Cisco Nexus Dashboard Insights User Guide, Release 6.2.1 - For Cisco NDFC

Table of Contents

First Published: 2023-03-20

Last Modified: 2023-04-14

New and Changed Information

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

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

Feature	Description	Release	Where Documented
Interface based Flow Telemetry	Added support to configure flow telemetry rules on interfaces such as L3Outs, SVIs, Physical Interfaces, and Port Channel.	6.2.1	Configure Flows
Microburst Enhancement	Added support to view microbursts in tabular format.	6.2.1	Microburst Support for Interface Statistics
UI Enhancement	Added support to enhance the endpoint filters and details, and flow record filters.	6.2.1	Browse and Endpoints

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

The user content describes features and use cases for the Nexus Dashboard Insights service using the Cisco Nexus Dashboard platform with the Nexus Dashboard Fabric Controller fabric. Nexus Dashboard Fabric Controller was formerly known as Data Center Network Manager.

Cisco Data Center Network Manager (DCNM) is renamed as Cisco Nexus Dashboard Fabric Controller (NDFC) starting with Release 12.0.1a.

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.

A NDFC site is comprised of a fabric running NX-OS that is either fully managed or only monitored by NDFC. All of the switches in the fabric can be analyzed as a part of the site. With a NX-OS based fabric, the fabric could be a NDFC managed fabric or it could be configured using other means such as CLI, Ansible, or any other configuration automation mechanism. For fabrics not using NDFC for configuration management, NDFC must be installed and the fabric must be discovered in read-only or monitor mode. Nexus Dashboard Insights uses NDFC for topology discovery and to identify the role of the switch in the fabric. 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.
- 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.
  - Best Practices—Provides access to configure, schedule, on-demand compliance job that runs

for a selected site. The compliance job collects technical support information and runs them against known set of signatures and then flags the defects that are not compliant.

- 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.

- Alert Rules-Enables you to acknowledge all new detected anomalies that match a criteria and adjust the anomaly score accordingly.

- Compliance Requirement-This feature is currently not supported.

- 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 the Nexus Dashboard Insights.

- Export Data—Streams the data collected from Nexus Dashboard Insights through a Kafka exporter to send the summary of the 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.

  - Connectivity Analysis—The connectivity analysis job traces all possible forwarding paths for a given flow, isolates offending nodes in the network for a given flow, and helps troubleshoot to narrow down the root cause of the issue.

- 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.

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 Dashboard User Guide for more information.

Before you begin

- You have installed and configured the Cisco Nexus Dashboard.
- You must have administrator credentials to add a site on 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. From the drop-down menu select Admin Console.
3. Click **Sites** in the left Navigation pane.
4. In the **Sites** page, click **Add Site**.
5. In the **Add Site** page, in the **Site Type** field, choose **NDFC** and perform the following actions.
6. In the **Host Name/IP Address** field, add the in-band IP address used to communicate with the site controller.
7. In the **User Name** and **Password** fields, add the values used to manage the site. As admin with read-write privileges, enter your NDFC username and password values.
8. (Optional) If you leave the **Login Domain** field empty, the site's local login is used.
9. (Optional) allows Nexus Dashboard to verify that the certificates of hosts to which it connects (such as site controllers) are valid and are signed by a trusted Certificate Authority (CA).
10. In the **Sites in NDFC** area, click **Select Sites** to select the NDFC fabrics managed by the controller you provided. Any services installed in Cisco Nexus Dashboard can access the added sites.
11. Select the site and click **Select**. You can select multiple sites.
12. In the **Site Type** field, click **Add**. You can view the new site in the **Sites** page.
13. (Optional) In the **Sites** table, if required, you can click the edit icon to modify the site name. The site name must be unique. To add multiple sites from another NDFC, repeat the above steps.
14. (Optional) Click on the Geographical Location map to specify where the site is located.
15. Continue with the installation of Cisco Nexus Dashboard Insights in 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.

ℹ️ 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.

Before you begin

- You have installed the Cisco Nexus Dashboard Insights service.
- The appropriate sites are added in Cisco Nexus Dashboard.

For Nexus Dashboard Fabric Controller (NDFC) Site Onboarding:

- The data port of your switch for telemetry and the management port of the switches must be reachable using the data network of a Cisco Nexus Dashboard Insights cluster.
- The data network of NDFC must be reachable using the data network of a Cisco Nexus Dashboard Insights cluster.

For Nexus Dashboard Fabric Discovery (NDFD) Site Onboarding:

- The data port of your switch for telemetry and the management port of the switches must be reachable using the data network of a Cisco Nexus Dashboard Insights cluster.

ℹ️ You must always onboard NDFD on a Cisco Nexus Dashboard Insights cluster.

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.

   ℹ️ 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.

> ℹ️ You must have admin read/write privileges to perform these actions. Enter your NDFC 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.

> ℹ️ 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**.
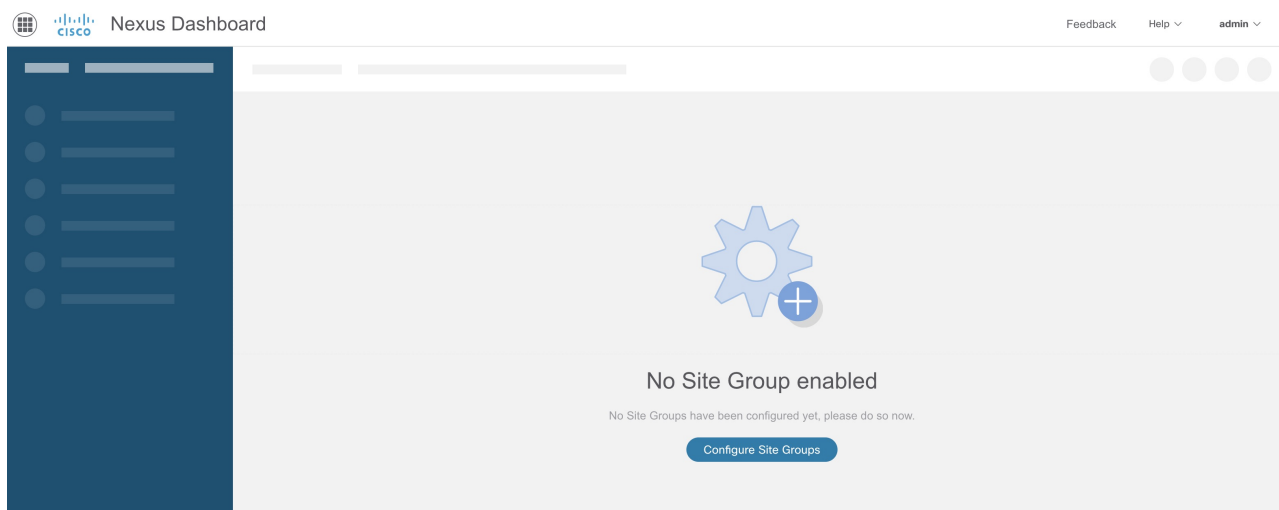
2. In the **Nexus Dashboard Insights Prerequisites** dialog box, verify that you have configured the required mandatory settings.

If you need help configuring these settings, refer to the documentation links:

a. NTP Configuration for NDFC Cisco NDFC NTP/PTP Configuration Documentation

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

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.

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

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.

Site Groups   Integrations

Add New Site Group

Name	Data Collection Type	Entities	Description	
			No data	

Done

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 **Add Member** and then click **Select Member**.

8. From the **Select a Site** dialog box, choose the appropriate site, and click **Select**.

   In the **Add New Site Group** dialog box, the site that you just added displays in the **Entity** area table.

9. In the **Configuration** column, click **Configure**.

10. In the **Configure** dialog box, in the **General Configuration** area, perform the following tasks:

a. In the **Fabric Type** field, select the appropriate option. The options are **Classic**, **VXLAN** or **SR-MPLS**.

> ℹ️ This is a **Beta** feature for Nexus Dashboard Insights release 6.1.1. In the **Fabric Type** field, the **SR-MPLS** option is also available. Choose this option to set up flows for SR-MPLS in a NX-OS fabric. See SR-MPLS Flows - Beta Feature for more details.

b. In the **Loopback** field, enter the loopback configured on the switches that provide connectivity to the Cisco Nexus Dashboard in-band IP address.

c. In the **VRF** field, enter the VRF name associated with the loopback interfaces. This is the VRF that provides connectivity to the Cisco Nexus Dashboard in-band IP addresses.

> ℹ️ Default and non-default VRFs are supported. In VXLAN/EVPN fabrics they must be part of the underlay.

d. In the **Username** and **Password** fields, as an admin with read/write privileges, enter your NDFC

username and password.

11. In the **Default LAN Credentials** area, in the **Username** and **Password** fields, as admin for the switches, enter your LAN username and LAN password.

> **ⓘ** Add switches to the list and specify their credentials below only if the switch credentials do not match the default credentials provided above.

12. In the **Switch Credentials to Override the Default Configuration** area, click **Add Switch Credential** and add the following information for the appropriate switches in the **Switch Credentials** area.

    a. In the **Switch Name** field, enter the name for the switch.

    b. In the **Switch IP** field, enter the IP address for the switch.

    c. In the **Switch Username** field, enter the username for the switch.

    d. In the **Switch Password** field, enter the password.

    e. Check the check mark to complete to add your entries, and add additional switches as appropriate.

13. Click **Save**.

14. In the **Add New Site Group** dialog box, in the **Status** column for your site, select **Enable**.

15. Check the check mark for your site to complete the configuration.

    To add additional sites in the Site Group, repeat the earlier set of steps starting by clicking **Add Member** in the **Entity** area.

16. Click **Save**.

    The site/s are added in the Site Group.

17. In the **Site Groups Setup** area, click **Done**.

18. In the **Let's Configure the Basics** page, click **Done**.

To enable and configure site group tabs, continue with the following task.

Enabling or Configuring Site Group Tabs

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.

- **Best Practices** tab: For details, see Best Practices.

- **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 and Upload a File to a Site Group and Run Assurance Analysis.

- **Export Data** tab: For details, see Export Data.

- **Flows** tab: For details, see Flows.

- **Alert Rules** tab: For details, see Alert Rules.

- **Collection Status** tab: Telemetry data displaying a status check is displayed here such as Site Name, Node, Resource, Environmental, Statistics, Endpoints, Events. See the following example page.

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**.
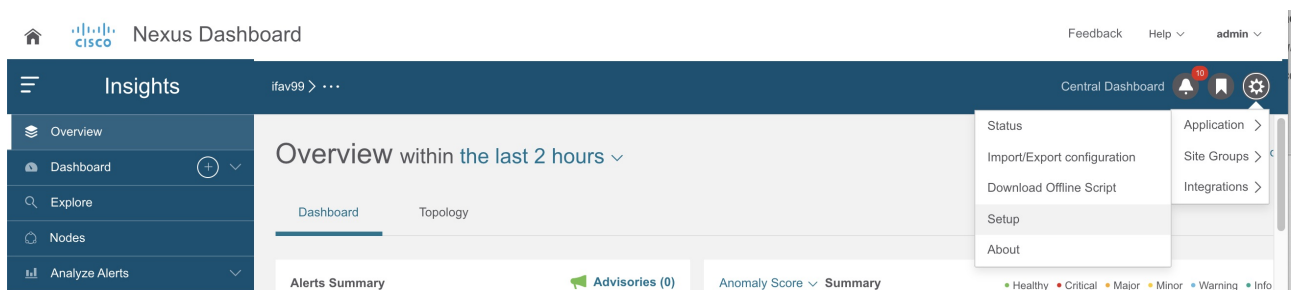
3. In the **Let's Configure the Basics** page, click **Click the Prerequisites for Cisco Nexus Dashboard Insights** link, and verify that you have configured the required mandatory settings.

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.

> ℹ️ 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**.

Nexus Dashboard Insights Switch Configuration Status

1. In the **Overview** page, on the top, next to your selected Site Groups, click the three dots and click **Configure Site Group**.

2. In the **Configure Site Group** page, **Sites** area table displays the onboarded sites.

| Configure Site Group - Scale_Fabric | ✕ |

General Bug Scan Best Practices Assurance Analysis Export Data Flows Alert Rules Compliance Requirement Collection Status

General

Site Group Details   Edit Site Group

NAME	DATA COLLECTION TYPE	DESCRIPTION
Scale_Fabric	Site	Restored during Upgrade

Sites

Collection Status	Name	Configuration Status	Node Status	Type
● Enabled - Configured	Scale_Fabric	● OK	⊘ 0 ⊘ 6 ⏱ 0 ⊗ 0	DCNM

3. Double-click a value displayed in the **Node Status** column to display the on-boarded switch configurations, status, and additional details.

The switch status includes:

- **Grey**—Nodes are in initial state and unconfigured.
- **Green**—Nodes configured successfully.
- **Orange**—Nodes are currently being configured.
- **Red**—Nodes that failed configuration.

```
Note: When you enable the telemetry configuration for a site and if Red Count is
greater than 0,
it implies that the initiated operation is not successful for enabling or disabling
the site.
Click Count and then click Retry for configuration to be pushed again to nodes.
Click Any Counts to view expected configurations.
You can exit the {CiscoNIRFullName} Setup page and return for immediate refresh of
the pages.
```

Configure Site Group - Scale_Fabric

General   Bug Scan   Best Practices   Assurance Analysis   Export Data   Flows   Alert Rules   Compliance Requirement   Collection Status

General

Site Group Details

NAME   DATA COLLECTION TYPE
Scale_Fabric   Site

Sites

Collection Status	Name
● Enabled - Configured	Scale_Fabric

Site Scale_Fabric

Search

Retry All Configurations

✓ nd76vg-Leaf
Switch

✓ nd77vg-Leaf
Switch

✓ EOR
Switch

✓ nd94vg-Leaf
Switch

✓ nd85vg-SP
Switch

✓ nd86vg-SP
Switch

Switch
nd76vg-Leaf

View Expected Configuration

General Information

SWITCH SERIAL
FDO230118MH

SWITCH IP
172.28.243.113

SOFTWARE TELEMETRY RECEIVER IP PORT
9.1.223.94:57500

FLOW TELEMETRY RECEIVER IP PORT
9.1.223.91:5640
9.1.223.92:5640
9.1.223.93:5640

SWITCH MODEL
N9K-C93108TC-FX

SWITCH SOFTWARE VERSION
9.3(6)

Status

SOFTWARE TELEMETRY CONFIGURATION STATUS

4. Select a switch and click **View Expected Configuration** to view expected switch configuration details in the **Expected Configuration** area.

Configure Site Group - Scale_Fabric

General   Bug Scan   Best Practices   Assurance Analysis   Export Data   Flows   Alert Rules   Compliance Requirement   Collection Status

General

Site Group Details

NAME   DATA COLLECTION TYPE
Scale_Fabric   Site

Sites

Collection Status	Name
● Enabled - Configured	Scale_Fabric

Site Scale_Fabric

Search

Retry

nd76vg-Leaf
Switch

nd77vg-Leaf
Switch

EOR
Switch

nd94vg-Leaf
Switch

nd85vg-SP
Switch

nd86vg-SP
Switch

Expected Switch Configuration for nd76vg-Leaf

Software Telemetry   Flow Telemetry

Configure Terminal

Copy Configuration

```
configure terminal

feature ntp
ntp server 9.1.223.21 prefer use-vrf default

feature lldp
feature icam
feature telemetry

telemetry
  destination-profile
    use-vrf default
    source-interface loopback100
  destination-group 500
    ip address 9.1.223.94 port 57500 protocol gRPC encoding GPB
    use-chunking size 4096
```

15

As a user, you must configure the appropriate switches by using the recommended configuration. From the **Expected Configuration** area, you can view and copy configurations under **Software Telemetry** and **Flow Telemetry**. For more details, see Configure Flows.

Guidelines and Limitations

The Cisco Nexus Dashboard Insights service, release 6.0.1 allows you to discover both ACI and NDFC sites.

About Device Connector

Data center apps and services such as Cisco Nexus Dashboard Insights 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.

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: Analytics—This includes monitoring of interfaces on the Cisco APIC and site nodes.

- Protocols: Analytics—This includes monitoring protocols on the Cisco APIC and site nodes.

Change Management: The sub-tab in this area is 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.

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.

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, tables, and lists appear in the work pane. When viewing the **Overview** page, it contains the **Dashboard** tab and the **Topology** tab.

Dashboard Tab

In the Nexus Dashboard Insights dashboard view, there are different tiles in this area 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.
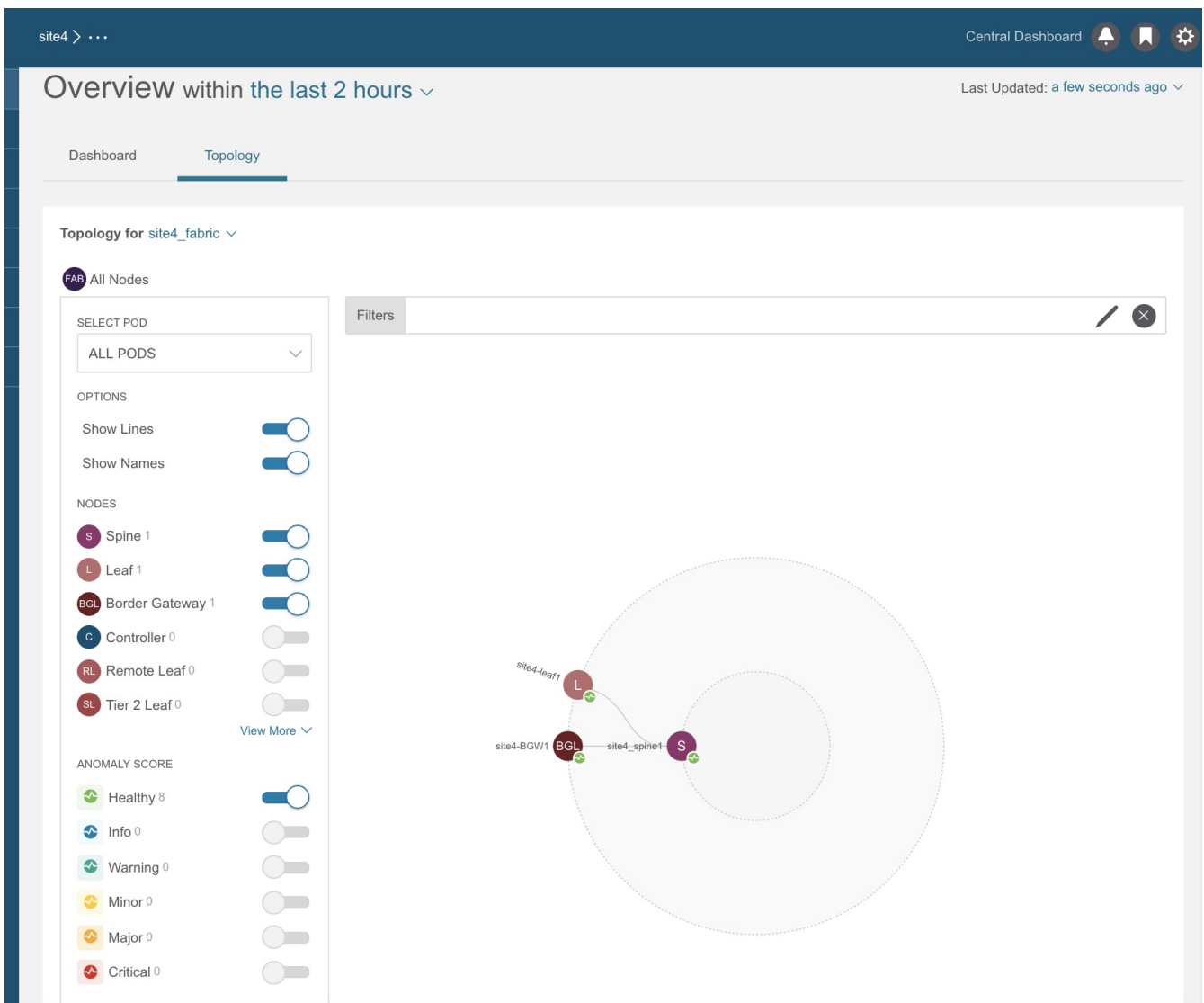
Tables

If a table in the GUI has a settings icon, , as one of its columns, you can use it to customize your columns. When you click the icon, the **Customize Columns** dialog box is displayed with a list of items. Some of the settings are mandatory, therefore the option to set them are grayed out. For the user-selectable items, you can choose to display or remove each column in the table. You can also

click and drag a column title to rearrange its location in the table. Click **Save** to update the table. Your customized column settings will persist in this login instance as well as your subsequent logins.

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 node in the site streams telemetry data and events to a service in Nexus Dashboard Insights which then analyzes the data and detects any anomalies. The Dashboards provide relevant information to view.

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 and Upgrade Impact

The main dashboard provides immediate access to anomalies occurring in the network. Anomalies are learned deviations from the last known "good" state of a switch and are displayed by type and severity. Anomalies include resource utilization, environmental, and interface-level errors, and are color coded based on severity:

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

In the **Anomaly Score** Summary area the total nodes are displayed. Depending upon your configuration, you may see a different display. For NDFC VXLAN sites, the breakdown shows **Leaf Nodes** and **Spine Nodes**. For NDFC Classic sites, the breakdown shows only **Nodes**.

