change Analysis**.
3. In the **Pre-Change Analysis** page, choose the appropriate pre-change analysis name that you want to clone.
4. Click **Actions** > **Clone Pre-Change Analysis**.
5. In the new page, perform the following actions:
   a. In the **Pre-Change Analysis Name** field, enter a name for the cloned job.
   b. Click **Save** to clone the Pre-Change Analysis job.

Download Pre-Change Analysis Job

You can download an existing Pre-Change Analysis as follows:

- In the **Pre-Change Analysis** table, click the appropriate pre-change analysis name for a completed Pre-Change Analysis job. In the sidebar for the Pre-Change Analysis, click the download icon to download the file.

- The pre-change analysis downloads as an offline tar file with the pre-change analysis contents displayed in JSON format.

> In the downloaded file, you can view all the attributes which include attributes that are modified and those that are not modified. If desired, the downloaded file can be uploaded to your Cisco APIC.

Delete Pre-Change Analysis Job

1. In the **Overview** page, at the top, choose your Site Group.
2. In the left Navigation, Click **Change Management** > **Pre-Change Analysis**.
3. In the **Pre-Change Analysis** page, check the check box for the job/s that you want to delete.
4. Click **Actions** > **Delete Pre-Change Analysis**.
5. In the **Delete Pre-Change Analysis** dialog box, click **Delete** to confirm.

The selected job/s are deleted, and the Pre-Change Analysis page refreshes and displays the updated page.

> You can delete up to 10 Pre-Change Analysis jobs at a time. You cannot delete a job in the **Running** state. If you attempt to do that, an appropriate notification will display.

Integrations

About AppDynamics Integration

Cisco Nexus Dashboard Insights provides the ability 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 is associated only at the Site level. Onboarding of the AppDynamics controller is only at the Site level, and it is not supported at the Site Group level.

AppDynamics hierarchy consists of the following components:

- Network Link—Provides the functional means to transfer data between network entities.
- Node—A working entity of an application and is a process running on a virtual machine.
- Tier—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 Nexus Dashboard Insights 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.

Nexus Dashboard Insights connects to the AppDynamics controller and pulls the data periodically. This data from AppDynamics controller, rich in application specific information is fed to Nexus Dashboard Insights, thereby providing Cisco Nexus Dashboard 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 Nexus Dashboard Insights with AppDynamics enables the following:

- Monitoring and presenting AppDynamics hierarchy in Nexus Dashboard Insights.
- Gathering and importing network related metrics into the Nexus Dashboard Insights.
- 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.
- The AppDynamics integration uses API server and multiple instances of Telegraph data collecting container to support load balancing of the onboarded controllers.
- Fabric flow impact calculation for AppDynamics anomalies.

Onboarding for SaaS or Cloud Deployments

Starting from Nexus Dashboard Insights release 6.0.2, you can connect to AppDynamics controller using a proxy for SaaS or cloud deployments. For onboarding an AppDynamics Controller running on cloud, Nexus Dashboard Insights uses proxy configured on Cisco Nexus Dashboard to connect to AppDynamics Controller.

Guidelines and Limitations

- After Nexus Dashboard Insights upgrade, AppDynamics takes about 5 minutes to report the information in AppDynamics GUI.
- The health and count of AppDynamics business transactions displayed in the application details page do not match the flow count in Nexus Dashboard Insights.
- Nexus Dashboard Insights 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 Nexus Dashboard Insights. Hence Nexus Dashboard Insights will not stitch the path fully and will not display complete path summary with all the information.
- To connect an HTTPS AppDynamics controller using an HTTP proxy you must configure HTTPS proxy in Nexus Dashboard with the HTTP proxy server URL address.
- To connect an HTTP AppDynamics controller using an HTTP proxy you must configure HTTP proxy in Nexus Dashboard with the HTTP proxy server URL address.
- Configuration import and export are not supported for AppDynamics integrations.

Installing AppDynamics

Before you begin using Nexus Dashboard Insights **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 Nexus Dashboard Insights using

GUI. For Cisco Nexus Dashboard Insights and AppDynamics integration, the Cisco Nexus Dashboard's data network must provide IP reachability to the AppDynamics controller. See the Cisco Nexus Dashboard Deployment Guide.