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 • Application • Environmental • Statistics • Endpoints • Connectivity Analysis • Bug
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
Total Controllers	Displays the total number of controllers in your network.
Total Switches	Displays the total number of switches in your network.
[Critical | Moderate | Healthy] Devices	Displays the total number of devices determined to be in one of the following categories: • Critical Devices • Moderate Devices • Healthy Devices Device counts in the higher category (Critical is highest) appear in the displayed count. If no devices are currently in the Critical category, then the device count of the Moderate category is displayed. If no issues are detected in any device, then the device count of the Healthy category is displayed.
Advisories	Displays the total number of advisories delivered for software and hardware in your network.

Property	Description
Issues By Severity	Displays the total number of issues (anomalies, bugs, and PSIRT notices) delivered for software and hardware in your network.

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.
Nodes	Displays the total number of nodes in the site with anomalies. NOTE: Depending upon your NDFC configuration, you may see a single **Nodes** count or a breakdown for **Leaf Nodes** and **Spine Nodes**.

- 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 the node number to view the details of the individual nodes.

Topology Tab

The Cisco Nexus Dashboard Insights dashboard provides access to the topology view of all the nodes with anomalies in the site.

Click **Site Dashboard** > **Topology** tab on the right dashboard pane.

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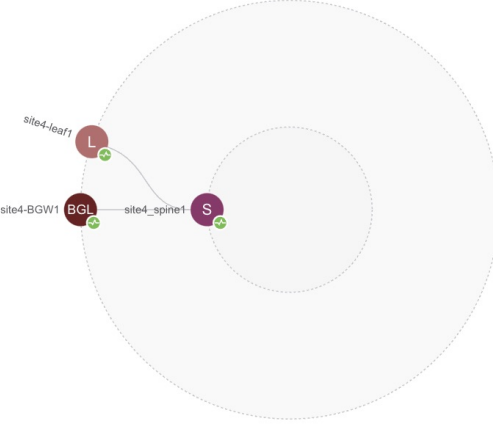
Use the zoom in capability to narrow down on portions of the infrastructure based on logical constructs such as EPG, VRF, Tenant.

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

- Name - Display only nodes with a specific name.

- VRF - Display only nodes from a specific VRF.

- Endpoint - Display only nodes for a specific endpoint.

- IP - Display only nodes for a specific IP address.

Use the operators to filter the refinement.

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

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

Topology Tab Limitations

Nodes that do not have LLDP information are not shown 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.
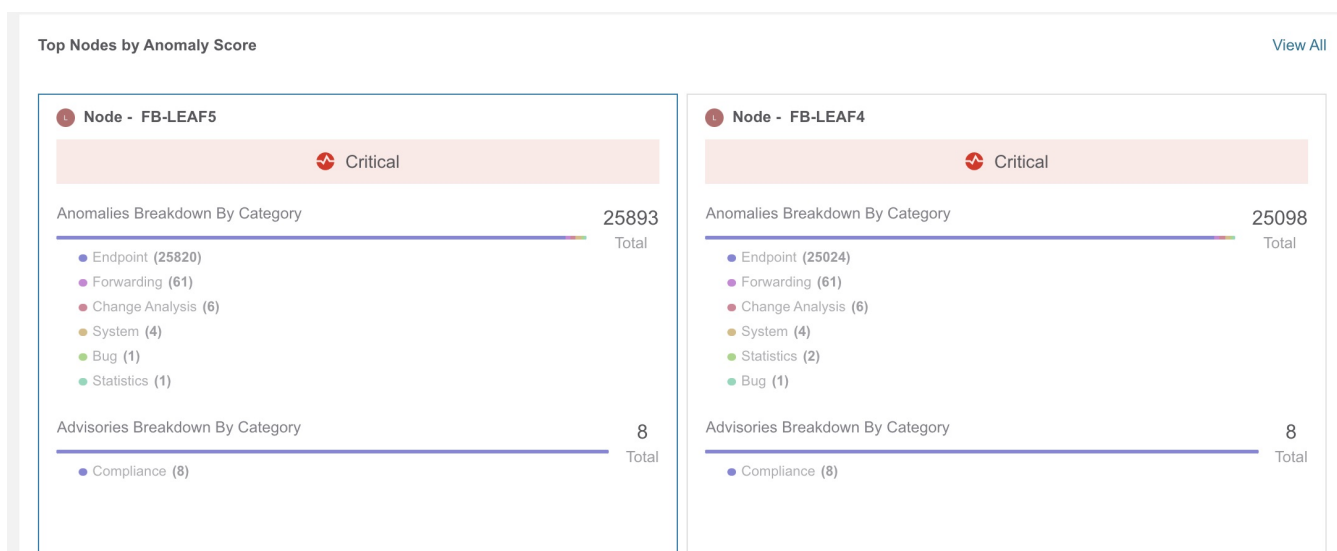
Anomaly Score and Anomaly Precedence

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

Guidelines and Limitations

- When the Device Connector is unclaimed from the on-premise GUI Nexus Dashboard Insights, the Device Connector must be unclaimed from Intersight for Log Collector's connected TAC functionality to work.

- NDFC allows `network-admin` and `network-operator` roles to assign read or write access for specific fabrics. Cisco Nexus Dashboard Insights displays only those fabrics that are granted permission.

- Nexus Dashboard Insights does not allow RBAC role on NDFC.

- The Telemetry Manager/Policy Gateway takes about 10 minutes to detect the site mode changes in NDFC from managed mode to monitored mode or vice versa.

- To enable telemetry on monitored site through Nexus Dashboard Insights, you must first delete all existing telemetry configurations on all the nodes in the monitored site before you enable this site from Nexus Dashboard Insights. The telemetry then assigns the receiver IP addresses to these nodes, which the Data Collection Setup page displays. The telemetry configuration will not push any telemetry configurations to the nodes because they are monitored. Therefore you have to check the receiver IP addresses from the Data Collection Setup page and must configure the nodes manually.

- For flow telemetry 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.

- For instances where one or more sites do not recover from disabling state, you must stop and restart Nexus Dashboard Insights in Cisco Nexus Dashboard. This will recover the failed disable state.

- The vPC domain ID for different vPC pair can not be the same across a fabric, when the Nexus Dashboard Insights is in managed or monitored mode on Cisco Nexus Dashboard.

- Cisco Nexus 7000 switches support only software telemetry in default VDC. Software telemetry fails to get enabled if the default VDC does not have modules and interfaces.

- You must create Layer 2 VNI Switch Virtual Interfaces on every leaf switch, Border Leaf, and Border Gateway for Nexus Dashboard Insights flow path stitching to function and display correct VNI information. This symmetric configuration may not be required for forwarding but is required for Nexus Dashboard Insights to obtain the fabric information.

- A Switch Virtual Interface must be configured for all host-facing VLANs. This enables Nexus Dashboard Insights to locate the corresponding VNIs irrespective of routed or bridged flows.

- 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.

- 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.

Cisco Nexus Dashboard Insights Topology

The Nexus Dashboard Insights on NDFC supports the following topologies:

- Leaf switch-Spine switch for 2-HOP and 3-HOP flow telemetry correlation.
- Leaf switch-Spine switch-Superspine switch for 3-HOP and 4-HOP flow telemetry correlation.

The following illustration describes the Leaf switch-Spine switch topology for 2-HOP flow telemetry correlation.
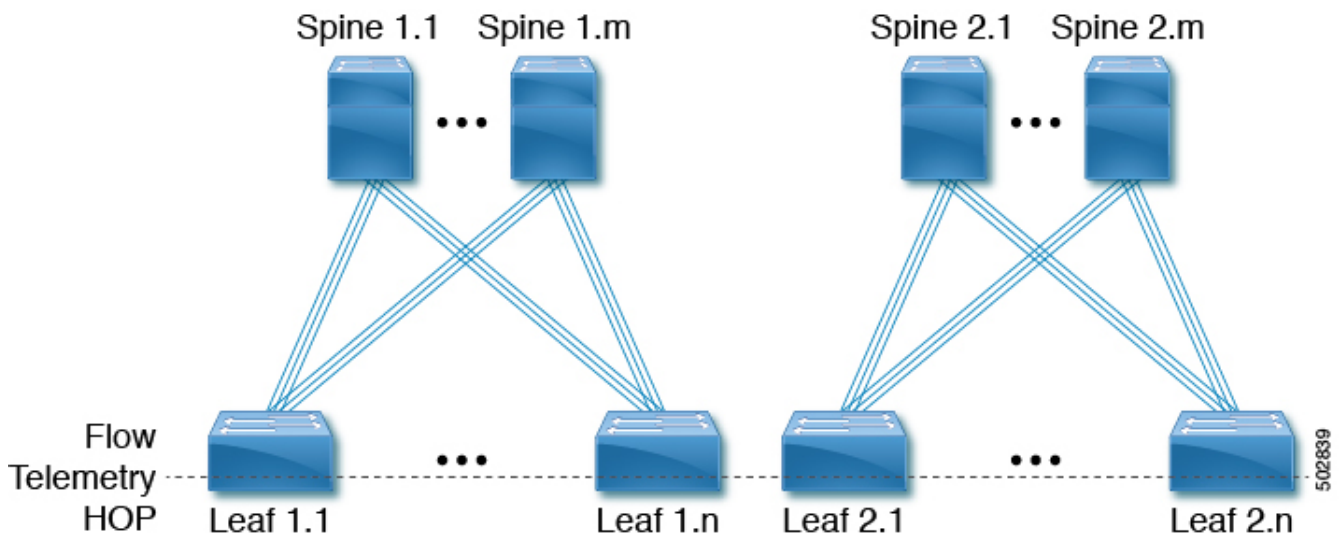
The Flow Telemetry HOP line crossing every switch in the illustration represents the switches that are capable of exporting the Flow telemetry data. For example: With the flow telemetry HOP line, the packet flows from Leaf 1.1 to Leaf 1.n are considered as 2 flow telemetry hops.

The following illustration describes the Leaf switch-Spine switch topology for 3-HOP flow telemetry correlation.
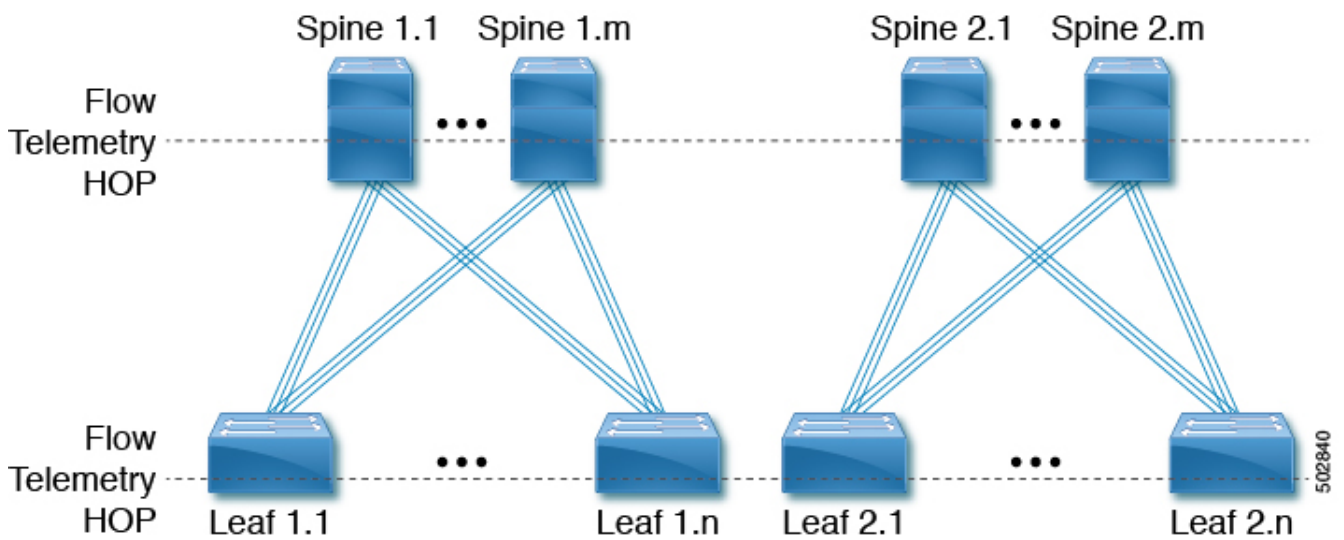
The Flow Telemetry HOP line crossing every switch in the illustration represents the switches that are capable of exporting the Flow Telemetry data. For Example: With the two flow telemetry HOP lines, the packet flows from Leaf 1.1 to Spine 1.1 and then to Leaf 1.n are considered are 3 flow telemetry hops.

The following illustration describes the Leaf switch-Spine switch-Superspine switch for 3-HOP flow telemetry correlation.
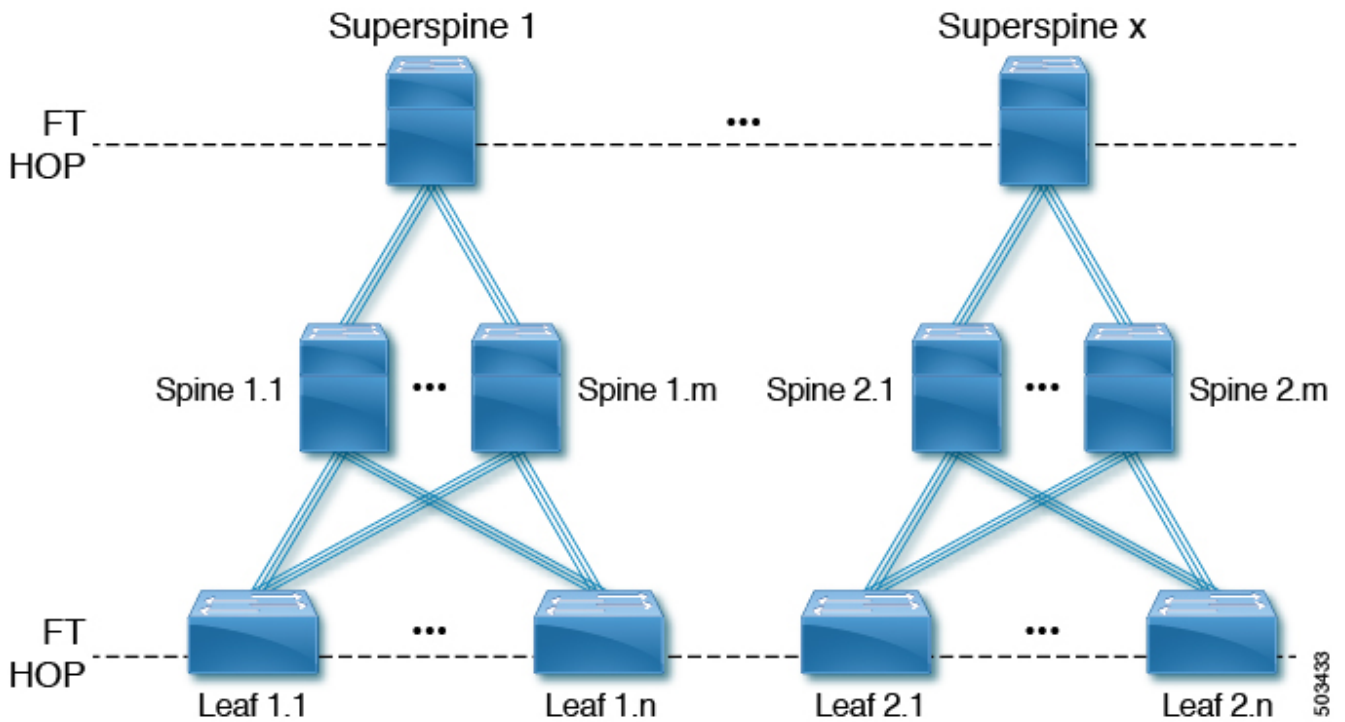
The Flow Telemetry HOP line crossing every switch in the illustration represents the switches that are capable of exporting the Flow Telemetry data. For Example: The packet flows from Leaf 1.1 to Superspine-1 and then to Leaf 1.n are considered as 3 flow telemetry hops.

The following figure describes the Leaf switch-Spine switch-Superspine switch for 4-HOP flow telemetry correlation.
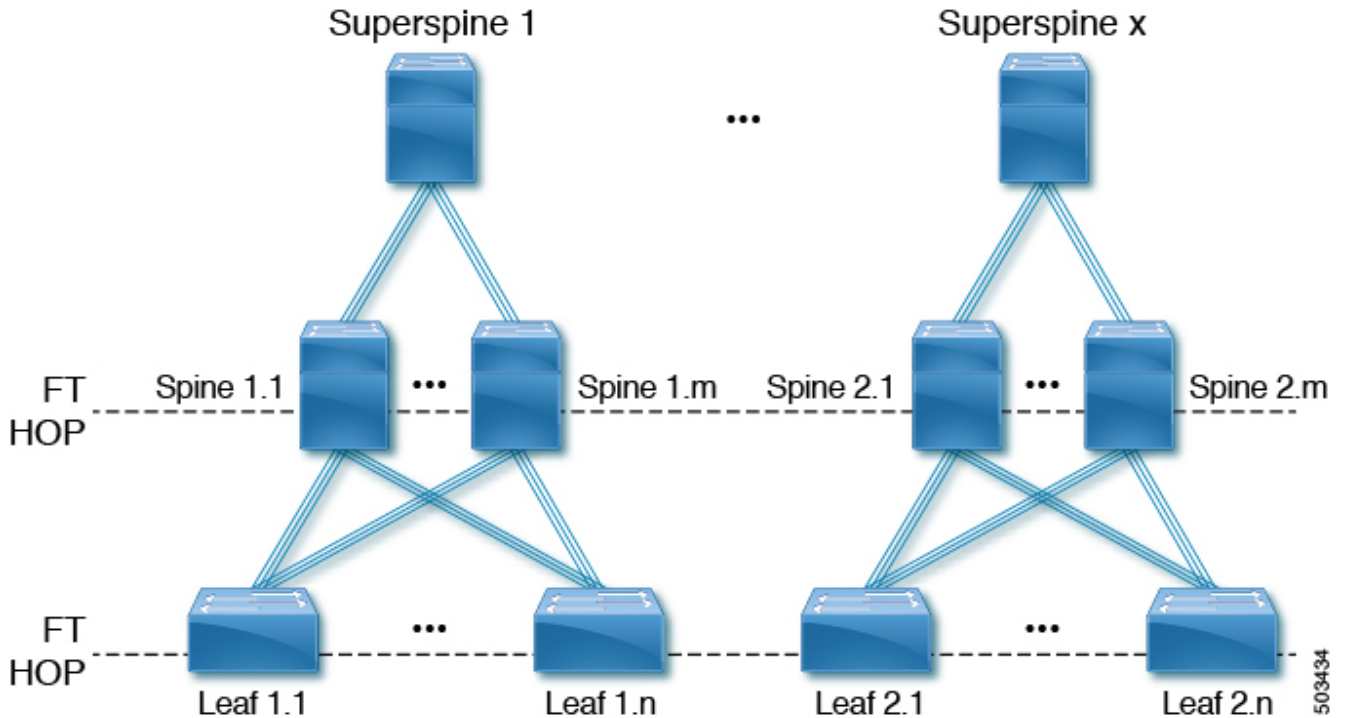
The Flow Telemetry HOP line crossing every switch in the illustration represents the switches that are capable of exporting the Flow Telemetry data. For Example: With the two flow telemetry HOP lines, the packet flows from Leaf 1.1 to Spine 1.1 and then to Spine 1.m to Leaf 1.n are considered as 4 flow telemetry hops.

Supported Scenarios

The Nexus Dashboard Insights topology supports the following scenarios.

VXLAN

- vPC on leaf switch
- Border spine switch
- Border leaf switch
- IR or Multicast underlay
- EBGP or IBGP
- IPv4 underlay
- IPv6 underlay

Legacy/Classic LAN

- vPC on leaf switch
- IPv4 or IPv6

Supported Roles

The Nexus Dashboard Insights topology supports the following roles.

VXLAN and Classic LAN

- Leaf switch
- Border switch
- Access
- Spine switch
- Border spine switch
- Aggregation
- Border gateway for spine switch
- Superspine switch
- Border Superspine switch
- Core router
- Edge router
- Border gateway Superspine switch

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 either select and analyze sites that are part of a Site Group, or you can upload files to be part of a Site Group and analyze them.

- 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 available 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.

> ℹ️ If you are configuring a Site Group to use SR-MPLS Flows (Beta feature), in the steps below, when you configure the **Fabric Type** field, you must select **SR-MPLS**. For more details, see the Cisco Nexus Dashboard Insights Configuring the Basics for Day 0 Setup and SR-MPLS Flows - Beta Feature.

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**.
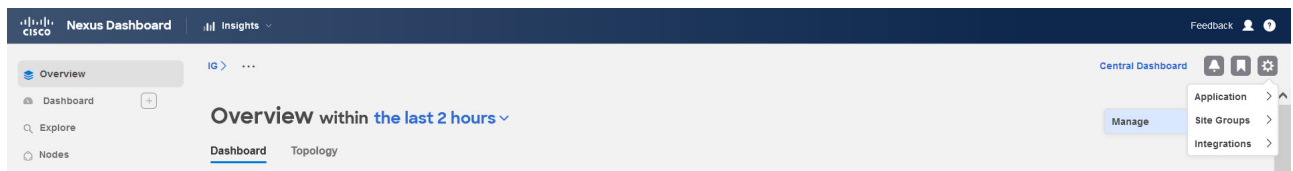
3. In the **Manage Site Groups** page, click **Add New Site Group**.

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 site/s are added in the 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 ellipses icon next to it and choose **Configure Site Group**.
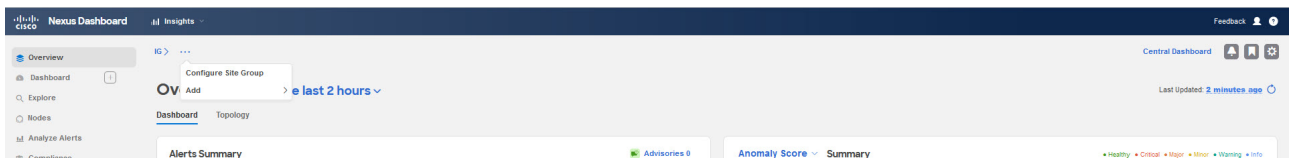
3. In the **Configure Site Group** page, perform the following actions:

   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 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 NDFC clusters for a series of REST API and CLI calls. The Nexus Dashboard Insights data collection script for NDFC supports only out-of-band management connectivity. 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 NDFC, spine switches, and leaf switches. The readme.md file is available inside the same zip file with the script file. The script is downloadable directly from the Nexus Dashboard Insights Settings icon.

The workstation on which the script is being launched must have out-of-band management connectivity to the Cisco ACI and NDFC clusters. Make sure that every node in the NDFC 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. 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 6.0.1. You will need the exported configuration file from Cisco NAE 5.1 setup to run this script.

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, choose **Settings** > **Application** > **Download Offline Collection Script** to download the Python script. Run the downloaded script to collect the data for assurance.
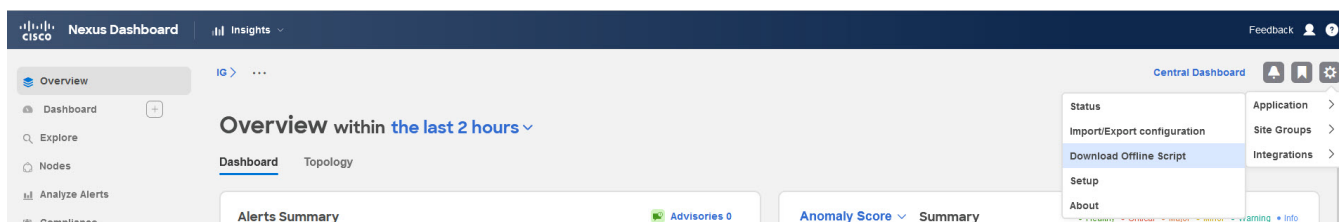
> ℹ️ The python offline data collection script is only supported on Mac OS or CentosOS. Running the script from a Windows server will result in an error and Cisco Nexus Dashboard Insights will indicate that the APIC version is unsupported.

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.

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

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**.
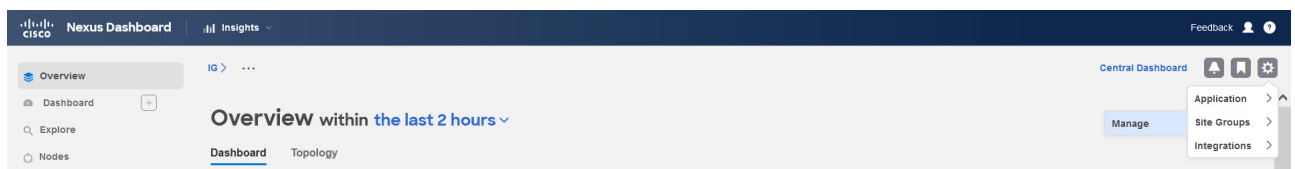
2. In the **Manage Site Groups** page, click **Add New Site Group**.

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 ellipses icon next to the selected Site Group, 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 NDFC 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 NDFC 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 for uploaded files, when you upload a file in a specific Site Group, you cannot associate that file with another Site Group.

- Alert 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 2 hours.

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 three dots to the right of 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 three dots 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 three dots 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.

> ℹ️ 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 three dots 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 ellipses icon next to your Site Group > **Configure Site Group**.

3. In the **Configure Site Group** page, click the **File Management** tab.

4. Click the delete icon to the right of the site you want to delete.

> ℹ️ 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.

- DNS Integration
- About AppDynamics Integration
- vCenter 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 and best practices follow 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. Default best practices is scheduled for once a day starting at Monday 5 AM (5 hours after the bug scan job).

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. Default best practices is scheduled daily at the time 5 hours after the bug scan time. The schedule will loop back running daily at 5 AM for every 5 sites.

Table 2. Example

Site Number	Bug Scan Schedule	Best Practices Schedule
Site 1	Once a week starting Monday at 12 AM	Once a day starting at 5 AM (12+5)

Site Number	Bug Scan Schedule	Best Practices Schedule
Site 2	Once a week starting the closest Monday at 6 AM	Once a day starting at 11 AM (6+5)
Site 3	Once a week starting Monday at 12 PM	Once a day starting at 5 PM (12+5)
Site 4	Once a week starting Monday at 6 PM	Once a day starting at 11 PM (6+5)
Site 5	Once a week starting Tuesday at 12 AM	Once a day starting at 5 AM (12+5)

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.

  When you navigate to the **Configure Site Group** > **Bug Scan** page, the default frequency rate is set based on the number of sites present at the time of site onboarding. If you are experiencing job failures due to overlapping jobs or the frequency being set to a duration shorter than the time required to complete the jobs, you can adjust your jobs as follows:

  Increase the frequency interval time to prevent job overlap and enable the scheduler to complete one job before the next is added to the scheduler queue. It is recommended to establish a weekly schedule with a start time computed based on the estimated time it takes for the previous job to complete, considering the fabric. The estimated time varies based on the number of devices present in the fabric, which are detailed in the table below.

Fabric Size	Estimated Time Taken
Nodes < = 50	14 hours
Nodes < = 100	28 hours
Nodes < = 350	48 hours
Nodes < = 500	68 hours

- 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. Click the ellipses icon 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**

   > ℹ️ 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. Click the ellipses icon 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.

Best Practices

You can schedule or run a Best Practices job on your network. Nexus Dashboard Insights collects technical support information from the site and runs them against known set of signatures and then flags the defects that are not compliant. Nexus Dashboard Insights also generates an anomaly list for the customer. See Analyze Alerts for more information.

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

See Default Bug Scan for information about schedule.

Schedule Best Practice

1. From the Site Group menu, select a Site Group or site.

2. Click the ellipses icon next to the Site Group, choose **Configure Site Group** > **Best Practice**.

   The **Best Practices** page appears. By default, best practice is enabled for a site. The **General** table displays all the sites.

3. Click ✎ to schedule a best practice job for the selected site.

4. Select the Start Time, Repeat Every, End On, End Date.

5. Click **Save**.

6. Click **Scan Now**.

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

8. Click the job in the table for the side pane to display additional job details.

9. Click the ⬚ icon to display **Best Practice** status page.

10. (Optional) Select an In Progress job and click **Stop** to stop a job.

On-Demand Best Practice

Use this procedure to run an on-demand best practice.

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** > **Best Practice** to run an on-demand best practice on the selected sites.

   The **Best Practice** page appears. By default, best practice is enabled for a site.

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

   The **History** table displays best practice 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 **Best Practice** status page.

6. (Optional) Select an In Progress job and click **Stop** to stop a job.

Collection Status

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

The **Collection Status** page displays the collection status for a node and the features supported and unsupported for each node. For each node, the collection status for categories such as resources, environmental, statistics, endpoints, and events are displayed.

Configuration Anomalies

The **Configuration Anomalies** page displays the system anomalies related to configuration of a site group.

Export Data

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.

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.

Export Data Guidelines and Limitations

- You can configure up to 10 emails per day for periodic job configurations.

- Intersight connectivity is required to receive the reports via email.

- A maximum of 5 exporters for Kafka Export is supported.

- Before configuring your Kafka Export, you must add the external Kafka IP address as a known route in your Nexus Dashboard cluster configuration.

- Nexus Dashboard supports Kafka export for Flow anomalies. However, Kafka export is not currently supported for Flow Event anomalies.

- Make sure all configuration in the *Message Bus Configuration* and *Email* page are removed before disabling Software Telemetry on any fabric and removing the fabric from NDFC.

- 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 Run Assurance Analysis.

Configure Kafka Exporter

Use the following procedure to configure the Kafka exporter:

1. In the **Overview** page, at the top, choose your Site Group.

2. Click the ellipses icon 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 **Site Name** field, select the appropriate site.

   b. In the IP Address and Port fields, enter the Kafka broker IP address and port.

c. In the **Mode** field, select the security mode. The supported modes are Unsecured, Secured SSL and SASLPLAIN mode.

d. In the **General Settings** area, enter the name and topic name, where the data must be sent, and 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.

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 ellipses icon 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.

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.

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.

Starting from Nexus Dashboard Insights release 6.1.1, you can also view the latest reports on the Conformance Dashboard. See Software and Hardware Conformance Dashboard.

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 and end of PSIRT 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* and the end of PSIRT date 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.

Software and Hardware Conformance Dashboard

From the navigation pane choose **Compliance** > **Software/Hardware Conformance** to access the Conformance dashboard.

- The Software and Hardware Conformance dashboard displays a graphical view of the status of the overall conformance inventory for a site. You can view the conformance for 18 months for a software release, hardware platform, and a combination of software and hardware conformance.

  In the Conformance Dashboard, the nodes are classified into the Healthy, Warning, and Critical severities based on the software release or hardware platform EOL dates and end of PSIRT dates.

- The page also displays the conformance of nodes in a tabular format.

  The **Nodes** table displays information such as name of the node, overall conformance, software conformance, hardware conformance, IP address, serial number, model number, and software version. The table is sorted by overall conformance of the nodes. Click a node to view additional

details.

- Use the filter bar to filter the nodes by name, overall conformance, software conformance, hardware conformance, IP address, serial number, model number, and software version.

  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.

- Click **View Detailed Report** to view the detailed report. The **Conformance Report** page displays information such as general information, conformance inventory, software conformance, hardware conformance, overall conformance, node details, and module details

  - From the **Actions** menu, click **Print/Download** to download the report as a PDF.

  - From the **Actions** menu, click **Schedule Email** to subscribe to the latest reports by configuring an email scheduler. See Configure Email.

Syslog

Starting from release 6.1.1, Nexus Dashboard Insights supports the export of anomalies and advisories in syslog format. You can use this feature to develop network monitoring and analytics applications on top of Nexus Dashboard Insights, integrate with the syslog server to get alerts, and build customized dashboards and visualizations.

After you choose the site where you want to configure the syslog exporter and you set up the configuration for syslog export, Nexus Dashboard Insights will establish a connection with the syslog server and send the data to the syslog server.

Nexus Dashboard Insights will read the anomalies and advisories from the Kafka message bus and then export this data to the syslog server. With syslog support, even if you do not use Kafka, you will be able to export anomalies to your third-party tools.

Guidelines and Limitations for Syslog

If the syslog server is not operational at a certain time, messages generated during that downtime will not be received by a server after the server becomes operational.

Configure Syslog

Use the following procedure to configure syslog to enable exporting anomalies and advisories data to a syslog server:

1. In the **Overview** page, at the top, choose the appropriate Site Group and click **Configure Site Group**.

2. In the **Configure Site Group** page for your Site Group, click the **Export Data** tab.

3. In the **Syslog** field, click **Add New**.

4. In the **Syslog Configuration** dialog box, in the **Credentials** area, perform the following actions:

a. In the **Site Name** field, click **Select Site** and choose the site name.

b. In the **IP Address** and **Port** fields, enter the IP address and port details.

c. In the **Transport** field, from the drop-down list, choose the appropriate option. The choices are **TCP**, **UDP**, and **SSL**.

d. In the **Facility** field, from the drop-down list, choose the appropriate facility string.

A facility code is used to specify the type of system that is logging the message. For this feature, the **local0-local7** keywords for locally used facility are supported.

5. In the **Mode** field, click the toggle button to choose between **Unsecured** and **Secured SSL**.

If you choose Secured SSL, you will be required to provide a server CA certificate.

6. In the **Configuration** area, enter a unique name for the syslog configuration for export.

7. In the **Collection Settings** area select the desired severity options.

The options available are **Critical**, **Error**, **Warning**, and **Info**. **Major** and **Minor** anomalies and advisories in Nexus Dashboard Insights are mapped to **Error**.

8. Click **Save**.

After you complete the configuration, in the **Configure Site Group** page under **Export Data** tab, the **Syslog** area will display the details of your configuration.

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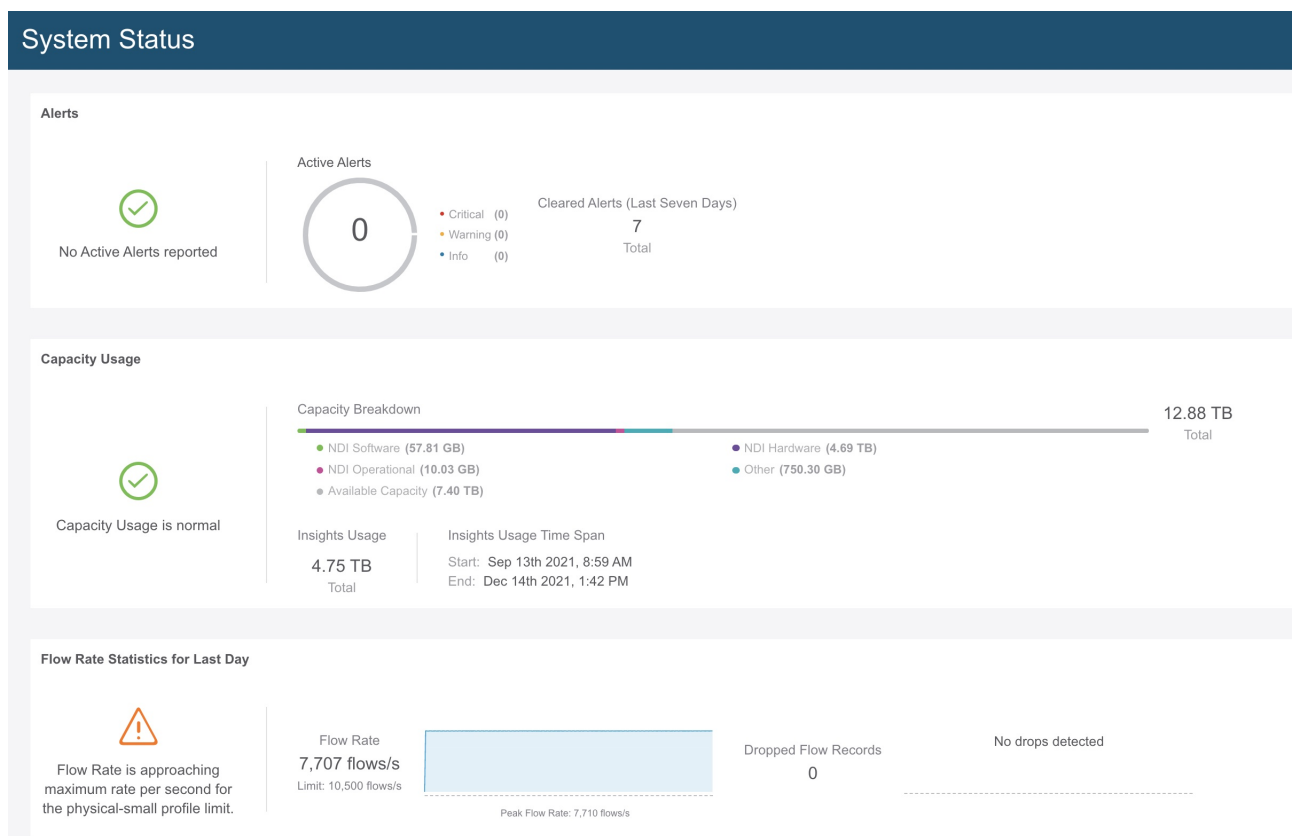
   The Alerts area displays the active and alerts cleared in the last 7 days. The Capacity Usage area displays the capacity usage status, capacity breakdown, and timespan. The Flow Rate Statistics area displays the flow rates and tracks the number of dropped flows.

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
  - Email
  - Message Bus Configurations
  - Syslog
- Flow Rules
- User Preferences
- Integrations

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.
- For any configuration, the passwords or certificates will either not be exported or will be encrypted for security reasons. You need to enter them again after importing the configurations.
- 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 an 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 an 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.

- 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.

- **Export Settings** import will fail if Nexus Dashboard Insights is not connected to Cisco Intersight. Nexus Dashboard Insights must be connected to Cisco Intersight before importing **Export Settings**.

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, Sites Groups, Alert Rules, Compliance, Export Settings, Flow Rules, Integrations, and User Preferences are exported.

5. The **Import/Export** table displays information of the exported files such as status, type, and content.

6. Click Click ⋯ and choose **Download** once the export job status has moved to **Completed**. The exported configuration is downloaded as a compressed file.

7. Click 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 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.

> ℹ️ 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

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

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

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

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

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

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

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

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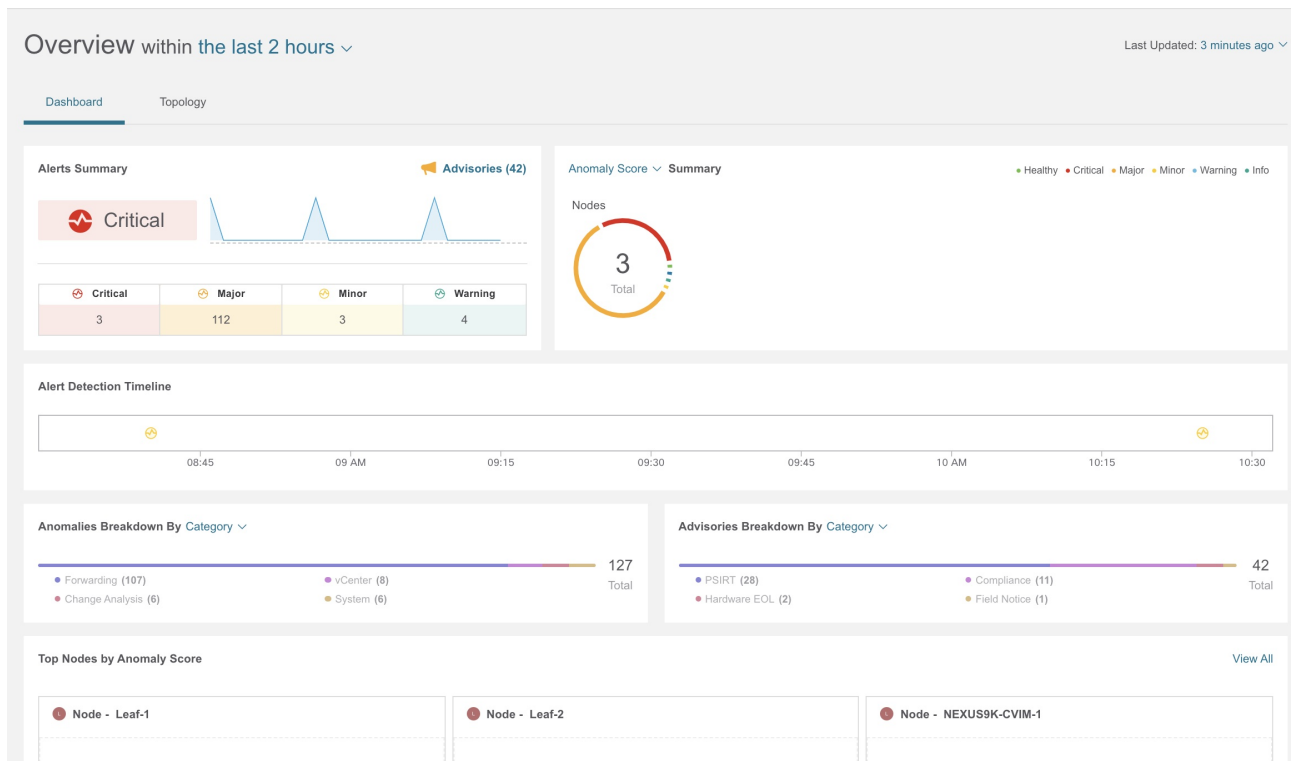
3. In the Site Groups area, click a Site Group to view specific information about the Site Group in the **Overview** page.

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**.