Before you begin

- You must have installed AppDynamics application and controller.
- You must have administrator credentials for Nexus Dashboard Insights.
- You must have user credentials for AppDynamics controller.
- You must have configured proxy on Nexus Dashboard to connect to AppDynamics controller using a proxy. See section **Cluster Configuration** in the Cisco Nexus Dashboard User Guide

Procedure

1. In the **Overview** page, click the **Settings** icon > **Integrations** > **Manage**.
2. Click **Add Integration**.
3. Select **App Dynamics**.
    a. Enter Controller Name, Controller IP or Hostname, and Controller Port. Controller Name can be alphanumeric and spaces are not allowed.

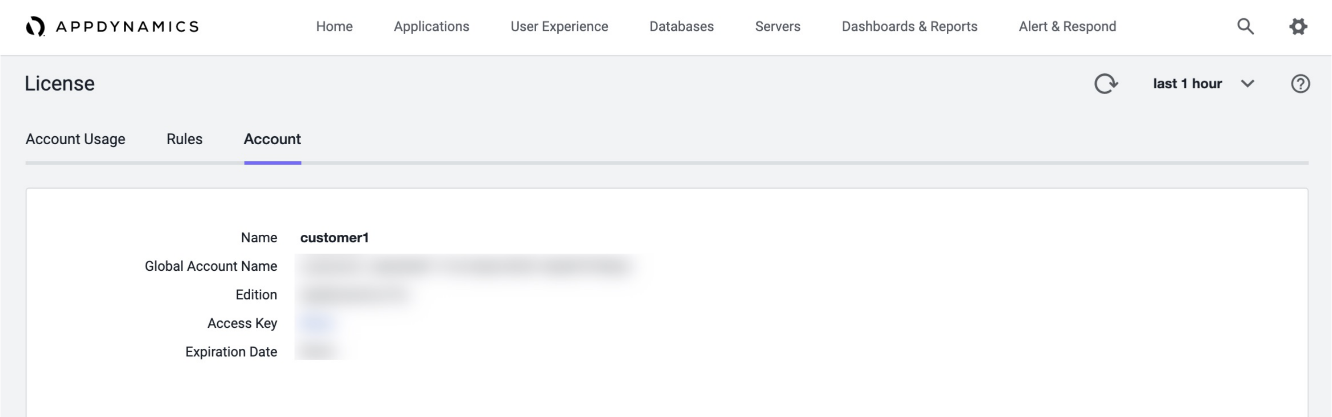
> AppDynamics Controller Name cannot be the same name as Nexus Dashboard site name.

a. Select Controller Protocol.

b. Check the **Enable** checkbox to connect to AppDynamics controller using a proxy. The proxy must be configured on Nexus Dashboard. In Nexus Dashboard, choose **Admin Console** > **Infrastructure** > **Cluster Configuration** > **Proxy Configuration** to configure the proxy.

c. Enter AppDynamics Account Name, User Name, and Password. Nexus Dashboard Insights supports only password based authentication while onboarding controller.

> You can obtain this information from your AppDynamics setup by navigating to Settings (Gear icon) > License > Account.



Name customer1

Global Account Name [redacted]

Edition [redacted]

Access Key [redacted]

Expiration Date [redacted]

4. Click **Add Association** to associate a Site Group or site.

   a. Select a Site Group or site.

   b. Click **Select**.

5. Click **Add**.

The AppDynamics controller displays on the **Manage Integration** page. When the **Status** is Active, the onboarding for the controller is complete.

AppDynamics Controller in Nexus Dashboard Insights

On the **Manage Integration** page, the active status indicates that the controller is active to fetch data. The down status indicates that the Nexus Dashboard Insights will not fetch data from the AppDynamics controller. You can hover over the red dot to see the reason for down status.

Use the filter bar to search for a specific integration. Click ··· and choose **Delete** to delete the integration. Click ··· and choose **Edit** to edit the integration.

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.

Nexus Dashboard Insights 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 Nexus Dashboard Insights. 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 Nexus Dashboard Insights on the dashboard.