Overview

Dashboard

Alerts Summary

Cr

	Critical
	1

Alert Detection Ti

Anomalies Break

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.
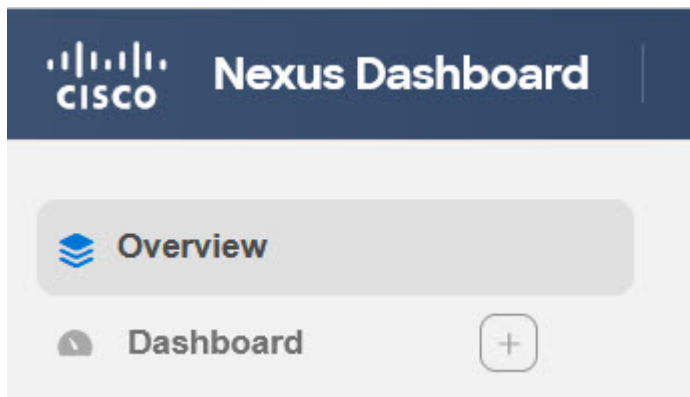
2. Enter a unique name. Click ✓ to save.

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.
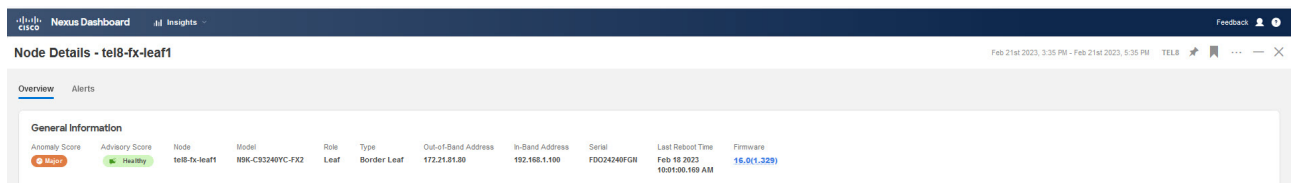
4. In the **Pin to Dashboards** dialog-box, complete the following:

   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 NDFC with NX-OS

The **Explore** feature analyzes a configuration snapshot from Cisco NX-OS to enable data center operators and architects to:

- Explore the NX-OS networking assets

- 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 with Cisco NX-OS.

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

> ℹ️ Currently, to explore NX-OS networking assets that are available through a NDFC Site Group, the **What Query** is supported. The **Can Query** and the **How Query** are not supported.

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

Examples for NX-OS:

1. What VLANs are associated with VRF: secure

2. What EPs are associated with INF: eth1/3 | leaf-1 or VRF: vrf_1 | leaf-1

3. What VLANs are associated with EP:100.x.x.x | vrf_secure

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.

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 **Explorer** 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
```

- For NX-OS fabric, the **Explore** feature provides a switch-wide view of VRFs, VLANs, interfaces, endpoints and leaf switch resources in the fabric. It also provides Layer 2 VNI and Layer 3 VNI as resources.

- Resource aggregation is supported for VLAN and VRF resources. With resource aggregation, resources like VRF and VLAN are discovered for the entire fabric and all the leaf switches are aggregated by these resources. If you query **What VLANs are associated with any?** in the **Query Results** area, you will see a list of all the VLANs available across the fabric. EP and LEAF counts will be aggregated by VLAN and you can find all the EPs and LEAFs associated to a single VLAN by clicking the aggregated resource counts. Additionally, as the VLAN and VRF queries are fabric wide, if you want to explore resources for a VLAN on a specific leaf switch, you must use the **AND** operator in your query. For example, **What EPs are associated with VRF:vrf-vrf_51020 and LEAF:CANDID-SYS-S1-L1**.

- A networking asset, such as interfaces on a leaf switch, must be associated with an endpoint in the leaf switch for you to be able to explore it in **Explore**.

- When a VRF is not operational, **Explore** discovers the endpoints as a Layer 2 endpoint.

- Endpoints are discovered as Layer 3 or Layer 2 endpoints. All endpoints present in a VLAN are discovered, and other endpoints are ignored.

- In **Explore** if you do not see endpoints or other network assets, look for system anomalies in the associated snapshot. Verify that the collection has succeeded in all the leaf switches. If the collection failed, it may result in endpoints not being discovered.

- For NX-OS with NDFC Site Group, only IPv4 endpoints support in **Explore** is available. IPv6 endpoints support in **Explore** is currently not available.

- **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).
- The Explore feature for NDFC based fabric must have endpoints available in VNI or VRF for certain WHAT queries to work, since the Explore feature is based on the endpoints learnt on VNI and/or VRF. If the endpoints is not available, the What query for VRF or L3 VNI will not display accurate results.

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.

5. 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. For example, **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 NX-OS networking assets.

See Analyze Alerts for details about anomalies and alerts.

Supported Queries

The following table lists the queries supported by the **Explore** feature for NX-OS.

Supported What Queries

Table 3. Supported What Queries

Query	Entity	Operator	Entity
What EPs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
What INFs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
What LEAFs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

Query	Entity	Operator	Entity
What VLANs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
What VRFs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
What L2VNIs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

Query	Entity	Operator	Entity
What L3VNIs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

Query	Entity	Operator	Entity

Multi-Site Traffic Path - Beta Feature

Multi-Site Traffic Path Trace and Fault Correlation

> ℹ️ This is a **Beta** feature. We recommend that you use features marked as **Beta** in your test environments but not in production deployments.

To monitor flows, you can stitch together flows from across two different sites in a Site Group into one single view. This enables you to have end-to-end views for the paths and end-to-end details for the particular flow and the latency information for that flow.

Use cases for Multi-Site Traffic Path Trace and Fault Correlation:

- You can correlate flows across sites and display flow details with stitched paths.

- You can monitor flows across sites and generate inter-site anomalies that are trigger based.

- You can monitor flows across sites and provide the end-to-end latency.

Configure Multi-Site Traffic Path Trace and Fault Correlation

In the **Explore** area, within a Site Group, you can view the flow path between two ports, their IP addresses, and their VRFs.

1. In the Cisco Nexus Dashboard Insights GUI **Overview** page, in the left Navigation pane, click **Browse** > **Flows**.

2. Click the desired node and then click the Details icon in the right top corner of the sidebar to display to view the **Flow Details** page.

3. In the **Flow Details** page the **Flow Record Information** and **Aggregated Flow Information** are displayed.

4. In the **Flow Path Summary** area, in the flow path, click the **Multi-Site Flow - View in Flow Explorer** tab to go to the **Explore** page.

In the **Explore Flows** page, the flow information filters in the Search field auto-populate, and you can see in which sites the flows exist. The **View** query area displays the information with the source IP address, source port information and the destination IP address, destination port information. **Explore** finds and returns all the sites where this flow was discovered for the specified VRF.

Next, select the appropriate source and destination sites to view their aggregated information, path summary, and anomalies. You must specify which site you want as your source and which site you want as your destination. Cisco Nexus Dashboard Insights will stitch the information based on your input. You can only choose one source and one destination at a time to stitch together this information. Based upon your selection of source and destination sites, Cisco Nexus Dashboard Insights returns the names of the sites that it finds.

In the **Flow Path Summary** area, details for the two sites are displayed in the **Explore** page as a

graphical flow path that displays the end-to-end information, from source to destination. You can see the first site with the endpoint and a set of nodes and it is connected to the second site with the second set of nodes followed by the endpoint. It will also identify the firewall in the path if a firewall is present. The graph also captures the end-to-end flow path network latency.

Specific details for the source and the destination sites are displayed in each of the **Aggregated Flow Records from** tables. In the **Anomalies** table, choose **Aggregated** to view the aggregated anomalies for your selections flows.

> If you enter different flow details in the Search field in the **Explore** page, you can view in which sites those flow exists. Alternatively, in the **Explore** page, you can directly begin your search by entering details in the Search field for details about flows and the Flow Path across more than one site within a Site Group.

Nodes

Nodes

The *Nodes* pane displays the graph 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 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.

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

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

- 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 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, 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 and root cause the anomalies.

- 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 NDFC 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.

- 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.

- Check code - Display only anomalies with a specified check code.

- 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.

- Status - Display only anomalies for a specific status.

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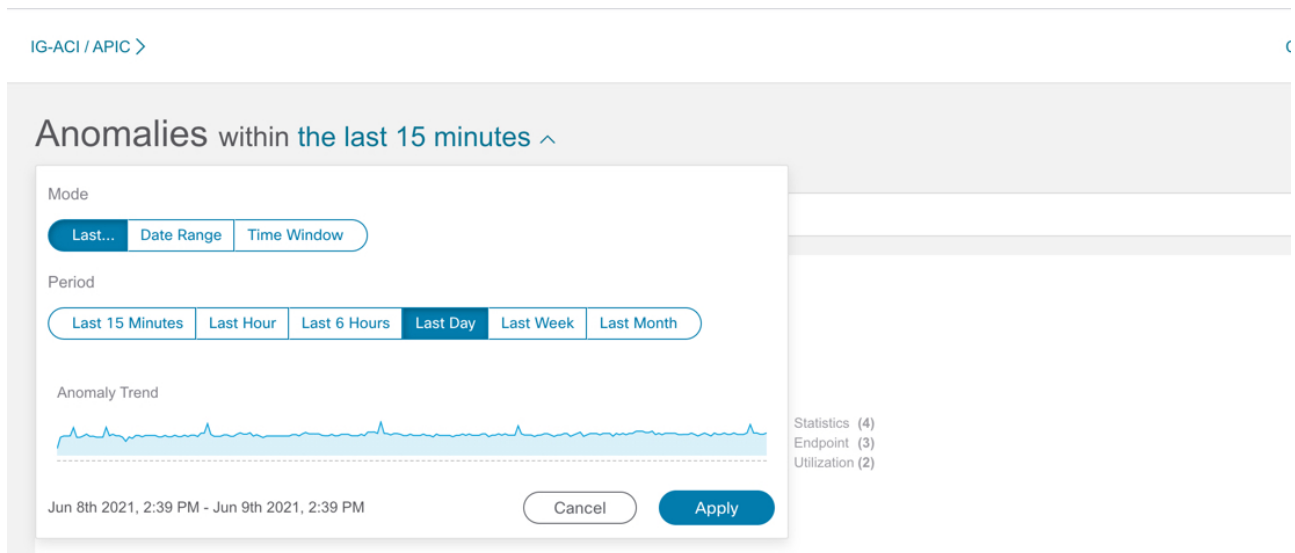
`>` - with the initial filter type, this operator, and a subsequent value, returns a match greater than the value.

`>=` - 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.

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

The **Anomalies** table displays individual, aggregated, or inter-site 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.

Filters ✎ ⊗

Anomalies By: Category ▾　　　　　　　　　　　　　　　　　　　　　　　　∧
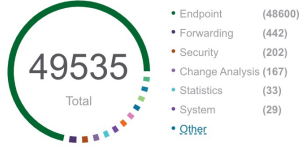
Top 10 nodes contributing to Anomalies

ifav201-apic1	🔴 Critical
ifav201-apic2	🔴 Critical
ifav201-apic3	🔴 Critical
ifav201-leaf1	🔴 Critical
ifav201-leaf10	🔴 Critical
ifav201-leaf11	🔴 Critical
ifav201-leaf2	🔴 Critical
ifav201-leaf3	🔴 Critical
ifav201-leaf4	🔴 Critical
ifav201-leaf5	🔴 Critical

49535
Total

- Endpoint (48600)
- Forwarding (442)
- Security (202)
- Change Analysis (167)
- Statistics (33)
- System (29)
- Other

Anomalies Individually ∨　　　　　　　　　　　　　　　　　　　　　　　　Actions∨

	Severity	Title	Category	Nodes	Detection Time	Last Seen Time	Description	Status	Check Codes	User State	⚙
☐	🔴 Critical	Leaf Used Interface Oper Down Admin Up	Interface `Forwarding`	ifav201-leaf9 DC-IFAV201	Jan 24 2022 07:45:58.000 AM	Mar 14 2022 10:54:37.000 PM	Leaf Interface allocated by Fabric Access Policy and consumed by EPG(…	⚠ Active	Leaf Used Interface Oper …	ⓘ ☑ 👤	..
☐	🔴 Critical	Fabric External Interface Oper Down Admin Up	Interface `Forwarding`	ifav201-spine1 DC-IFAV201	Jan 24 2022 07:45:58.000 AM	Mar 14 2022 10:54:37.000 PM	A fabric external facing interface on the spine is administratively up…	⚠ Active	Fabric External Interface …	ⓘ ☑ 👤	..
☐	🔴 Critical	Fabric External Interface Oper Down Admin	Interface `Forwarding`	ifav201-spine3 DC-IFAV201 more	Feb 02 2022 10:54:43.000 PM	Mar 14 2022 10:54:37.000 PM	A fabric external facing interface on the spine is administratively up	⚠ Active	Fabric External Interface …	ⓘ ☑ 👤	..
☐	🔴 Critical	Enforced VRF Policy Violation	VRF Security `Security`	ifav201-leaf7 DC-IFAV201 view (1) more	Mar 02 2022 10:54:43.000 AM	Mar 14 2022 10:54:37.000 PM	VRF is in enforced mode. APIC policy for implicit deny log is not enforced on Le…	⚠ Active	L T Equivalence L C Congruence C T Equivalence	ⓘ ☑ 👤	..
☐	🔴 Critical	Enforced VRF Policy Violation	VRF Security `Security`	ifav201-leaf3 DC-IFAV201 view (1) more	Jan 24 2022 07:45:58.000 AM	Mar 14 2022 10:54:37.000 PM	VRF is in enforced mode. APIC policy for implicit deny log is not enforced on Le…	⚠ Active	L T Equivalence L C Congruence C T Equivalence	ⓘ ☑ 👤	..
☐	🔴 Critical	Connected EP Learning Error	Endpoint Learning `Endpoint`	ifav201-leaf6 DC-IFAV201 view (2) more	Jan 24 2022 07:45:58.000 AM	Feb 04 2022 07:54:49.000 PM	Endpoint information is not consistent across the fabric leafs and spines.	⚠ Active	-	ⓘ ☑ 👤	..
☐	🔴 Critical	Connected EP Learning Error	Endpoint Learning `Endpoint`	ifav201-leaf6 DC-IFAV201 view (2) more	Jan 24 2022 07:45:58.000 AM	Feb 04 2022 07:54:49.000 PM	Endpoint information is not consistent across the fabric leafs and spines.	⚠ Active	-	ⓘ ☑ 👤	..
☐	🔴 Critical	Connected EP Learning Error	Endpoint Learning `Endpoint`	ifav201-leaf6 DC-IFAV201 view (2) more	Jan 24 2022 07:45:58.000 AM	Feb 04 2022 07:54:49.000 PM	Endpoint information is not consistent across the fabric leafs and spines.	⚠ Active	-	ⓘ ☑ 👤	..
☐	🔴 Critical	Connected EP Learning Error	Endpoint Learning `Endpoint`	ifav201-leaf5 DC-IFAV201 view (3) more	Jan 24 2022 07:45:58.000 AM	Feb 04 2022 07:54:49.000 PM	Endpoint information is not consistent across the fabric leafs and spines.	⚠ Active	-	ⓘ ☑ 👤	..

4. Choose one of the following:

   a. Select **Individually** 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.

    c. Select **Inter-Site** from the Anomalies drop-down list to view the Nexus Dashboard Orchestrator-associated Site Group anomalies.

5. Click the ⚙ icon to customize the columns in the table.

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

    a. Starting from release 6.1.1, you can filter anomalies by check code and the results are displayed in the anomalies table. An anomaly can have multiple check codes.

    b. Click **View More** to view all the check codes for a particular anomaly.

    c. Enter the search criteria in the search bar to search for a particular check code.

7. 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. In the inter-site view, an additional **Sites** column is displayed that lists the Nexus Dashboard Orchestrator-associated site/s in the Site Group that are affected by the anomalies.

8. Click **Analyze**. The **Analyze Anomaly** page displays the general information of the anomaly, state, impact analysis, affected object, proactive diagnostic report, mutual occurrences, and in-depth analysis. In the **Analyze Anomaly** page the check code is displayed in the **Proactive Diagnostic Report** area.

Analyze the anomaly 20 minutes ⌄ before and after ⌄

General   View More Details ⌄

Severity	Category	Sub-category	Type		Nodes	Description
😐 Major	Change Analysis	Forwarding Policy	LEAF_PROFILE_HAS_NO_INTERFACE_SELECTOR_PROFILE		ifav201-apic1 view (2) more	The Switch Profile is not associated with any Interface Selector Profile.

State   Show Anomaly Lifespan ⌄

Status	Verification Status	Acknowledgement	Assigned To	Duration	Detection Time	Last Seen Time	Cleared Time
⚠ Active	● New	☑ Unacknowledged	👤 Not Assigned	49 Days 15 Hours	Jan 24 2022 07:45:58.000 AM	Mar 14 2022 10:54:37.000 PM	-

Impact Analysis

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

Affected objects

Leaf Profile (Primary) (Unhealthy)

high_dual_fast_link_fail_over_leafs*

Proactive Diagnostic Report

Code
EPG Leaf Profile Has No Interface Selector Profile

Description
The leaf profile does not have an interface profile associated with it.

Recommendation
1. Determine if the leaf profile is needed in Fabric > Access Policies > Switch Policies > Profiles > Leaf Profiles.
2. If the leaf profile is needed, determine the correct set of interface selector profiles that should be bound to this leaf profile and make the association, or create a new interface selector profile with the correct set of interface policy groups and interface selectors.
3. If the leaf profile is not needed, determine if you can delete the leaf profile.

Tenant	App Profile	Affected EPG	Path Type	Static Port Path Binding Information	Path Binding Encap
tn-scale1-epa*	ap-ap1*	epg-epg2*	STATIC	[topology/pod-1/paths-108/pathep-[eth1/5]]*	212*
fteEvents*	ap1*	epg1*	STATIC	[topology/pod-1/paths-108/pathep-[eth1/5]]*	233*
l2mcast*	ap*	epg2*	STATIC	[topology/pod-1/paths-107/pathep-[eth1/18]]*	224*
ep_move*	ap*	epg2*	STATIC	[topology/pod-1/paths-108/pathep-[eth1/23]]*	241*

Mutual Occurrences

| Anomalies (221010) |
| Faults (11261) |
| Events (1) |
| Audit Logs (21611) |

Jan 30   Feb 06   Feb 13   Feb 20   Feb 27   Mar 06   Mar 13

Jan 30   Feb 06   Feb 13   Feb 20   Feb 27   Mar 06   Mar 13

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

e. The **Proactive Diagnostic Report** displays the check code, description, and recommendations.

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

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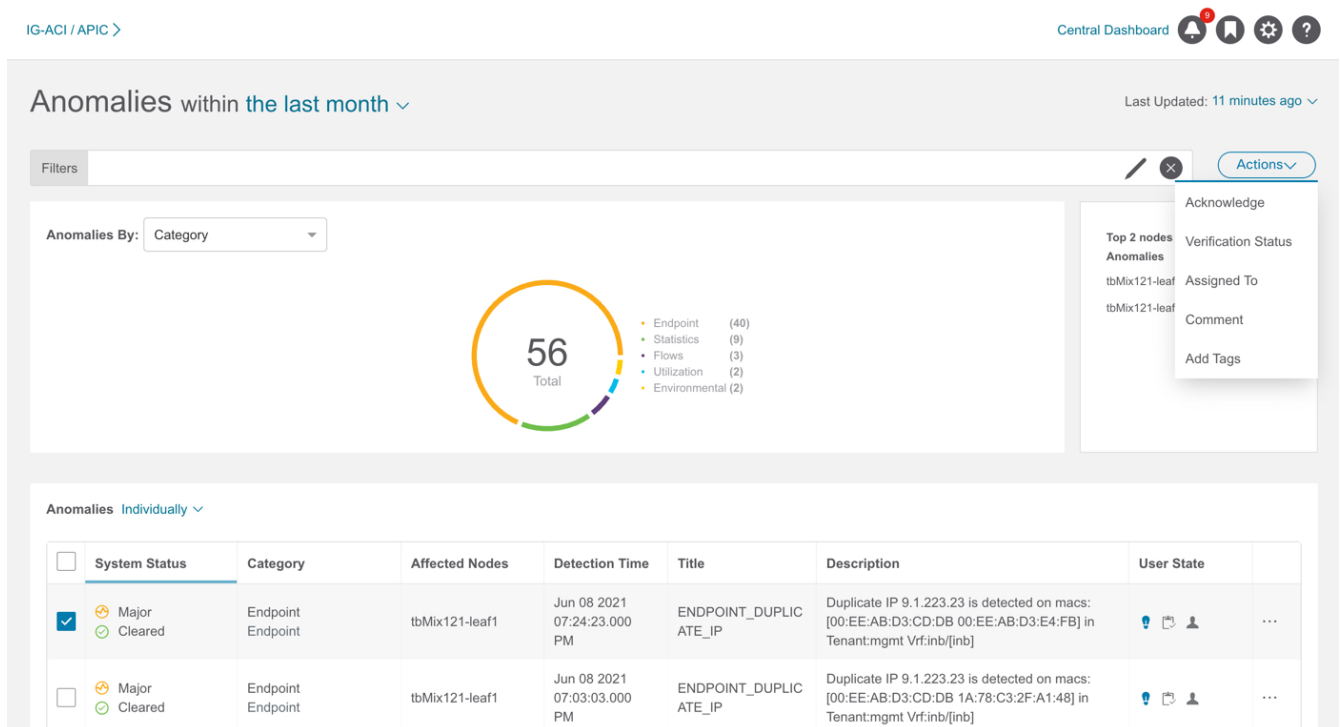
The comparison chart updates automatically and displays the resource utilization for the selected nodes with the anomalies. You can compare and analyze resources for the selected nodes with the anomalies.

8. Click the ellipses ![ellipses icon] 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 ![bookmark icon] 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.

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 Acknowledge=true filter.

> ℹ️ 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.

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. With metadata support for air-gap environment, if Nexus Dashboard is not connected to Cisco Intersight Cloud, you can manually upload the latest metadata to Nexus Dashboard Insights in a secure and trusted way. You can download the bundle updates from the Cisco DC App Center. See Metadata Support for Air-Gap Environment.

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

- Hover around Metadata Version to view the digitized defects for the metadata version in the current release. See Viewing Defect Analysis to view the digitized defects associated with the firmware version.

- Click **Update** to upload metadata for air-gapped environments. See Metadata Support for Air-Gap Environment.

Metadata Support for Air-Gap Environment

With metadata support for air-gap environment, if Nexus Dashboard is not connected to Cisco secure cloud, you can upload the latest metadata to Nexus Dashboard Insights periodically in a secure and trusted way.

You can download the encrypted metadata file from the Cisco DC App Center and upload it to Nexus Dashboard Insights to get decrypted updates on exposure to Bugs, PSIRTs, Defects, Field Notices, and End of Life Notices.

Update Metadata Version

Use this procedure to update the latest metadata version in an Air-Gap or offline environment.

1. Log in to Cisco DC App Center.

2. From the User drop-down menu, select **My Account**.

3. Click **Config Files Requests** tab.

4. Click **Request Config File**.

5. From the **Choose App ID** drop-down list, select Nexus Dashboard.

Request for Config File

Choose App Name:

Nexus Dashboard Insights ⌄

Min App Version Supported: 6.1.1

Cancel   **Request**

6. Verify the minimum supported app version and click **Request**.

   It takes approximately 15 minutes for the request to be completed. In the Config Files Request page, the generated file is displayed in the table below.

7. Select the file and click **Download** to download the file locally.

Request Id	App Name	Created At	Last Update	Status	Version	Link
2	Nexus Dashboard Insights	2022-02-25 17:47:16	2022-02-25 17:48:26	Processed	22	Download

8. Log in to Cisco Nexus Dashboard Insights.

9. Choose **Settings** > **Application** > **About**.

10. Click **Update**.

11. In the Metadata Version Update page, upload the file you have downloaded from the Cisco DC App Center.

12. Click **Done** to upload the latest metadata to Nexus Dashboard Insights.

Advisory Filters

The filter bar allows you to filters the advisories.

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

- Acknowledgement- Display only anomalies with acknowledged status.

- Category - Display only advisories from a specific category.

- Description - Display only advisories with a specified description.

- Detection Time - Display only advisories with a specific detection time.

- Last Seen Time - Display only advisories with a specific time.

- Nodes - Display only advisories for specific nodes.

- Severity - Display only advisories of a specific severity.

- Status - Display only advisories for a specific status.

- Sub-category - Display only advisories from a specific sub-category.

- Title - Display only advisories with a specified title.

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.

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.

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.

- Maximum alert rules supported across all sites is 500.

Creating Alert Rules

Use this procedure to create 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**.

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**.

Add Match Criteria

General

Site*

Select an Option ⌄

Category

Any ⌄

Sub Category

Any ⌄

Event Title

Any ⌄

Object Match Rule

⊕ Add Object Match Rule

⊕ Add Code Rule

Severity

Any ⌄

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 category, subcategory, event title, object match rule, code rule, and severity to define the attribute for the match criteria.

c. Click **Add Object Match Rule** to define the primary affected objects for the match criteria.

> ℹ️ 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 **Add Code Rule** to define the check code for the match criteria.

g. 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.

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 NDFC

Policy Delta for NDFC 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.

- When you choose a switch in the **Changed Nodes** area, in the **Policy Delta** page, the difference in the configuration between the two snapshots is displayed.

- For Policy Delta, **Audit Logs** is not currently supported.

Creating Delta Analysis

Use this procedure to create a delta analysis.

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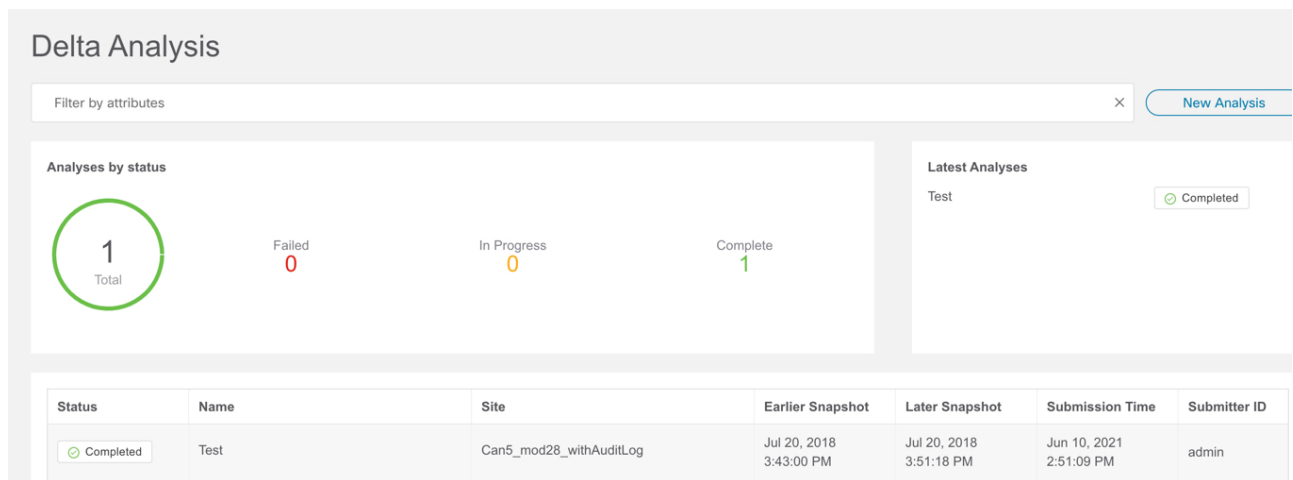
You can perform one delta analysis at a time. To perform another delta analysis, you must stop the current delta analysis and then start the another delta analysis.

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.
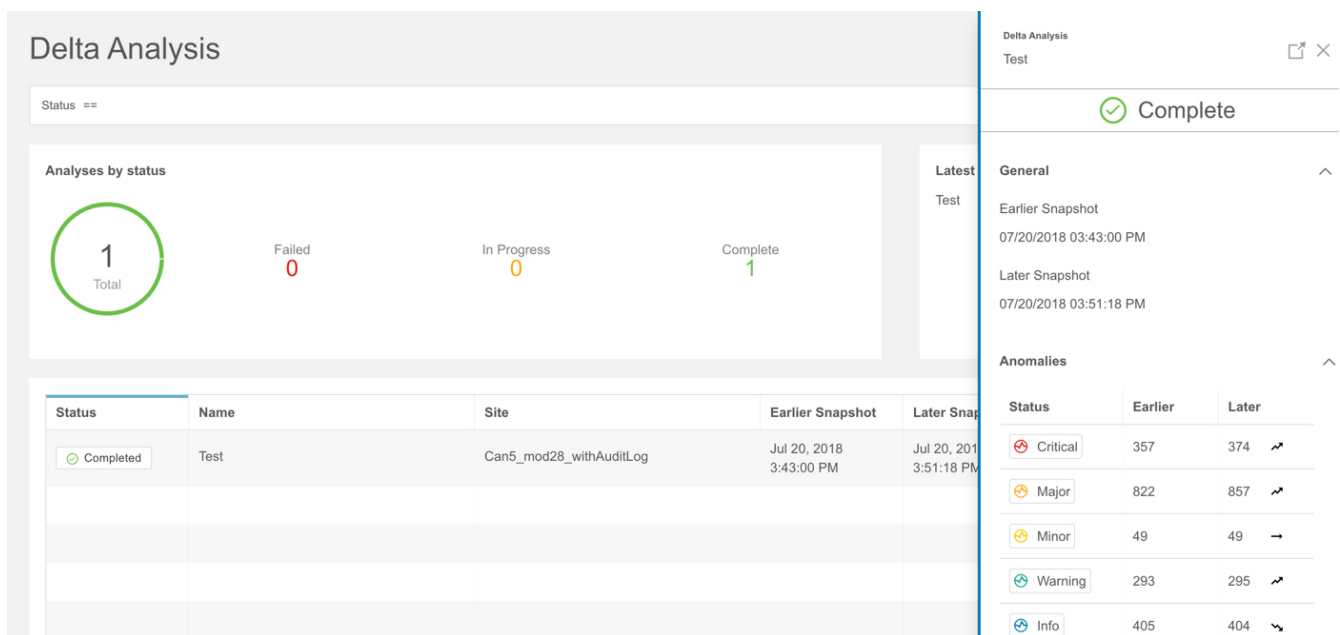
Viewing Delta Analysis

The Delta Analysis Dashboard displays a graph of analyses by status for a particular Site Group or site and displays the latest analyses.
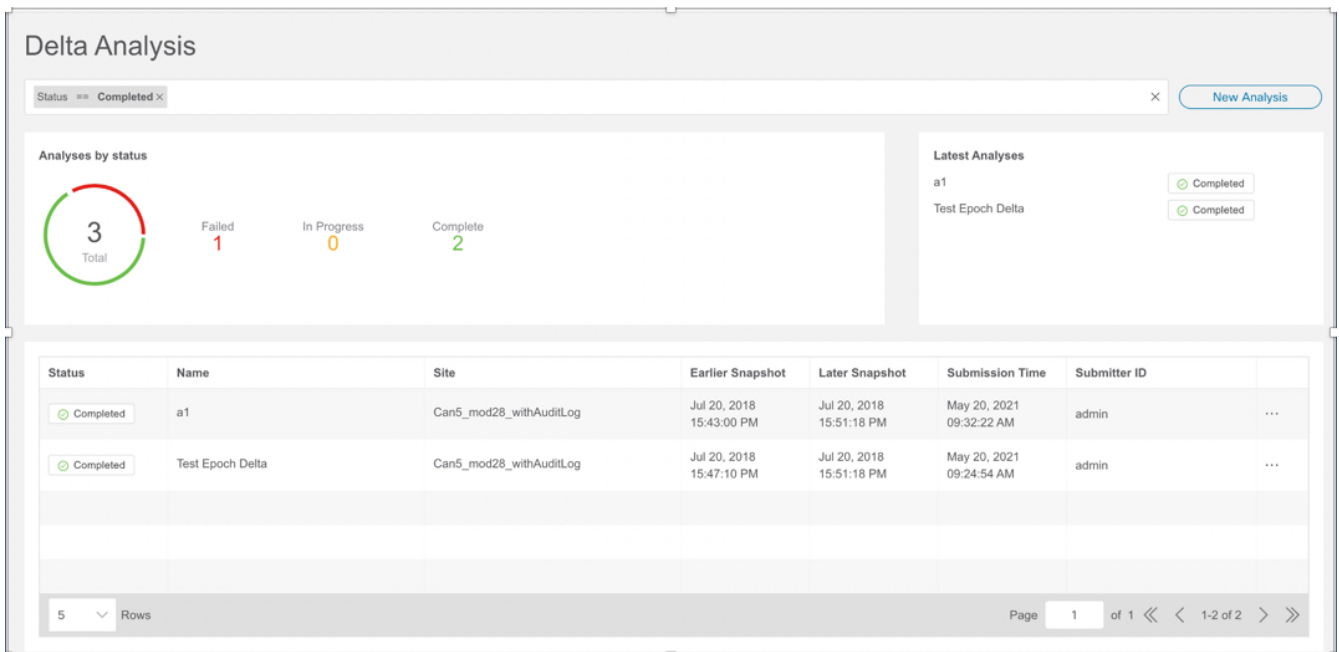
The filter bar allows you to filters the analysis by status, name, and submitter.

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	07/20/2018 03:51:18 PM	8mins 18secs
Earlier	Later	Time Range

Health Delta   Policy Delta

Anomaly Count

	Critical			Major			Minor			Warning			Info			Total	
1	356	18	1	821	36	0	49	0	0	293	2	9	396	8	11	1.9 K	64

	Earlier	Later		Earlier	Later		Earlier	Later		Earlier	Later		Earlier	Later		Earlier	Later
	357	374		822	857		49	49		293	295		405	404		1.9 K	2 K

Health Delta by Resources

☐ Only Show Mismatch

Resources	Total Earlier	Later		Unhealthy Earlier	Later		Total Unhealthy in Earlier Only	Total Unhealthy in Later Only	Total Unhealthy in Both	No issues 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 › ≫

93

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 NDFC

Use this procedure to view the results of the policy delta analysis for the NDFC 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 2 panels, Changed Nodes and *<Switch Name>* Policy Viewer.

5. The **Changed Nodes** panel, displays the changed nodes or switches across the two snapshots.

6. Click **Show Changes** to view the changes in the *<Switch Name>* **Policy Viewer** panel.

7. The *<Switch Name>* **Policy Viewer** panel displays the configuration across the earlier and later

snapshots. The switch configuration for the earlier snapshot is called the earlier snapshot policy. The switch configuration for the later snapshot is called the later snapshot policy.

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

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

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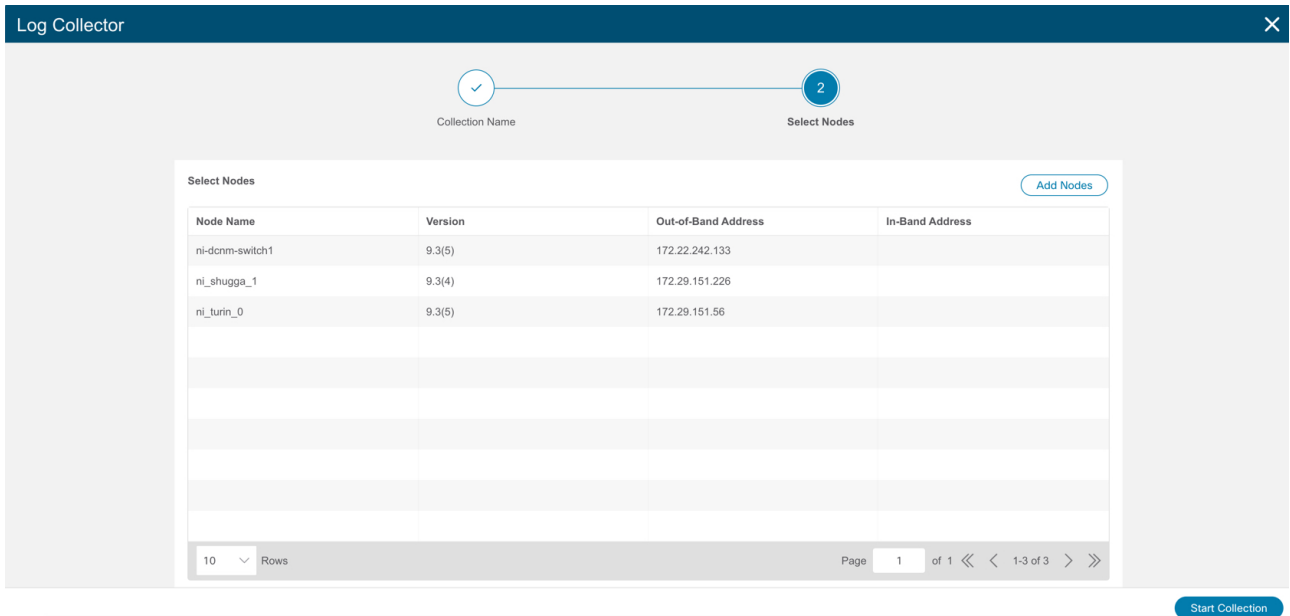
8. Click **Start Collection** to initiate the log collection process.

   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.
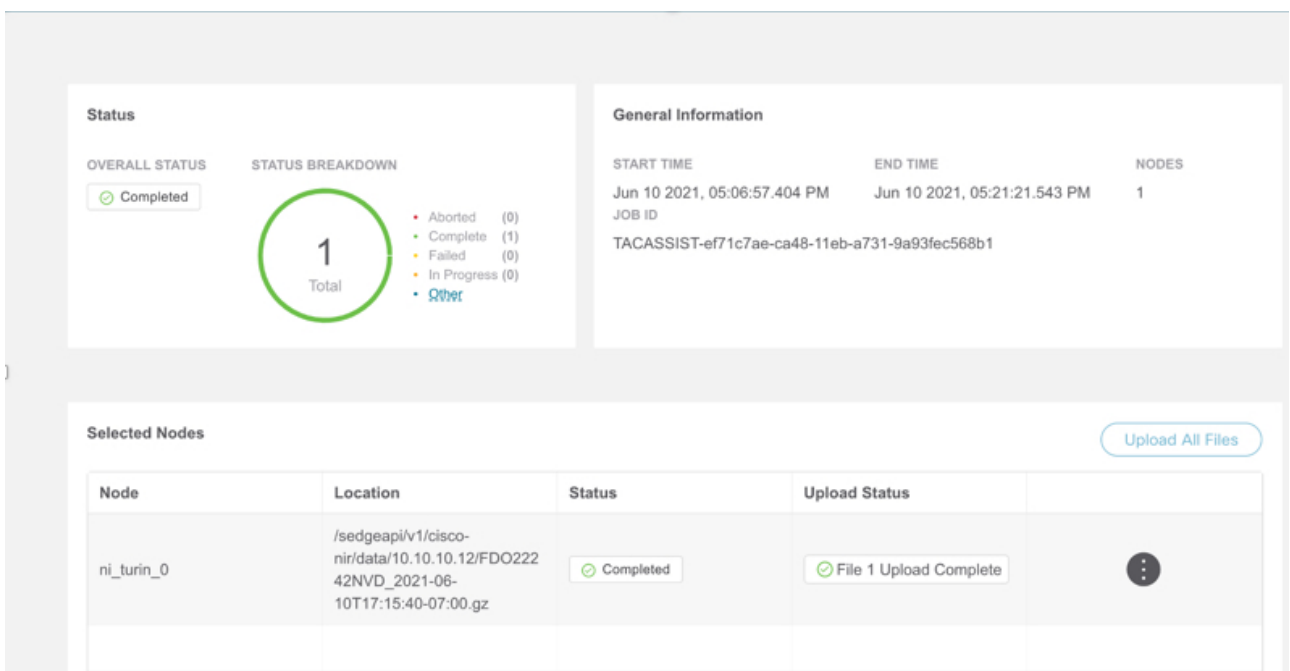
Guidelines and Limitations

- 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.

Connectivity Analysis

Connectivity Analysis feature enables you to run a quick or full analysis for a flow within a fabric or spanning multiple fabrics. It is a micro-service launched through Nexus Dashboard Insights,used for tracing end-to-end forwarding path for a given flow and narrowing down the offending device on its path.

Connectivity Analysis detects and isolates offending nodes in the network for a given flow and includes the following functionalities.

- Traces all possible forwarding paths for a given flow across source to destination endpoints.

- Identifies the offending device with issue, resulting in the flow drop.

- Helps troubleshoot to narrow down the root cause of the issue, including running forwarding path checks, software and hardware states programming consistencies through consistency-checkers, and further details related to packets walkthrough.

The Nexus Dashboard Insights agent is a RPM based application service, which is pre-installed on the Cisco NX-OS. The Nexus Dashboard Insights agent gets the path for a specific flow. The job uses the path returned from the agent and goes to the next hop running the connectivity analysis job.

Schedule a Connectivity Analysis

Use this procedure to schedule a new connectivity analysis job for all the devices compatible with the job.

1. From the Site Group menu, select a Site Group or site.

2. Choose **Troubleshoot** > **Connectivity Analysis**.

3. Click **New Connectivity Analysis**. The **Analyze Connectivity** page appears.

4. Choose **VXLAN** or **Classic LAN** installation mode.

5. Enter the required fields and optional fields to configure the job.

Connectivity Analysis Job	Input Fields
Classic Lan - L3 routed flow	Mandatory: Source IP address, Destination IP address, and VRF name (if non-default). Optional: All the other fields such as Source MAC address, Destination MAC address, and Source VLAN.
VXLAN – L2 VNI switched flow	Mandatory: Source IP address, Destination IP address, Source MAC address, and Destination MAC address. Optional: All the other fields on the UI.
VXLAN – L3 VNI routed flow	Mandatory: Source IP address, Destination IP address, and VRF name. Optional: All the other fields such as Source MAC address, Destination MAC address, and Source VLAN.

6. Toggle between the **Mode** - **Quick** or **Full**. The **Quick** validator traces the network path using L2, L3, and VXLAN CLI for a specific flow to detect and isolate the offending nodes that result in the flow drop.

   The **Full** validator runs consistency checker between software and hardware for programming consistencies. It also traces the network path using L2, L3, and VXLAN CLI for a specific flow.

7. Click **View Nodes** to display the devices compatible with the job and RPM version.

Nodes