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

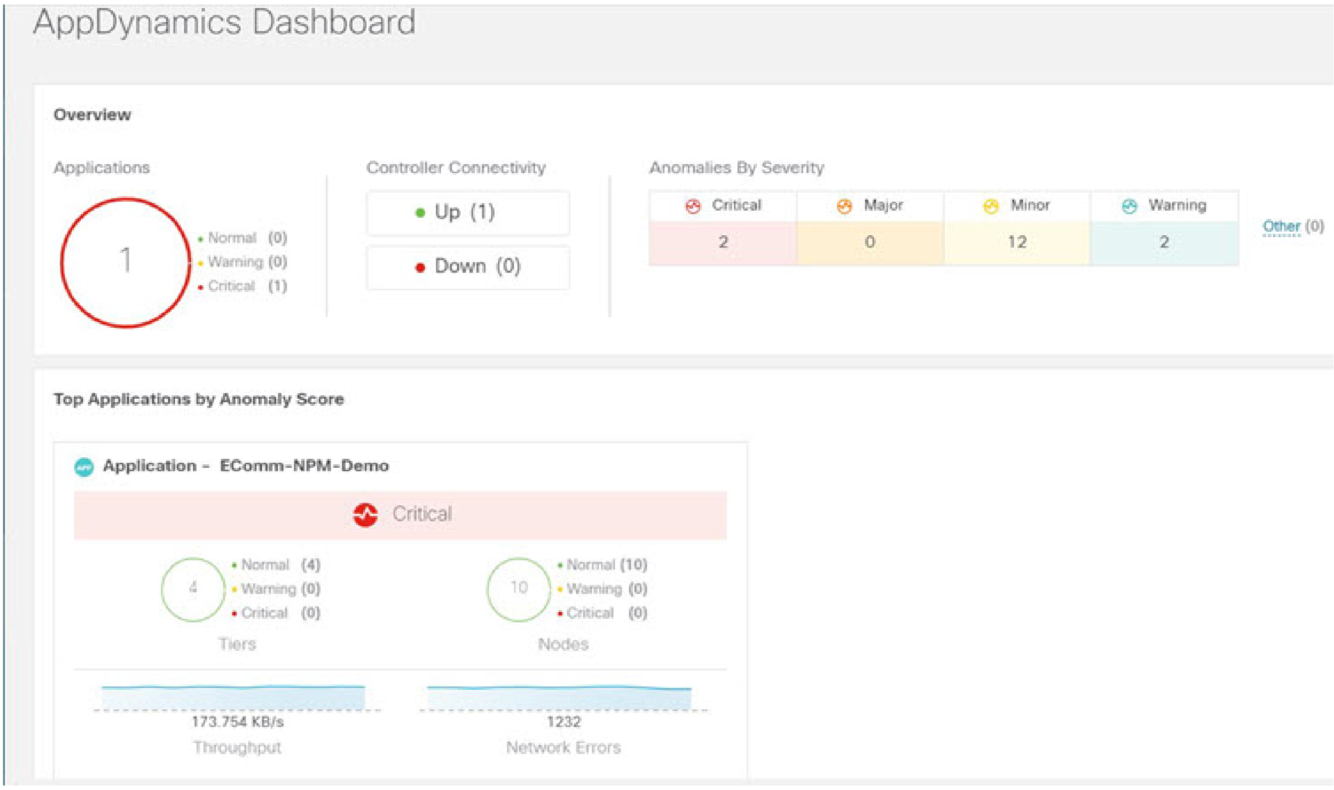
Controller Connectivity— Represents the number of integrations that are **Up** or **Down**.

Anomalies by Severity—The Nexus Dashboard Insights 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 Anomalies page.

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



AppDynamics Dashboard

Overview

Applications

1

Normal (0)
Warning (0)
Critical (1)

Controller Connectivity

Up (1)
Down (0)

Anomalies By Severity

Critical	Major	Minor	Warning
2	0	12	2

Other (0)

Top Applications by Anomaly Score

Application - EComm-NPM-Demo

Critical

4
Normal (4)
Warning (0)
Critical (0)
Tiers

10
Normal (10)
Warning (0)
Critical (0)
Nodes

173.754 KB/s
Throughput

1232
Network Errors

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.

Use the filter Category == Application for the summary pane to list the anomalies. The summary pane lists the anomaly score, controller name, account, application name, number of tiers, number of nodes, throughput, TCP loss, and errors.

1. Click an anomaly in the summary pane for the side pane to display additional details.
   a. Click **Analyze**.

      The *Analyze Anomaly* details page displays estimated impact application, recommendations, mutual occurrences, and other details affected by the anomaly.

   b. Click **View Report**.

      The side pane displays the flow groups affected where each flow group can correspond to multiple fabric flows. View reports also display the proxy/entity IP address, node source, and node destination IP address.

2. 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.
3. 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.

4. 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.
5. 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.

6. 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.

1. Click **Network Connection** for the side panel to display additional flow connection details.
2. Click **Browse Network Flows** on the side pane to navigate to Browse Flows Records with the flow properties set in the filter.

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

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

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.

AppDynamics 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 Nexus Dashboard Insights 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.

The fabric flow impact calculation for AppDynamics anomalies calls flow APIs to fetch the fabric flows corresponding to the AppDynamics flow groups that were affected by the anomaly. Nexus Dashboard Insights app displays the top 100 fabric flows ordered by the anomaly score for AppDynamics anomalies.

About DNS Integration

The Cisco Nexus Dashboard Insights Domain Name System (DNS) integration feature enables the name resolution feature to telemetry data. DNS integration can be associated at the Site Group level or the Site level.

For DNS integration you can use any of the following 3 data source methods.

DNS File Upload

This method is simple because mappings do not change often. In the GUI, you can upload a file containing mappings. Use one of the supported formats (.csv and .json). Cisco Nexus Dashboard Insights verifies the integrity of the file.

If no VRF, or Site name, or Tenant information is specified, DNS will be applied to the sites for which the DNS server is configured based on the selections in the **Add Integrations** page, **Associations** section. If the DNS server is configured for a Site Group, then DNS will be applied to all the sites in the Site Group.

The DNS file upload size is limited to 1.8 MB.

DNS Query

Use this method one query at a time to retrieve data from the DNS server using reverse lookup. Reverse lookup zone(s) must be configured on the DNS server.

Cisco Nexus Dashboard Insights queries the DNS server at regular intervals and resolves IP addresses that are learned using **Endpoints**.

When information is changed on the DNS server it may take up to 3 hours to update corresponding name mappings on Cisco Nexus Dashboard Insights. During that interval, the old name will be displayed for endpoints until the sync is completed.

Cisco Nexus Dashboard Insights allows one primary and multiple secondary DNS servers, the primary DNS server will be polled first. If the resolution does not succeed, the secondary servers will be polled thereafter.

DNS Zone Transfer

DNS Zone Transfer is also known as AXFR downloads. Nexus Dashboard Insights can retrieve zone data in bulk from the DNS server using AXFR downloads. This method is convenient for large quantities of data as you no longer have to work on one query at a time.

When information is changed on the DNS server it may take up to 3 hours to update corresponding name mappings on Cisco Nexus Dashboard Insights. During that interval, the old name will be displayed for endpoints until the sync is completed.

A zone transfer requires at least one DNS zone. If you configure a forward mapping zone, then all the A and AAAA records will be fetched from a DNS server, and if you configure a reverse mapping zone, then PTR records will be fetched. When onboarding the DNS server, you must provide a list of zones from which to fetch the data. Cisco Nexus Dashboard Insights will fetch the data from each zone configured from the DNS server.

TSIG (transaction signature) is a computer-networking protocol defined in RFC 2845. Primarily it enables the DNS to authenticate updates to a DNS database. For a secure transfer, Cisco Nexus Dashboard Insights allows you to configure the TSIG key for a zone to initiate the transaction. Configure the zone with the TSIG key, and an associated algorithm. In the Cisco Nexus Dashboard Insights GUI, the supported algorithms are displayed in a drop-down list.

When you delete an onboarded DNS server, all the zones will be un-configured automatically. A zone can be a forward mapping or a reverse mapping zone.

Configure DNS File Upload

Follow this procedure to configure DNS using the File Upload method.