N9Kv-106	FDO222336L106	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-109	FDO222336L109	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-3	FDO222336L3	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-4	FDO222336L4	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-5	FDO222336L5	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-6	FDO222336L6	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-7	FDO222336L7	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-8	FDO222336L8	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
scaleleaf-207	FDO222336L207	9.3(5)	1.3.1.1	1.3.1.1	N9K-C93180YC-EX	Simulation	⊘ Compatible	⊘ Installed
N9Kv-102	FDO222336L102	7.0(3)I7(6)	1.3.1.1		N9K-C9336PQ	Simulation	⊗ Not Compatible	⊘ Installed
N9Kv-103	FDO222336L103	9.2(3)	1.3.1.1		N9K-C93128TX2	Simulation	⊗ Not Compatible	⊘ Installed

8. Click **Upgrade** to trigger a latest Nexus Dashboard Insights agent RPM install for all the devices that are compatible with the latest version.

9. Click **Run Analysis**. The connectivity analysis jobs are displayed in the **Connectivity Analysis** Dashboard.

Connectivity Analysis Dashboard

The **Connectivity Analysis** Dashboard displays a graph of Analysis by status for a particular Site Group or site and displays the latest Connectivity Analysis.
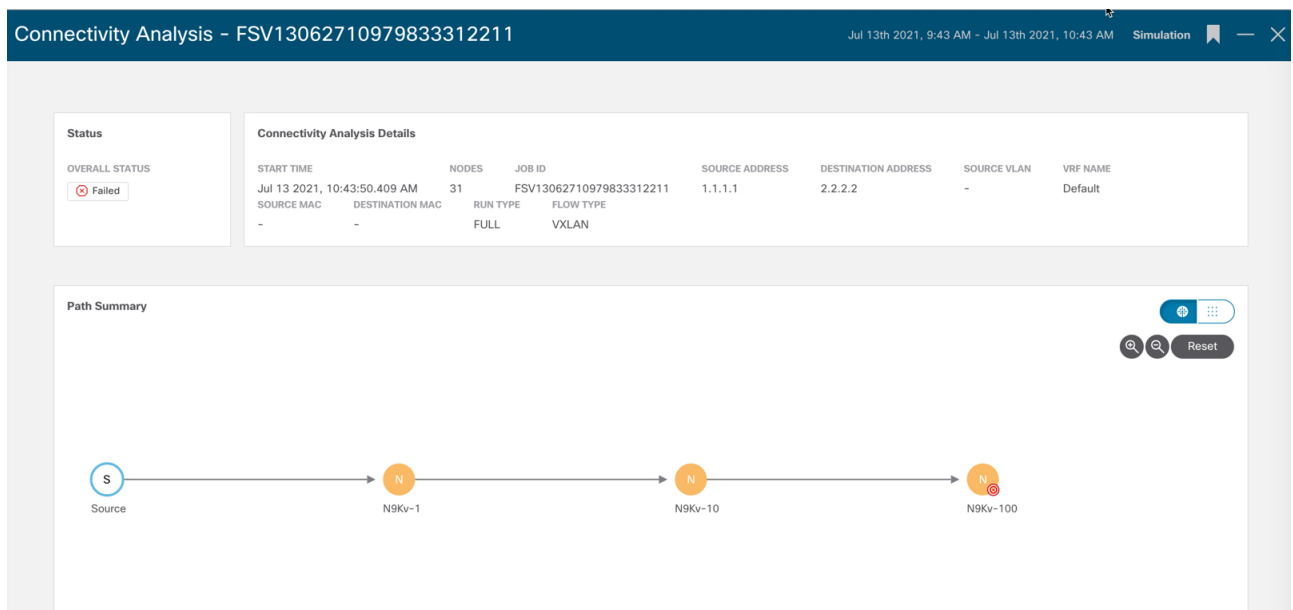
The filter bar allows you to filters the analysis by status, job ID, nodes, source, destination.

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 Connectivity Analysis jobs in a tabular format. The jobs are sorted by status.

1. Select the Connectivity Analysis job in the table for the side pane to display additional details.
2. Click the ⬈ icon to view the **Connectivity Analysis** status page. The **Connectivity Analysis** status page displays information such as status, node details, and path summary .

Oct 14th 2020, 10:32 AM - Oct 14th 2020, 11:32 AM   **tel4**

Status

OVERALL STATUS

⏱ In Progress ⌄

Connectivity Analysis Details

START TIME	NODES	JOB ID	SOURCE ADDRESS	DESTINATION ADDRESS	SOURCE VLAN	VRF NAME
Oct 14 2020, 11:24:09.888 AM	0	FSV10685908447660322009	26.1.0.3	16.1.0.2	-	fwd-fsv-test2:ctx-1

SOURCE MAC	DESTINATION MAC	RUN TYPE	FLOW TYPE
-	-	FULL	FSV_CLASSIC_LAN_L3

Path Summary

Source → swtb21-leaf7 → swtb21-spine3 / swtb21-spine4 → swtb21-spine1 / swtb21-dual-1 / swtb21-spine2 → swtb21-leaf3 → Destination
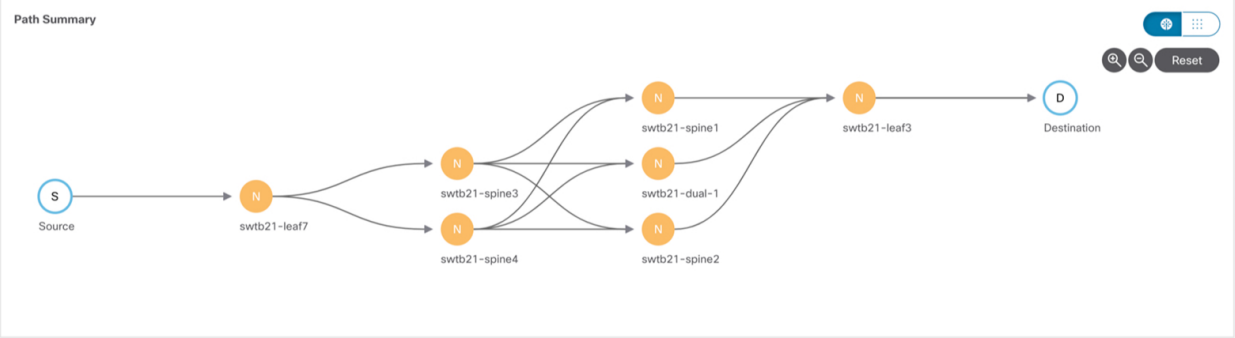
Browse

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 anomalies for the nodes collected across the entire site.

- **Interfaces** —Displays switch nodes interface usage.

- **Protocols** —Displays protocol statistics.

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	The leaf node observations search can be more refined by filtering the information by the top leaf nodes.
Top Nodes by Utilization	Displays the node trend observations by resource type: - Operational Resources - Configuration Resources - Hardware Resources

Guidelines and Limitations

The Hardware Resources tab in Resource Utilization Dashboard is not supported for Cisco Nexus 7000 series switches. The hardware resources do not have a direct mapping to the objects that show in Nexus Dashboard Insights. The command that shows hardware details does not provide the percentage of entries used and the maximum number of entries allocated for a particular feature. Nexus Dashboard Insights raises the anomalies and details page for any resource in Hardware

Resources tab for Cisco Nexus 7000 series switches.

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.

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.

Property	Description
Top Nodes by	Displays the top nodes by: • MAC • IPv4 Host Routes • IPv6 Host Routes • IPv4 Prefix Routes • IPv6 Prefix Routes • Multicast Routes • VLAN • VRF • Port Usage • Ingress Port Bandwidth • Egress Port Bandwidth • CoPP • LPM • HRT • L2 QoS TCAM • L3 QoS TCAM • VLAN • Ingress VLAN ACL • Egress VLAN ACL • Ingress Port ACL • Ingress Routed ACL • Egress Routed ACL

Property	Description
Operational Resources	Displays a list of operational resources based on anomaly score. List information includes: • Anomaly Score • Node • MAC • IPv4 Host Routes • IPv6 Host Routes • IPv4 Prefix Routes • IPv6 Prefix Routes • Multicast Routes

Configuration Resources	Displays a list of configuration resources based on anomaly score. List information includes:
	
	• Anomaly Score
	
	• Node
	
	• VLAN
	
	• VTEP
	
	• VNI
	   ◦ L2
	   ◦ L3
	
	• VRF

Property	Description

Hardware Resources	Displays a list of configuration resources based on anomaly score. List information includes:
	
	• Anomaly Score
	• Node
	• Port Usage
	• Port Bandwidth
	• CoPP
	• LPM
	• HRT
	• QoS TCAM
	   ◦ L2
	   ◦ L3
	• VLAN ACL
	   ◦ Ingress
	   ◦ Egress
	• Port ACL
	   ◦ Ingress
	• Routed ACL
	   ◦ Ingress
	   ◦ Egress

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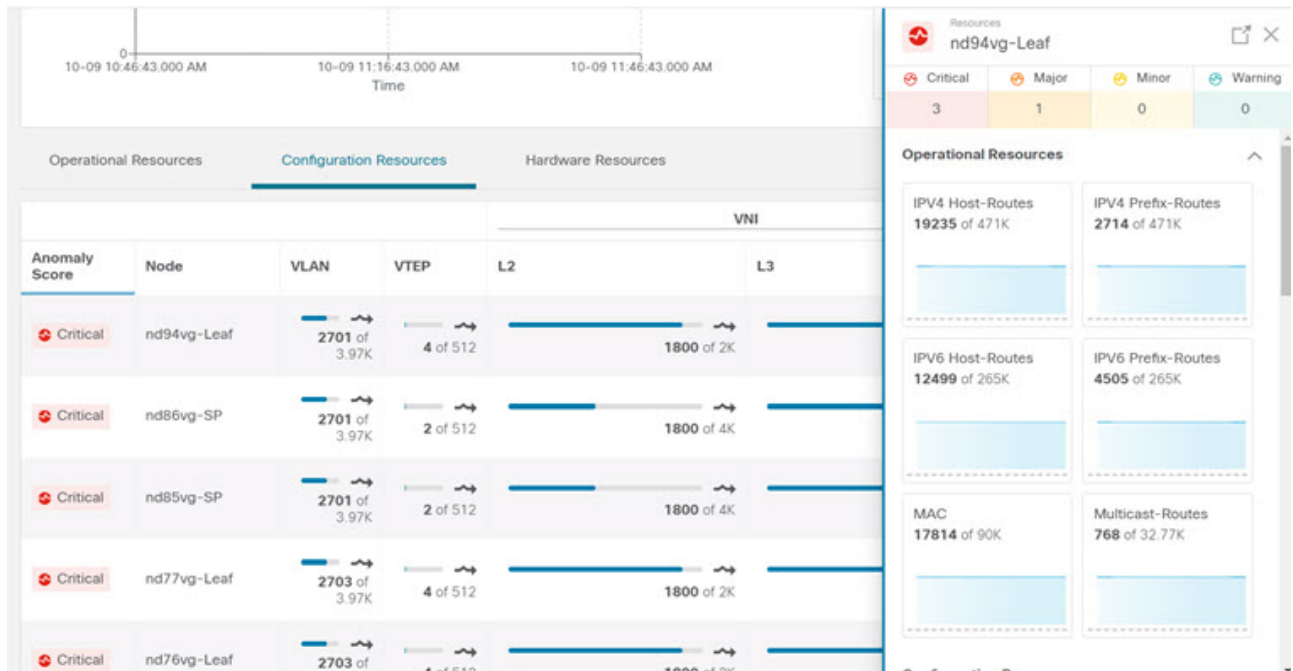
- On the side summary pane, click the ⬀ icon on the right top corner to open the *Resource Details* page.

- 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.
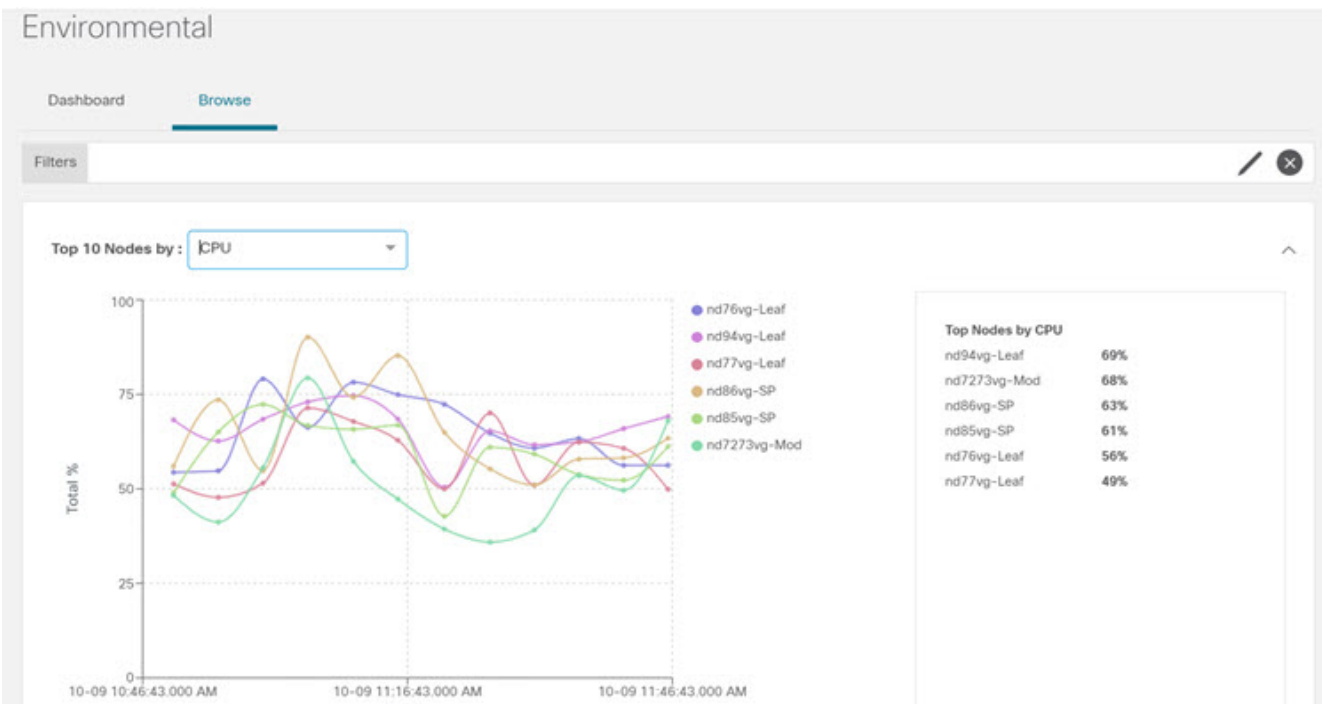
Property	Description
Top Nodes by Utilization	Displays the percentage utilized per component: • CPU • Memory • Temperature • Fan Utilization • Power Supply • Storage
Node Details	Displays the node trend observations by environmental resource type.

Click a node card in the 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.

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.

Property	Description
Top Nodes by	Displays the top nodes by: • CPU (percent utilization) • Memory (percent utilization) • 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.
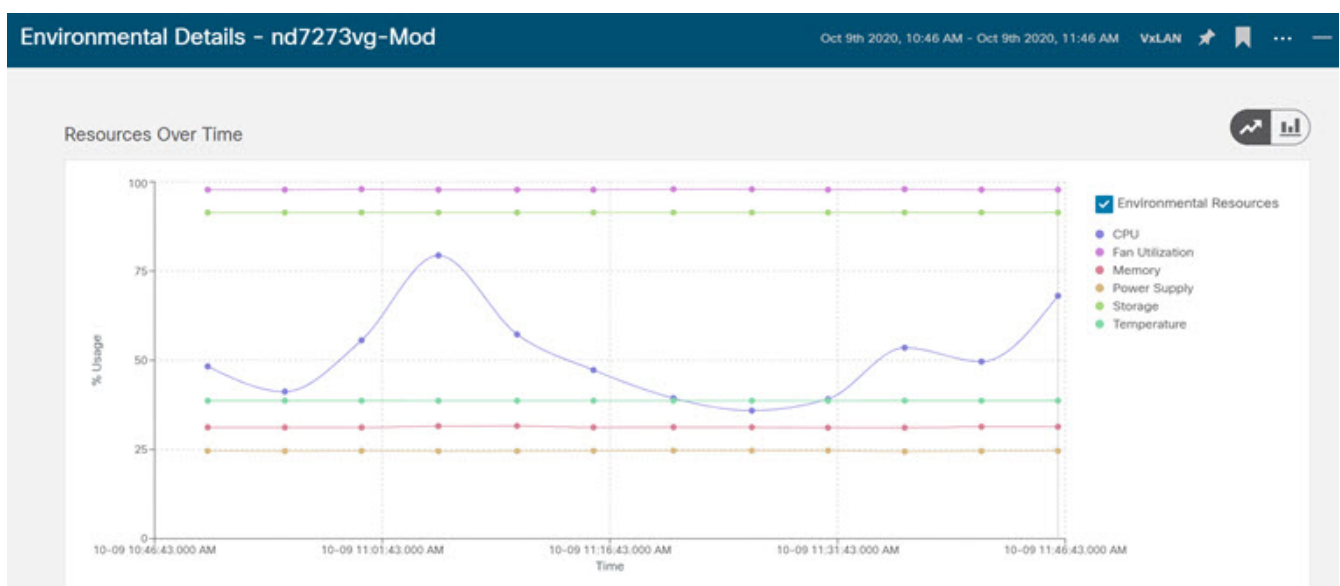
- Click the **Overview** tab.

  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.
- Interface Type - Display only specific interface types.
- Protocol - Display only protocols.
- Operational State - Display nodes with specific operational state.
- Admin State - Display nodes with specific admin 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.

Property	Description
Top 10 Interfaces by	Displays the top interfaces by: • Transmit Utilization • Receive Utilization • Error
Interface Statistics	Displays a list of interface statistics based on anomaly score. List information includes: • Anomaly Score • Interface • Interface Type • Node • Receive Utilization • Transmit Utilization • Errors
Protocol Statistics	Displays a list of protocol statistics based on anomaly score. List information includes: • Anomaly Score • Protocol • Node • Count • Errors

> **i** In order for Nexus Dashboard Insights to receive data from the nodes, confirm that all the nodes in the site are synced with PTP grandmaster for hardware telemetry and NTP clock for software telemetry. You are responsible for configuring the switches with external NTP servers for Cisco NDFC fabrics.

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

> **i** 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 under the **Neighbors** tab. The L4-L7 category is supported.

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.

> ℹ️ When using Nexus Dashboard Insights with NDFC, 1000 SVIs per fabric are supported so only the host-facing SVIs will be present. Anomalies will be raised if the number of SVIs are greater than 1000 per fabric. If this threshold is exceeded, the behavior will be undefined.

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.

> ℹ️ When you start the Nexus Dashboard Insights service for the first time in an existing fabric, you must clear the microburst history by executing the `clear queuing burst-detect` command at the NX-OS exec prompt. As it is a `clear` command, there is no response but the prompt. This ensures a clean microburst state that detects the new microbursts and generates appropriate anomalies.

Configuring and Monitoring Microburst

See 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. In case the flow telemetry is enabled and microburst is enabled, then Nexus Dashboard Insights displays the estimated impact of flows for a particular microburst anomaly.

4. In case 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 Interface Statistics 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.

> ℹ️ 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.

To view the interface's microburst details:

1. In the **Nexus Dashboard** page, navigate to **Browse** > **Interfaces**.

2. In the **Top Nodes by Interface** page, click on the interface for a detailed view.

3. In the **Overview** tab, you can view the microbursts details such as Queue, Start Time, Number of Bursts, Max Duration, Avg. Duration, Max Peak, and Avg Peak in the **Microbursts** section. The following are the two available views:

a. Chart

b. Tabular

Microburst Diagnostic Impact and Recommendation

The microburst egress interface of the node and other details of the node are associated with the flow records in the flow database.

1. Click **Analyze Alerts** > **Anomalies** to browse anomalies.

2. Filter by ResourceType == Interface; Description == Microburst

3. The summary pane lists the anomalies with minor or major microburst severity.

4. Click the anomaly with microburst severity for the side pane to display the affected object.

    a. Click the affected object on the side pane to display the affected entities and anomalies associated with the affected object.

5. Click the anomaly in the summary pane to open the side pane with details.

    a. Click **Analyze** on the side pane to display flow record details.

    b. Click ⬚ on the right corner of the side pane.

    The flow record details page displays **Overview**, **Alerts**, and **Trends** tabs on the page.

    c. Click the **Overview** tab. The path summary section displays the node where the microburst anomaly occurred.

    d. Click the **Alerts** tab to display the anomalies that are associated with microburst.

    e. In the *Mutual Occurrences* section click the circles to see the anomalies that occurred at a particular time.

    The mutual occurrences show the aggregated flows that are microburst affected. They are not individual flows that are affected.

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. 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 summary 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 and more details of the interface.
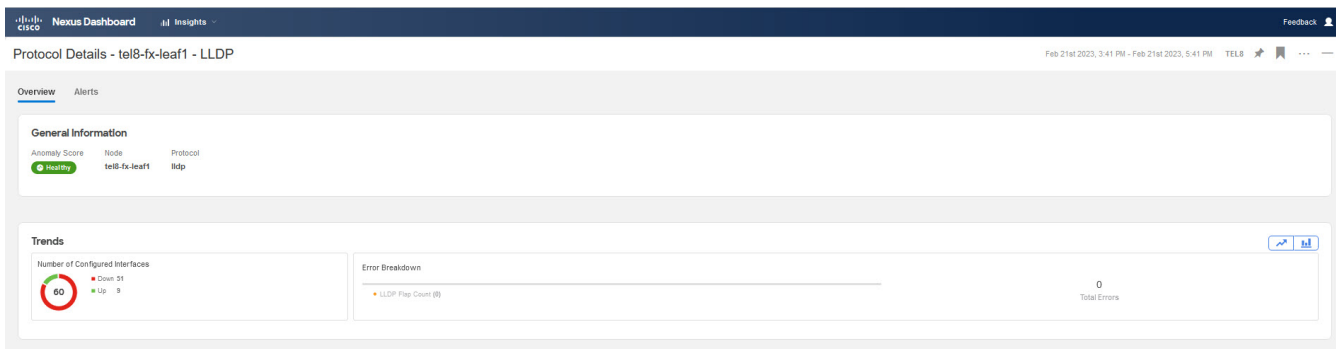
Multicast Protocols

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, node name, protocol, number of domains, number of interfaces, and number of groups 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 where VRF is enabled or disabled, 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.
- Click on rendezvous point address, for example *1*, which displays a side pane with IP address details. This includes the group range the rendezvous point address refers to, lists the group range for a particular rendezvous address.

The **Multicast PIM Interfaces** section displays the summary table with interfaces that are enabled with PIM. It displays the VRF, IP address, designated router address, neighbor addresses, and errors for a specific PIM interface.

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

The **Multicast PIM Groups** section summarizes the PIM group related details such as RPF source, RPF neighbors, VRF, group address, incoming interfaces, and flags that are enabled for the PIM group.

Internet Group Management Protocol

Use filters from browse statistics page to display the summary of a specific node for IGMP interface. The **General Information** section displays the anomaly score, node name, protocol, number of interfaces enabled for a specific node, and number of groups enabled on the interface. On NDFC the IGMP groups can be enabled on VLAN and can also be enabled on the interface.

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

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

The IGMP interfaces can be configured in 3 methods on the specific node. These are not configurable from Nexus Dashboard Insights.

- Enable PIM in the interface.
- Statistically bind the interface to a protocol.
- Enable link reports.
- Double-click a row for the side pane to display additional interface details. This includes groups enable status, statistical data about error counters, flags that are enabled on IGMP, and other properties that are specific to the node.

The **Multicast Groups** section displays the IGMP groups related details such as source, multicast group, VRF, version, last reporter, and outgoing interface specific to the IGMP group. It is possible to have multiple outgoing interfaces.

Internet Group Management Protocol Snoop

Use filters from browse statistics page to display the summary of a specific node for IGMP Snoop. In the VLAN the IGMP is enabled by default, where the IGMP snoops on VLAN for information. 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 per VLAN.

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 information per VLAN. This includes VLAN, admin state, querier address, querier version, multicast routing state (enabled or disabled), node 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 VLAN name, VLAN ID, properties that are enabled or disabled, statistical

details and various error counters specific to the IGMP Snoop instance.

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

Multicast Protocol Statistics Limitations

- The PIM, IGMP, and IGMP Snoop multicast statistics protocols are supported only on Cisco Nexus 9000 series switches.
- The PIM, IGMP, and IGMP Snoop multicast statistics protocols are not supported for the following:
  - Cisco Nexus 7000 and 3000 series switches.
  - Cisco N9K-X9636C-R, N9K-X9636Q-R, N9K-X96136YC-R, and N3K-C3636C-R line cards.
- When Nexus Dashboard Insights programs these devices in Managed mode it avoids enabling the NXAPI export for the unsupported devices. When the fabric is in Monitored mode, the generated configuration avoids the NXAPI commands for the unsupported devices. If you configure these exports manually using direct switch configuration and if the data for these features comes from the unsupported devices, the multicast statistical data may be shown in the Nexus Dashboard Insights GUI.
- The total multicast routes (S, G, and *G together) supported per device is 8000 and per fabric is 64000.

Protocol Statistics Limitations

- The CDP protocol statistics is not supported for Cisco Nexus 7000 series switches.
- Nexus Dashboard Insights does not support BGP `PrefixSaved` statistics on the following:
  - Cisco Nexus 3000, 7000, and 9000 series switches.
  - Cisco N9K-X96136YC-R, N9K-X9636C-R, N9K-X9636Q-R, and N3K-C3636C-R line cards.

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 4. 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**.

Flows

The Flows section of Nexus Dashboard Insights displays the anomalies detected in the flow such as average latency, packet drop indication, and flow move indication collected from various nodes in the site.

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.

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 Hardware Requirements

For details on Flows Telemetry support for Cisco Nexus platform switches, see Nexus Dashboard Insights Release Notes Compatibility Information section.

Flows Guidelines and Limitations

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, and N9K-C93180LC-EX line cards will not be displayed.

- Flows does not support multicast traffic. The access list must be provisioned to exclude the multicast traffic flows.

- A maximum of 63 VRFs are supported on flow telemetry nodes.

- The number of anomalies in the **Site Overview** dashboard will not match the number of anomalies in the flow browse page. The Site Dashboard contains the total anomaly count for the time range you selected. The flow records are not aggregated in the flow browse view, where multiple flow records can point to the same anomaly entry.

- The L3-VNI flows show as L2-VNI flows when the VXLAN flow is dropped in the ingress node. When VXLAN packets are dropped in the first-hop, the exported VXLAN flow telemetry records will indicate the drop. However, they don't carry the VNI information in it. The Ingress interface from the flow telemetry export along with the VRF associated with the interface, does not deduce if the flow is L2-VNI or L3-VNI. In this case Nexus Dashboard Insights associates the L2-VNI for the flow.

- When a VXLAN encapsulated packet enters an Cisco Nexus 9500-EX switch and feature overlay (EVPN) is configured, the packet will be treated like a VXLAN transit node packet. Also the ingress interface and egress interface are set as zeros in the flow telemetry export. The ingress

and egress interfaces are needed to consider this record for flows. The limitation on these switches results in the Cisco Nexus 9500-EX switch not being considered in the path stitching and correlation if the switch is in ingress, transit, or egress direction. Cisco Nexus 9500-EX switches will be treated like a transit node for an overlay packet.

- For Nexus Dashboard Insights to work in VXLAN deployments, you must have symmetric configuration on the switches involved in the overlay. This enables Nexus Dashboard Insights to correlate and stitch the overlay flows. When such a symmetric configuration is not present, the VXLAN feature and forwarding will work, but Nexus Dashboard Insights will not stitch the flows correctly. See the following examples to understand what is meant by symmetric configuration on switches:

  - For Layer 2 VXLAN VNI cases: If vlan-x is mapped VNI-A in PE1, then the same vlan-x must be mapped to VNI-A in PE2, where PE1 and PE2 are VTEP endpoints for the Layer 2 overlay.

  - For Layer 3 VXLAN VNI cases: If SVI-x is mapped to VRF-A mapped VNI-P on PE1, then the same SVI-x must be mapped to VRF-A mapped VNI-P in PE2, where PE1 and PE2 are VTEP end points for the Layer 3 overlay.

- The ingress and VRF information will not be shown for all interfaces which use the flow telemetry 'tenant-id' for encoding the logical interface ID, as this ID will be used for 'overlay-id'. It's not possible to derive the logical interface (SVI with trunk port, sub interface, SVI with trunk and port channel) and get the VRF associated with it. This results in the flow browse page and details page not showing the ingress and egress VRFs.

- On the Cisco Nexus 9500-EX switches connected to VPC pair, the current design limits in identifying the ingress leaf nodes between VPC pairs causing the loss of flow in Nexus Dashboard Insights.

- When there are 29 million anomalies in the indices, flow database writes are too slow, which causes KAFKA lag on 350 nodes supported for software telemetry and flow telemetry. The KAFKA lag results in partial data in Nexus Dashboard Insights user interface.

- Flows information is retained for 7 days or until flow database reaches 80%, which ever happens first, then older flows information is deleted from the database.

- Flow telemetry and flow telemetry events will not export `drop bit` if there is an egress ACL drop in Cisco Nexus FX switches.

- For Nexus Dashboard Insights to receive Flow Telemetry data, the TCAM region for `ing-netflow` must be set to 512. See [Nexus 9000 TCAM Carving](#).

- 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.

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 NDFC 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.
Top Nodes by Flow Anomalies	Flows telemetry and analytics gives in-depth visibility of the data plane. The Flows engine collects the flow records streamed from the nodes and converts to understandable 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 Flow Records

The Browse Flow Records page displays the active nodes, ingress nodes, egress nodes, and flow collection filters, which display the anomalies in the site nodes.

The Browse Flow Records page displays Site flows by Anomaly Score, Packet Drop Indicator, Average Latency, and Flow Move Indicator.

Property	Description
Nodes	Shows all the nodes where the flows are reported.

Property	Description
Filters	Display the node flow observations sorted by the following filters: • Record Time • Nodes • Flow Type • Protocol • Source Address • Source Port • Destination Address • Destination Port • Ingress Node • Ingress Interface • Ingress VRF • Ingress VNI • Egress Node • Egress Interface • Egress VRF • Egress VNI • IP Address • Port
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.

Property	Description
Top Flows	Lists the top flows in the entire site that scored highest in the following: • **Anomaly Score**—The score is based on the number of detected anomalies logged in the database. • **Record Time**—The node flows are captured at individual record times between the start and end time that you selected. Flows records multiple entries for a flow that are captured at individual record times. • **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.

L4-L7 Traffic Path Visibility

Starting with Nexus Dashboard Insights release 6.1.1, you now have expanded visibility in the Flow Path to L4-L7 external devices such as firewalls. Nexus Dashboard Insights tracks the end-to-end flow across the service chain in real-time and helps locate data plane issues across the device silos. In the current release, a non-NAT environment across all third-party vendors is supported.

For L4-L7 traffic path visibility, your flow telemetry must be enabled and the appropriate rules must be configured. See Flow Telemetry for details about configuring. Based on your rules, if the flow is passing through Policy Based Redirects (for example, a firewall), it will display that information in the flow path.

To view traffic path visibility in the GUI, navigate to the **Flows** page, under the **Browse** tab, in the table that follows the graph, in the **Nodes** column, and click the appropriate node. It displays the summary pane. Click the ⬈ Details icon in the top right corner of the summary pane to open the

Flow Details page. Scroll down in this page, to view the **Path Summary** graph.

In the **Path Summary** area, a graphical flow path will display the end-to-end information, from source to destination, and it will also identify the firewall in the path if a firewall is present. The graph also captures the end-to-end flow path network latency that is occurring. See the following example of a **Flow Details** page that displays the **Path Summary** that passes through Policy Based Redirect which is a firewall.
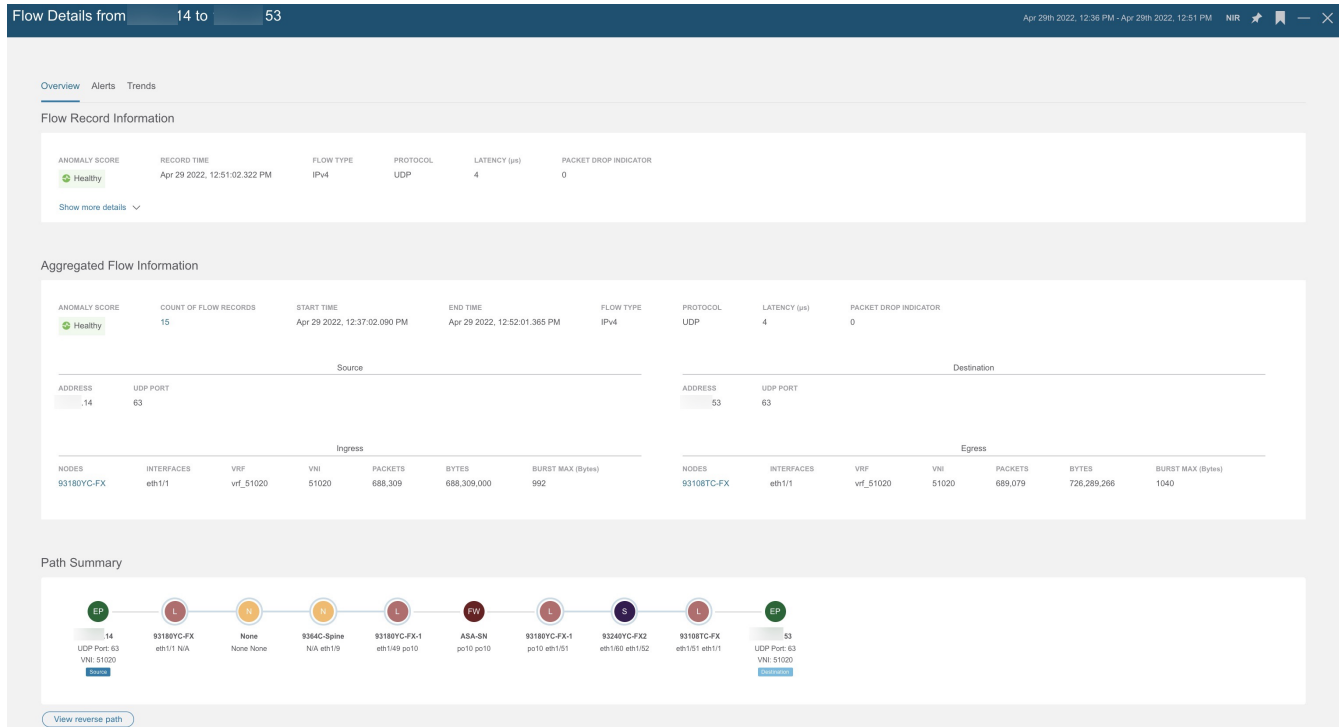
In the graph, if there are any anomalies, a red dot is displayed next to the symbol for the leaf switch or the spine switch. Click the **Alerts** tab in the **Flow Details** page to view further details related to the anomaly.

> In the current release firewalls are not supported for anomalies.

Guidelines and Limitations for L4-L7 Traffic Path Visibility

- This feature is currently recommended only if Policy Based Redirect can be configured using L4-L7 Service for NDFC.

- Service node types will be detected if the service node is directly connected. However, if multiple service nodes are connected on the same physical port, Nexus Dashboard Insights will not identify the exact service node type information. As a result, it will be identified as an unknown service node.

- In the current release, firewalls are not supported for anomalies.

- In the current release, the latency information that is being displayed is the network latency, and it does not capture the latency that is occurring in the firewall.

- In the current release, NAT is not supported.

- This feature is currently supported if you use the following switches:

- Cisco Nexus 9300-FX Platform Switches

- Cisco Nexus 9300-FX2 Platform Switches

- Cisco Nexus 9300-GX Platform Switches.

- Policy Based Redirect destinations on L3Out are not supported because such configurations use an internal VRF because of which only a partial flow path would be available.

- Without a service graph for L4-L7, if the client > service node is VRF_A and the service node > server is VRF_B, the paths will be recorded as separate flows as there is no common or single contract to stitch the flows.

- Load Balancers are not supported.

Flow Telemetry Events

Flow telemetry events are enabled implicitly when flow telemetry is enabled and flow rules are configured. 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 NDFC 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:

- **Cisco ACL Drop**—When packet hits `sup-tcam` rules and the rule is to drop the packet, the dropped packet is counted as ACL_Drop and it will increment the forward drop counter. When this occurred, it usually means the packet is about to be forwarded against basic Cisco ACI forwarding principals. The `sup-tcam` rules are mainly to handle some exceptions or some of control plane traffic and not intended to be checked or monitored by users.

- **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.

TCP packet RTO anomaly is not supported on NDFC.

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

- Flow telemetry event anomalies are aggregated. For example, a packet drop anomaly occurred from time T0 to T1. No packet drop anomaly occurred from time T1 to T2. Another packet drop anomaly occurred from time T2 to T3. Although there is no anomaly from T1 to T2, the time stamp for the aggregated packet drop anomalies is from T0 to T3.

- The flow telemetry events do not report policing drop anomalies in Nexus Dashboard Insights, 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.

Host Overlay Flow Monitoring