> The .json or .csv file used in this task must be uploaded in a specific schema. See the following section for the formats to use.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**.
2. In the **Manage Integrations** page, click **Add Integration**.
3. In the **Add Integration** dialog box, choose the radio button for **DNS**.
4. In the **Configuration** area, perform the following actions:
   a. In the **DNS Type** field, choose the type, **Mapping File**
   b. In the **Name** field, enter a name associated with the file to identify the onboarding.
   c. In the **Description** field, enter a description.
   d. In the **Select a file or drag and drop it here area**, add your file. The accepted files are .csv or .json.
   e. In the **Associations** area, click **Add Associations** to associate a Site Group or Site.
   f. Click **Add** to complete the configuration.

In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

Edit Your DNS File Upload Configuration

Follow this procedure to edit the DNS configuration.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**

In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

2. To edit your DNS configuration, in the **Integrations** table, click the Actions icon and click **Edit**.
3. You can re-upload a file here as required.
4. When you have completed the upload, click **Add**. This completes the editing procedure.

Delete Your DNS File Upload Configuration

Follow this procedure to delete the DNS configuration.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**

   In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

2. To delete your DNS configuration, in the **Integrations** table, click the Actions icon and click **Delete**. This action deletes your DNS configuration.

Formats for Files Used in DNS File Uploads

When configuring the DNS file uploads, .json and .csv formats are supported. Use the formats provided below for the files that you upload.

The fields in a DNS file upload can have optional VRF, or Site name, or Tenant information. If you specify details for one of these options you must specify all of them. If you have a file that contains the site name, you must specify the VRF and Tenant also.

Format .json

```
[
  {
        "recordType": "dnsEntry",
        "fqdn": "host1.cisco.com",
        "ips": ["1.1.0.0"],
        "vrf": "vrf-1",
        "siteName": "swmp3",
        "tenant": "tenant-1"
  },
  {
        "recordType": "dnsEntry",
        "fqdn": "host2.cisco.com",
        "ips": ["1.1.0.1"],
        "vrf": "vrf-1",
        "siteName": "swmp3",
        "tenant": "tenant-1"
 }
 {
         "recordType": "dnsEntry",
         "fqdn": "host3.cisco.com",
         "ips": ["1.1.0.2"],
 },
]
```

Format .csv

```
recordType,fqdn,ips,siteName,tenant,vrf
dnsEntry,swmp3-leaf1.cisco.com,"101.22.33.44",swmp3,tenant-1,vrf-1
dnsEntry,swmp5-leaf1.cisco.com,"10.2.3.4,10.4.5.6,1.2.3.4",fabric2,tenant-2,vrf-2
dnsEntry,swmp4-leaf1.cisco.com, "1.1.1.1",,,
```

Configure DNS Query Server

Follow this procedure to configure the DNS Query Server method.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**.
2. In the **Manage Integrations** page, click **Add Integration**.
3. In the **Add Integration** dialog box, choose the radio button for **DNS**.
4. In the **Configuration** area, in the **DNS Type** field, choose the type, **Query Server**.
5. In the **Name** field, enter a name for the integration.
6. In the **DNS Server IP** field, enter the IP address.

7. In the **DNS Server Port** field, enter the port number. The default port value is 53.
8. In the **Secondary Controllers** area, add your secondary controller IP address and port number. Add additional secondary controllers as appropriate.
9. Click the check mark next to the selections when done.
10. In the **Associations** area, click **Add Associations** to associate a Site Group or a site.
11. Click **Add** to complete the task.

In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

Edit Your DNS Query Server Configuration

Follow this procedure to edit the DNS configuration.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**

   In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

2. To edit your DNS configuration, in the **Integrations** table, click the Actions icon and click **Edit**.
3. In the **Secondary Controllers** area, you can add IP address details.
4. When you have completed your editing, click **Save**. This completes the editing procedure.

Delete Your Query Server Configuration

Follow this procedure to delete the DNS configuration.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**

   In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

2. To delete your DNS configuration, in the **Integrations** table, click the Actions icon and click **Delete**. This action deletes your DNS configuration.

Configure DNS Zone Transfer

Follow this procedure to configure DNS using the Zone Transfer method.

Procedure

Follow this procedure to configure the DNS Zone Transfer method.