The host overlay flow monitoring and flow traffic analysis on NDFC allows the following on the site:

- Monitoring of IPv4 and IPv6 host flows on the overlay from server VTEPs.

- Provides information about the host overlay flow's VNI, fabric-ingress, fabric-egress interfaces.

- Provides information about the host overlay flow's network path inside the fabric, drops experienced by the host overlay flow inside the fabric, packet count, byte count, and burst information of the traffic.

Trunk and sub-interface ingress interfaces will not show site VRF.

Classic fabric type is supported for host overlay flow monitoring. VXLAN fabric type is not supported for host overlay flow monitoring. When a NDFC site is configured as Classic site type, the following flow telemetry are collected:

- The host underlay flow traffic is correlated as classic flows.

- The overlay flows are correlated as host overlay flow traffic.

- The node configuration to collect interface to VLAN mapping is done by the telemetry manager.

Host Overlay Flow Monitoring Guidelines and Limitations

- Classic fabric type is supported.

- VXLAN fabric type is not supported.

- Cisco Nexus 9000 -FX, -FX2, and -GX platform switches are supported.

Configuring Host Overlay Flow Monitoring

1. In the Overview page, at the top, choose your Site Group.

2. Click the ellipses icon next to it and choose Configure Site Group.

3. Click Flows. See Configure Flow Telemetry.

Browse Host Overlay Flow Monitoring

1. Click **Browse** > **Flows**.

2. Filter by Nodes.

3. Double-click an anomaly in the summary pane.

4. The *Flow Record Details* page opens with **Overview**, **Alerts**, **Trends** tabs.

The *Flow Record Information* section displays the flow type, protocol, and anomaly score. The *Aggregated Flow* section describes the source and destination IP address, VLAN information. The *Path Summary* section displays the source, destination, node/interface details, packet exceptions such as forwarding drop, buffer drop for the outer data packet for the site.

5. Click an anomaly in the summary pane to display the side pane with general information, source, ingress, and flow type.

   For host overlay flows, the *Logical Encap* column in the browse table shows the flow's VNI information.

Endpoints

The Endpoints section of Nexus Dashboard Insights contains endpoint information, charts, and history for the nodes with endpoint anomalies collected across the entire NDFC site.

Endpoints provides detailed analytics of endpoints learned 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 the discover configuration and operational information of the endpoint.

The following anomalies are detected for Endpoints:

- Rapid endpoint moves across nodes, interface, and endpoint groups

- Endpoints that have duplicate IP address

- Missing endpoints that fail to get learnt after a node reboot

- 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. 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** > **Endpointd**.

4. 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 anomaly in the table to display the *Endpoint Details* page.

- Or, click an endpoint in the summary table for the sidebar to display configuration, operational, endpoint status, and additional details about the anomaly.

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

The following anomalies are detected as part of endpoint analytics:

- Rapid endpoint moves across nodes, interface, and endpoint groups

- Endpoints that have duplicate IP addresses

- Spurious endpoints

Endpoints Filters

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

You can view, sort, and filter endpoints through the work pane. Use the **Filter** field to refine the endpoints by choosing from the following filters:

- VRF - Displays nodes with IP address.

- BD - Displays nodes with domain id.

- 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.

- Encap - Displays nodes with specific encapsulation.

- 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

The *Overview* tab displays general information about the endpoint. The *Endpoint Details* page describes general information about the endpoint based on configuration and operation of the endpoint. The configuration section displays the IP address or hostname, MAC address, BD, VRF, and Encap details for the selected endpoint. The operational section displays the Node name, Interface, VM id, hypervisor id, and other details.

This page also lists the *Endpoint History*, *IP History*, and *Duplicates*.

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. Hovering over the highlighted value shows the change for that value. Hovering over Changes column shows all changes.

The L2 endpoints have VLAN information while L3 endpoints have VRF information.

The *IP History* lists the history based on a given IP address.

The *Duplicates* section lists duplicate IP addresses attached to the endpoint. Duplicate IP address occurs 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 occurred 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.

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.

You can configure the Flow Telemetry rule for the following interface types:

- VRFs
- Physical Interfaces
- Port Channel Interfaces

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 NDFC. See Cisco Nexus Dashboard Insights Deployment Guide for more information. You are responsible for configuring the switches with external NTP servers for Cisco NDFC fabrics.

- 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 NDFC, and the flows are aggregated under the same umbrella.

- In the **Edit Flow** page, it is possible to enable all three, you choose the best possible mode for a product. sFlow is most restrictive, Netflow has some more capability, and Flow Telemetry has the most capability. So the recommendation is to enable Flow Telemetry if it is available for your configuration. If Flow Telemetry is not available, then use Netflow. If Netflow is not available, use sFlow.

- 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, Netflow, and sFlow by the user if required for your configuration.

- Flow telemetry including Flow Telemetry Events supports the following:

  - 20,000 unique flows/s [physical standard]
  - 10,000 unique flows/s [physical small]
  - 2,500 unique flows/s [vND]

- If there are multiple NDFC clusters onboarded to Cisco Nexus Dashboard Insights, partial paths will be generated for each site.

- If you manually configure the fabric to use with Cisco Nexus Dashboard Insights and Flow Telemetry support, the Flows Exporter port changes from 30000 to 5640. To prevent a breakage of the Flows Exporter, adjust the automation.

- Nexus Dashboard supports Kafka export for Flow anomalies. However, Kafka export is not currently supported for Flow Event anomalies.

- Flow telemetry is supported in -FX3 platform switches for the following NX-OS versions:
  - 9.3(7) and later
  - 10.1(2) and later
  - Flow telemetry is not supported in -FX3 platform switches for NX-OS version 10.1(1).

- Interface based Flow telemetry is only supported on modular chassis with -FX line cards on physical ports and port channels rules.

Flow Telemetry Rules guidelines and limitations:

- If you configure an interface rule (physical/port channel)on a subnet, it can monitor only incoming traffic. It can't monitor outgoing traffic on the configured interface rule.

- If a configured port channel that contains two physical ports, only the port channel rule is applicable. Even if you configure physical interface rules on the port, only port channel rule takes precedence.

- You can configure up to 500 rules on a node.

- For NX-OS release 10.3(2) and earlier, if a flow rule are configured on an interface, then global flow rules are not matched.

- For NX-OS release 10.3(3) and later, a flow rule configured on an interface is matched first and then the global flow rules are matched.

Configure Flow Telemetry

Configure Flow Collection Modes

Before you begin

As a user, you must configure the appropriate switches by using the recommended configuration. For more details, see Nexus Dashboard Insights Switch Configuration Status.

Procedure

1. In the **Overview** page, at the top, choose your Site Group.

2. Click the ellipse icon 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 ellipse icon. (The **General** tab table

displays the site name and whether the flow collection is enabled or disabled.)

5. Click **Edit Flow Collection Modes**.

6. In the **Edit Flow Collection Mode** page, select **Flow Telemetry** to enable Flow Telemetry. All the flows are disabled by default.

7. Click **Save**.

Configure Flow Collection Rules

Procedure

1. In the **Overview** page, at the top, choose your Site Group.

2. Click the ellipse icon 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 ellipse icon. (The **General** tab table displays the site name and whether the flow collection is enabled or disabled.)

5. Click **Edit Flow Rules**.

6. To add a VRF rule, click VRF tab and perform the following:

    a. From the **Actions** drop-down menu, select **Create New Rule**.

    b. In the **General** area, complete the following:

        i. Enter the name of the rule in the **Rule Name** field.

        ii. The VRF filed is disabled. The flow rule applies to all the VRFs.

        iii. In the **Flow Properties** area, select the protocol for which you intend to monitor the flow traffic.

        iv. Enter the source and destination IP addresses. Enter the source and destination port.

        v. Click **Save**.

7. To add a physical interfaces rule, click **Physical Interfaces** tab and perform the following:

    a. From the **Actions** drop-down menu select **Create New Rule**.

    b. In the **General** area, complete the following:

        i. Enter the name of the rule in the **Rule Name** field.

        ii. Check the **Enabled** check box to enable the status. If you enable the status, the rule will take effect. Otherwise, the rule will be removed from the switches.

        iii. In the **Flow Properties** area, select the protocol for which you intend to monitor the flow traffic.

        iv. Enter the source and destination IP addresses. Enter the source and destination port.

        v. In the **Interface List** area, click **Select a Node**. Use the search box to select a node.

        vi. From the drop-down list, select an interface. You can add more than one row (node+interface combination) by clicking **Add Interfaces**. However, within the rule, a node can appear only once. Configuration is rejected if more than one node is added.

      vii. Click **Save**.

8. To add a port channel rule, click **Port Channel** tab and perform the following:

    a. From the **Actions** drop-down menu, select **Create New Rule**.

    b. In the **General** area, enter the name of the rule in the **Rule Name** field.

       i. Select the **Enabled** check box to enable the status. If you enable the status, the rule will take effect. Otherwise, the rule will be removed from the switches.

      ii. In the **Flow Properties** area, select the protocol for which you intend to monitor the flow traffic.

     iii. Enter the source and destination IP addresses. Enter the source and destination port.

     iv. From the drop-down list, select an interface. You can add more than one row (node+interface combination) by clicking **Add Interfaces**. However, within the rule, a node can appear only once. Configuration is rejected if more than one node is added.

      v. Click **Save**.

9. Click **Done**

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** > **Flows**, 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 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 5. Supported Interfaces for Netflow

Interfaces	5 Tuple	Nodes	Ingress	Egress	Path	Comments
Routed Interface/Port Channel NOTE: Port Channel support is available if the user monitors only the host-facing interfaces.	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

For Nexus 9000 Series switches with NDFC type, Full Netflow is supported. For Nexus 7000 and Nexus 7700 Series switches, F/M line cards with NDFC type, Sampled Netflow is supported.

Full Netflow

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.

Sampled Netflow

With Sampled Netflow, packets on configured interfaces are time sampled. Flows are sent to the supervisor or a network processor for aggregation. Aggregated flow records are exported at configured intervals. The probability of a record for a flow being captured depends on the sampling frequency and packet rate of the flow relative to other flows on the same interface.

Netflow Guidelines and Limitations

- In the **Edit Flow** page, it is possible to enable all three, you choose the best possible mode for a product. sFlow is most restrictive, Netflow has some more capability, and Flow Telemetry has the most capability. So the recommendation is to enable Flow Telemetry if it is available for your configuration. If Flow Telemetry is not available, then use Netflow. If Netflow is not available, use sFlow.

- 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.

- In Nexus 7000 and Nexus 9000 Series switches, only the ingress host-facing interface configured for Netflow are supported (either in VXLAN or Classic LAN).

- 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.

- For NDFC type, the Netflow supported fabrics are Classic and VxLAN. VXLAN is not supported on fabric ports.

- Netflow configurations will not be pushed. However, if a site is managed, the software sensors will be pushed.

- If you manually configure the fabric to use with Cisco Nexus Dashboard Insights and Netflow support, the Flows Exporter port changes from 30000 to 5640. To prevent a breakage of the Flows Exporter, adjust the automation.

- To configure Netflow on fabric switches, see the **Configuring Netflow** section in the [Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#).

Configure Netflow

Before you begin

As a user, you must configure the appropriate switches by using the recommended configuration.

For more details, see Nexus Dashboard Insights Switch Configuration Status.

Procedure

Configure Netflow as follows.

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, 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.

6. Click **Save**.

This enables the Netflow process to begin.

sFlow

sFlow is an industry standard technology traffic in data networks containing switches and routers. Cisco Nexus Dashboard Insights supports sFlow version 5 on Cisco Nexus 3000 series switches.

sFlow provides the visibility to enable performance optimization, an accounting and billing for usage, and defense against security threats.

The following interfaces are supported for sFlow:

Table 6. Supported Interfaces for sFlow

Interfaces	5 Tuple	Nodes	Ingress	Egress	Path	Comments
Routed Interface	Yes	Yes	Yes	Yes	Yes	Ingress node is shown in path

sFlow Guidelines and Limitations

- Cisco Nexus Dashboard Insights supports sFlow with Cisco Nexus 3000 series switches using NDFC.

- It is recommended that enable Flow Telemetry if it is available for your configuration. If that is not available for your configuration, use Netflow. If Netflow, is not available for your configuration, then use sFlow.

- For sFlow, Cisco Nexus Dashboard requires the configuration of persistent IPs under cluster configuration, and 6 IPs in the same subnet as the data network are required.

- sFlow configurations will not be pushed. However, if a site is managed, the software sensors will be pushed.

- If you manually configure the fabric to use with Cisco Nexus Dashboard Insights and sFlow support, the Flows Exporter port changes from 30000 to 5640. To prevent a breakage of the Flows Exporter, adjust the automation.

- Cisco Nexus Dashboard Insights does not support sFlow in the following Cisco Nexus 3000 Series switches:

    ◦ Cisco Nexus 3600-R Platform Switch (N3K-C3636C-R)

    ◦ Cisco Nexus 3600-R Platform Switch (N3K-C36180YC-R)

    ◦ Cisco Nexus 3100 Platform Switch (N3K-C3132C-Z)

- Cisco Nexus Dashboard Insights does not support sFlow in the following Cisco Nexus 9000 Series fabric modules:

    ◦ Cisco Nexus 9508-R fabric module (N9K-C9508-FM-R)

    ◦ Cisco Nexus 9504-R fabric module (N9K-C9504-FM-R)

- To configure sFlow on fabric switches, see the **Configuring sFlow** section in the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.

Configure sFlow

Before you begin

As a user, you must configure the appropriate switches by using the recommended configuration. For more details, see Nexus Dashboard Insights Switch Configuration Status.

Procedure

Configure sFlow Telemetry as follows.

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, 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 **sFlow** button. All the flows are disabled by default.

6. Click **Save**.

This enables the sFlow process to begin.

SR-MPLS Flows - Beta Feature

SR-MPLS Flows in NX-OS Fabrics

> **ℹ** This is a **Beta** feature. We recommend that you use features marked as **Beta** in your test environments but not in production deployments

Starting with release 6.1.1, Nexus Dashboard Insights will support SR-MPLS flows in the following areas:

- Flow analytics for SR-MPLS flows in NX-OS fabrics

- Flow information with associated **Transport** and **VPN** labels

- The ability to search flows with **VPN** labels

SR-MPLS will provide support in Nexus Dashboard Insights these areas:

- Flow analytics for flows encapsulated with SR-MPLS labels

- Provide the flow path for the inner flow with associated labels for the flows

- Provide SR-MPLS flow path changes with associated labels for changed paths

- Provide hop-by-hop transport label and the label operations will be performed on the flow

- Provide end-to-end VPN labels that are used by the flow

- Provide end-to-end latency experienced by the SR-MPLS flow

- Provide max-burst, packet, and byte counters for the SR-MPLS flow

- Provide drop indications like forward, buffer, ACL, and QoS drops for the SR-MPLS flows

- Provide the ability to search the flows matching a particular transport or VPN label (if the flow is tracked using Flow Telemetry analytics)

Supported Platforms are as follows:

- SR-MPLS flow analytics are supported only for NX-OS fabrics.
- NX-OS supported platforms are ToR and EoR:
    - Nexus 9300-GX Platform Switches
    - Nexus 9300-FX Platform Switches
    - Nexus 9300-FX2 Platform Switches
- NX-OS supported release 10.2.3F
- Nexus Dashboard release 2.2
- DCNM release 11.5.3 and NDFC release 12.0.2

Supported Topologies

The following topologies are supported:

- Leaf-Spine-Leaf

- Leaf-Spine-SuperSpine-Spine-Leaf

- Border Spine (Border SuperSpine cases are not supported)

> **ℹ** Only end-to-end latency is supported.

Workflow for SR-MPLS Flows for NX-OS

To setup and monitor flows for SR-MPLS flows in NX-OS fabrics, follow this workflow sequence.

1. **Configure the Site Group with SR-MPLS Fabric Type**: When adding a new Site Group, one of the steps requires you to choose the **Fabric Type** in the **Configure** dialog box, in the **General Configuration** area. From the **Fabric Type** field drop-down list, you must choose **SR-MPLS** and complete the remaining steps. Further details about adding a Site Group are available in Cisco Nexus Dashboard Insights Configuring the Basics for Day 0 Setup or in Add a Site Group, as applicable to your setup.

2. **Configure the Flows**: Configure the flows as desired for your SR-MPLS fabric type Site Group/s. See Configure Flows for more details.

3. **View SR-MPLS Flows**: In the Navigation pane of the GUI, click **Browse** > **Flows** to view the desired flows. More details in View SR-MPLS Flows.

View SR-MPLS Flows

In the Navigation pane of the GUI, for your Site Group, click **Browse** > **Flows**. In the **Flows** page, click the **Browse** tab. In the **Flows Individual Records** table, in addition to the other columns, you can view the **VPN** and **Transport** columns and their label values in the **Ingress** and **Egress** areas of the table. The label values for **VPN** and **Transport** are numerical. For VPN, there is a single value and for Transport there could be a list of values.

In the **Browse** tab, you can search for a specific label in the **Filter** field, and the related flows are displayed in the Anomalies table. Click in the appropriate row in the Anomalies table to open the summary pane. Click the ⬈ Details icon in the summary pane to open the **Flow Details** page.

In the **Flow Details** page, the **Flow Record Information**, **Aggregated Flow Information** and **Flow Path Summary** areas are displayed. In the **Flow Details** page, in the **Aggregated Flow Information** area, you can view the **VPN Label** values in the Ingress and the Egress area.

In the **Flow Path Summary** area, when you hover on each segment in the path, you can view the **VPN** label and its value. The **Transport** label is present at every hop. Every interface on a node will have the **view** link. When you hover over the **view** link below a hop, the Transport details will display.

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 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**.

   > ℹ️ 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.

    b. Click **Next**

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 NDFC.

    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 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 NDFC

Pre-Validation Criteria	Descriptioon	Release
Could not connect to devices	This validation checks if all devices are connected.	6.0.1

Pre-Validation Criteria	Descriptioon	Release
Check if modules are in ok/active/standby state	This validation checks if all modules are online.	6.0.1
Found exception log messages in module	This validation checks for non-user initiated resets.	6.0.1
Found core files on devices	This validation checks for core files.	6.0.1
Found active supervisor without HA standby	This validation checks the redundancy status on dual supervisor systems.	6.0.1
One or more port-channel members are not up	This validation checks if all port-channel members are in Up state.	6.0.1
Found non user-initiated system resets	This validation checks if system reset is due to reasons other than user-initiated.	6.0.1
Found non user-initiated module resets	This validation checks if module reset is due to reasons other than user-initiated.	6.0.1
Found modules not in ok state and without backup power	This validation checks if all modules are in ok state and if backup power present.	6.0.1
Found FAILURE/ABORT/INCOMPLETE/ ErrorDisabled in module	This validation checks for FAILURE/ABORT/INCOMPLETE/ ErrorDisabled results in any module.	6.0.1
Found vPC status is not in Up state	This validation checks if vPC status is in Up state.	6.0.1
Found vPC sticky bit is false	This validation checks if vPC sticky bit is false.	6.0.1
Found vPC role is not secondary	This validation checks if vPC role is secondary.	6.0.1
Found OSPF is in FULL FULL/DR state	This validation checks for OSPF interfaces and process uptime stability (12 hours).	6.0.1
Found BGP session are not in Up state	This validation checks for BGP neighbors up time stability (12 hours).	6.0.1
Found HSRP MGO state is not Active/Standby	This validation checks if HSRP MGO state is Active/Standby.	6.0.1

Pre-Validation Criteria	Descriptioon	Release
Found ARPs are in Incomplete state	This validation checks if ARPs are in Incomplete state.	6.0.1
Not enough free space to continue	This validation checks if bootflash free space is greater than threshold of 5GB.	6.0.1
Found filesystems with usage higher than 85%	This validation checks if all filesystems usage is equal to or below 85%.	6.0.1
Found console register bits are not RTS or DTR orDSR	This validation checks if console register bits are RTS or DTR or DSR.	6.0.1
Found Severity 1, 2 or 3 messages	This validation checks for Severity 1, 2 or 3 messages.	6.0.1
ISSU impact check was disruptive	This validation checks if ISSU is disruptive or non-disruptive.	6.0.1
All spines are selected in same upgrade group or no redundant spine available for some nodes	This validation checks if spine nodes are upgraded with at least two separate groups to avoid traffic loss.	6.0.2
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.
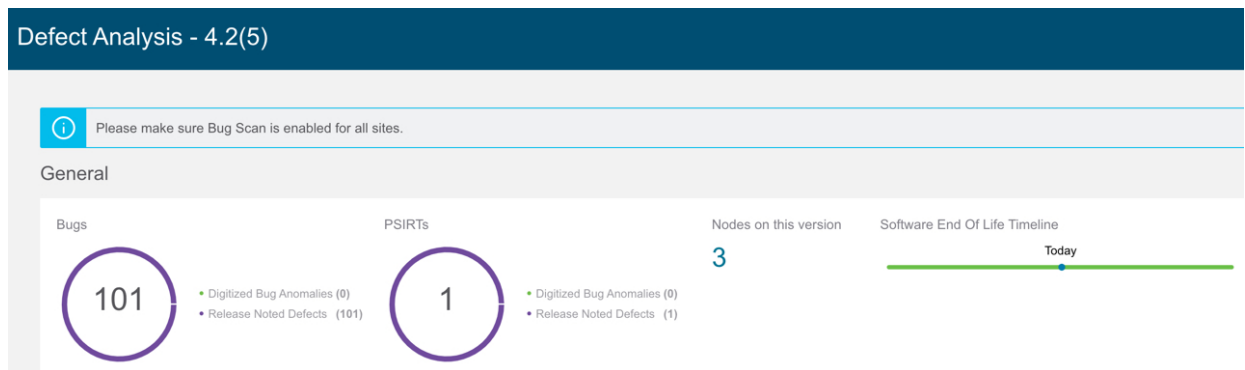
Digitized Bug Anomalies are digitized bugs that are also found as system anomalies in the Bug Scan feature. Release Noted Defects are bugs mentioned as Known Issues in the release notes for a specific firmware version. The software EOL timeline displays the EOL timeline for the firmware version and is 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**

DNS Integration

About DNS Integration

The 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). Nexus Dashboard Insights verifies the integrity of the file. When required, you can also download or delete the file from the GUI.

If no VRF or Site name 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.

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.

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. 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, 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 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.

> ℹ️ 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 a 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 information. If you have a file that contains the site name, specifying the VRF is optional.

Format .json