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**.
2. In the **Manage Integrations** page, click **Add Integration**.
3. In the **Add Integration** dialog box, choose the radio button for **DNS**.
4. In the **Configuration** area, in the **DNS Type** field, choose the type, **Zone Transfer**.
5. In the **Name** field, enter a name for the integration that uniquely identifies the controller in Cisco Nexus Dashboard Insights.
6. In the **DNS Server IP** field, enter the IP address of the DNS server.
7. In the **DNS Server Port** field, enter the port number. Specify port if it is different from the default port (53).
8. In the **Zones** area, enter the value for Zone Name. Optional values that can be entered are TSIG Key Name, TSIG Key Value, TSIG Algorithm.

   The **TSIG Algorithm** dropdown menu selections are hmac-sha1, hmac-sha256, hmac-sha512, hmac-md5.

9. Click the check mark next to the selections when done.
10. In the **Associations** area, click **Add Associations** to associate a Site Group or a site.
11. Click **Add** to complete the task.

In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

Edit Your DNS Zone Transfer Configuration

Follow this procedure to edit the DNS configuration.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**

   In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

2. To edit your DNS configuration, in the **Integrations** table, click the Actions icon and click **Edit**.
3. In the **Edit Integration** dialog box, in the **Zones** area, you can edit the values for the Zone Name, TSIG Key Name, TSIG Key Value, TSIG Algorithm. You can also add more Zones if required.
4. When you have completed your editing, click **Save**. This completes the editing procedure.

Delete Your DNS Zone Transfer Configuration

Follow this procedure to delete the DNS configuration.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**

   In the **Manage Integrations** page, the **Integrations** area lists the details of each integration by Name, Connectivity Status, Type, IP address, Last Active, Associations.

2. To delete your DNS configuration, in the **Integrations** table, click the Actions icon and click **Delete**. This action deletes your DNS configuration.

Alternate Method to Access the Integrations Page

An alternate method to view existing integration details and also to add integrations is as follows:

To view your DNS configurations, in the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Application** > **Setup**. In the **Let’s Configure the Basics** page, in the **Site Groups Setup** area, click **Edit configuration**. In the **Site Groups Setup** page, click the **Integrations** tab to see the **Integrations** page.

DNS Integration Guidelines and Limitations

- DNS onboarding can be done at a Site Group level or at a site level.
- Only one type of DNS integration method is supported in one Site Group or in one site. For example, in one Site Group or in a site, you cannot configure using DNS file uploads as well as DNS Zone Transfer methods.
- Multiple DNS integration onboarding of the same type is allowed in a Site Group or in a site. For example, multiple files can be onboarded, to a Site Group or a site using the DNS file uploads method.
- If you perform DNS integration onboarding at a Site Group level, you cannot also onboard a site in that same Site Group.
- When a corrupted or malformed .CSV of .JSON file is uploaded to the DNS server, Cisco Nexus Dashboard Insights raises system anomalies. However, the **Connectivity Status** of the third-party onboarding server, remains in the initialized state and does not change to display a failed state. If the third-party onboarding server remains in the initialized state, check the system anomalies for any anomalies related to the specific integration.
- The supported scale for DNS integration is 40,000 DNS entries. For vND application profiles, the supported scale for DNS integration is 10,000 DNS entries.
- Data from DNS servers will be polled or refreshed every 3 hours. So, any changes in the mapping on the DNS server will reflect after the next polling cycle.
- Configuration import and export are not supported for DNS integrations.

Add Nexus Dashboard Orchestrator and Configure Assurance Analysis

Cisco Nexus Dashboard Orchestrator Assurance is a BETA feature.

> We recommend that you use features marked as ‘Beta’ in your test environments but not in production deployments.

Follow this procedure to add Nexus Dashboard Orchestrator.

Procedure

1. In the Cisco Nexus Dashboard Insights **Overview** page, click the Settings icon > **Integrations** > **Manage**.
2. In the **Manage Integrations** page, click **Add Integration**.
3. In the **Add Integration** dialog box, choose **Nexus Dashboard Orchestrator**.
4. In the **Authentication** area, perform the following actions:
    a. In the **Controller Name** field, enter the name.
    b. In the **Controller IP or Hostname** field, enter the controller IP address or the hostname.
    c. In the **User** and **Password** fields, enter the username and password credentials.

> The admin account must be used to perform these actions. Enter your APIC username and password values.

d. In the **Associations** area, click **Add Associations** to associate the appropriate Site Group.

> All sites that are added in the Site Group are a part of the Site Group. These sites may be a subset of all the sites that are managed by Nexus Dashboard Orchestrator. It is not necessary that all the sites that belong to a Site Group are managed by Nexus Dashboard Orchestrator.

5. In the **Managed Sites** area, click **Direct Managed Sites**. All the sites that are managed my Nexus Dashboard Orchestrator will be listed. Clicking a site will take you to the site itself.

    > There may be sites in this list that are part of the Site Group but are not managed by Nexus Dashboard Orchestrator.

6. Click **Add** to complete the on-boarding.
7. To enable assurance analysis, from the **Overview** page, click **Configure Site Group** for your Site Group.

    In the **Configure Site Group** page, in the **General** tab, in the **General** area, in the **Orchestrator** column, the Nexus Dashboard Orchestrator name is displayed. In the **Sites** area, the Nexus Dashboard Orchestrator managed sites that are assured by Nexus Dashboard Insights are listed.

8. In the **Configure Site Group** page, **Assurance Analysis** tab, in the **Inter-Site Details** area, under **Inter-Site Assurance**, locate your Nexus Dashboard Orchestrator name.
9. In the **Inter-Site Details** area, click **Edit** and in the **Edit Inter-Site Assurance** dialog box, change the **State** to **Enabled**, and click **Save**.

This completes the Nexus Dashboard Orchestrator assurance setup process.

Nexus Dashboard Orchestrator Guidelines and Limitations

- You must have the Site Group added in Nexus Dashboard Insights before you integrate Nexus Dashboard Orchestrator with Nexus Dashboard Insights. This is required because when you integrate Nexus Dashboard Orchestrator, you must associate a Site Group.
- If, at a later time, you add additional sites to a Site Group that is managed by Nexus Dashboard Orchestrator, Nexus Dashboard Insights will automatically incorporate assuring the added sites.
- Configuration import and export are not supported for Nexus Dashboard Orchestrator integrations.

About VMware vCenter Server Integration

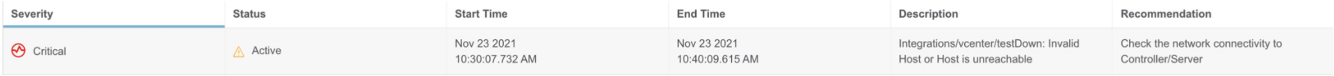
VMware vCenter Server Integration is a Beta feature. We recommend that you use features marked as ‘Beta’ in your test environments but not in production deployments.

Integrating VMware vCenter server allows Nexus Dashboard Insights to collect data and metrics of the virtual machines and hosts monitored by VMware vCenter, and then correlate the collected information with the data collected from the Cisco ACI or Cisco DCNM fabric.

Data collected from vCenter includes

- Virtual machine data
- vSphere network data
- Virtual machine NIC data
- Host data
- Datastore data
- vSphere standard switch information
- DVS information
- vCenter Alarms

Nexus Dashboard Insights collects data from vCenter every 5 minutes. A system anomaly is raised if Nexus Dashboard Insights is enable to reach vCenter.



Severity	Status	Start Time	End Time	Description	Recommendation
Critical	⚠ Active	Nov 23 2021 10:30:07.732 AM	Nov 23 2021 10:40:09.615 AM	Integrations/vcenter/testDown: Invalid Host or Host is unreachable	Check the network connectivity to Controller/Server

vCenter Anomalies

In Nexus Dashboard Insights, the alarms from vCenter are displayed as anomalies. The following types for anomalies are generated for vCenter Integration in the category **vCenter**.

- Alarms from vCenter
- Baseline anomalies for checks such as CPU, memory, storage
- Threshold and packet drop anomalies
- Host alarms

See Analyze Anomalies.

Prerequisites

- You have installed VMware vCenter 6.5 and later.
- You have admin credentials for VMware vCenter.
- You have read access to all the resources in vCenter.

Guidelines and limitations

Configuration import and export are not supported for VMware vCenter integration.

Add vCenter Server Integration

Use this procedure to add a VMware vCenter server on to Nexus Dashboard Insights.

Procedure

1. In the **Overview** page, click **Settings** > **Integrations** > **Manage**.
2. Click **Add Integration**.
3. Select **vCenter Server**.
   a. Enter Controller Name, Controller IP or Hostname, and Controller Port. Controller Name can be alphanumeric and spaces are not allowed.
   b. Select Controller Protocol.
   c. Enter vCenter User Name and Password.
4. Click **Add Association** to associate a Site Group or site.
   a. Select a Site Group or site.
   b. Click **Select**.
5. Click **Add**.
6. The vCenter Server displays on the **Manage Integration** page. When the **Status** is Active, the addition of the integration is complete.
7. (Optional) In the **Manage Integration** page, use the filter bar to search for a specific integration.
   a. Click ⋯ and choose **Delete** to delete the integration.
   b. Click ⋯ and choose **Edit** to edit the integration details.

vCenter Server Dashboard

The vCenter Dashboard presents a view of the of the **Top Virtual Machines by Anomaly Score** along with various metrics. Once a vCenter is added, data related to virtual machines monitored by that vCenter is pulled by Nexus Dashboard Insights. It can take up to 5 minutes for the first set of data to appear on the GUI.

The **Overview** area in the dashboard displays the the virtual machines by anomaly score, anomalies by severity, and vCenter connectivity status.

- Virtual Machines by Anomaly Score - Represents the aggregated health state of the virtual machines
- Anomalies by Severity — Represents the alarms from the vCenter server. Click the number on **Anomalies by Severity** to view the Anomalies page.
- vCenter Connectivity — Represents the number of vCenter integrations that are **Up** or **Down**.

The **Top Virtual Machines by Anomaly Score** displays top six out of all the virtual machines based on the anomaly score.

From the drop-down list, select CPU, memory, storage , or network usage to view the six out of all the virtual machines based on drop-down list selection.

Browse

The browse page presents the **Top Virtual Machines** by CPU utilization plotted on a timeline. From the drop-down list, select CPU utilization, memory utilization, storage utilization, or network usage to view the graphical representation of the top virtual machines based on drop-down list selection.

1. Use the filter bar to filter by vCenter, VM, state, average net usage, and CPU.

   The valid operators for the filter bar include:

   - `==` - display logs with an exact match. This operator must be followed by text and/or symbols.
   - `contains` - display logs containing entered text or symbols. This operator must be followed by text and/or symbols.
2. The page also displays the virtual machines or hosts in a tabular format. From the drop-down list, select **Virtual Machines** or **Hosts**.
   a. The **Virtual Machines** table displays information such as Anomaly score, vCenter IP address, virtual machine IP address, state, number of network adapters, IP address, average net usage, CPU %, memory %.
   b. The **Hosts** table displays information such as Anomaly score, vCenter IP address, host IP address, state, virtual machine, cluster, CPU %, memory %.
3. Click the **Settings** menu to customize the columns to be displayed in the **Virtual Machines** or **Hosts** table.
4. Select any item in the table for the side pane to display additional details.
5. Click the ↗ icon to view the page for the item selected.

Virtual Machine Page

- The **Overview** tab in the virtual machine page displays information such as anomaly score, usage, host, datastore, and network adapters.
- The **Anomalies** tab in the virtual machine page displays the alarms from vCenter.
- The **Topology** tab in the virtual machine represents a hierarchical view of **virtual machine** > **host** > **leaf switch in the fabric** and the links between them with a logical or network view of how various objects are related.

  If there is a AppDynamics controller associated to the particular virtual machine, then the applications running on the virtual machine is displayed.

Hosts Page

- The **Overview** tab in the hosts page displays information such as anomaly score, usage, virtual machines, datastore, distributed switch, standard switch, and physical adapters.
- The **Anomalies** tab in the virtual machine page displays the alarms from vCenter for the host.
- The **Topology** tab in the virtual machine represents a hierarchical view of **host** > **virtual machines** > **DVS or virtual switch in the fabric** and the links between them with a logical or network view of how various objects are related.