```
[
  {
        "recordType": "dnsEntry",
        "fqdn": "host1.cisco.com",
        "ips": ["1.1.0.0"],
        "vrf": "vrf-1",
        "siteName": "swmp3",
  },
  {
        "recordType": "dnsEntry",
        "fqdn": "host2.cisco.com",
        "ips": ["1.1.0.1"],
        "vrf": "vrf-1",
        "siteName": "swmp3",
  }
  {
         "recordType": "dnsEntry",
         "fqdn": "host3.cisco.com",
         "ips": ["1.1.0.2"],
  },
]
```

Format .csv

```
recordType,fqdn,ips,siteName,vrf
dnsEntry,swmp3-leaf1.cisco.com,"101.22.33.44",swmp3,vrf-1
dnsEntry,swmp5-leaf1.cisco.com,"10.2.3.4,10.4.5.6,1.2.3.4",fabric2,vrf-2
dnsEntry,swmp4-leaf1.cisco.com, "1.1.1.1",,,
```

Configure DNS Server Onboarding for Query

Follow this procedure to configure the DNS Server Onboarding using the 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.

AppDynamics Integration

About AppDynamics Integration

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

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

AppDynamics 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 site nodes.

In a scenario where an application communicates through the 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 site nodes.

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 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.

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.

> ℹ️ 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.

> ℹ️ You can obtain this information from your AppDynamics setup by navigating to Settings (Gear icon) > License > Account.
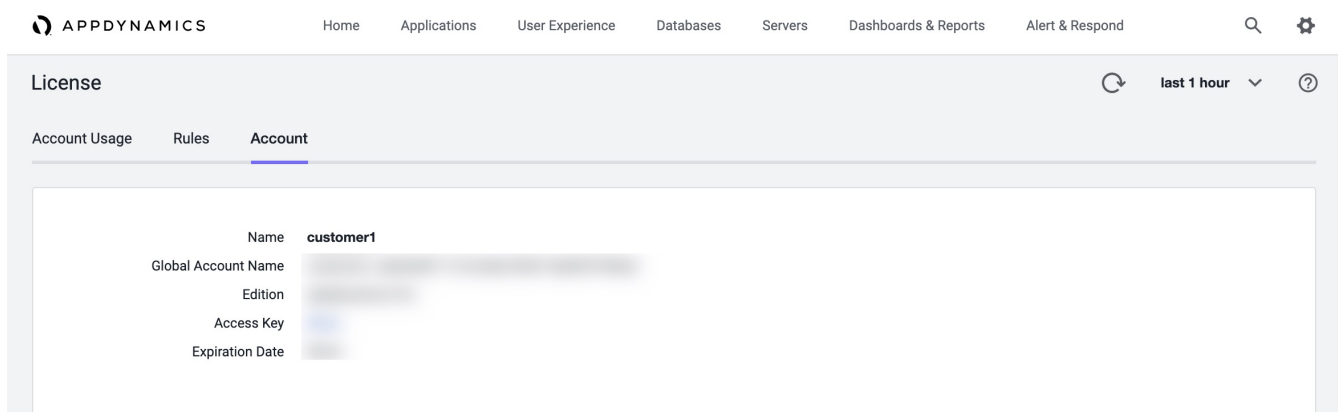
4. Click **Add Association** to associate a Site Group or site.

   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.

Cisco 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—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** for 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.
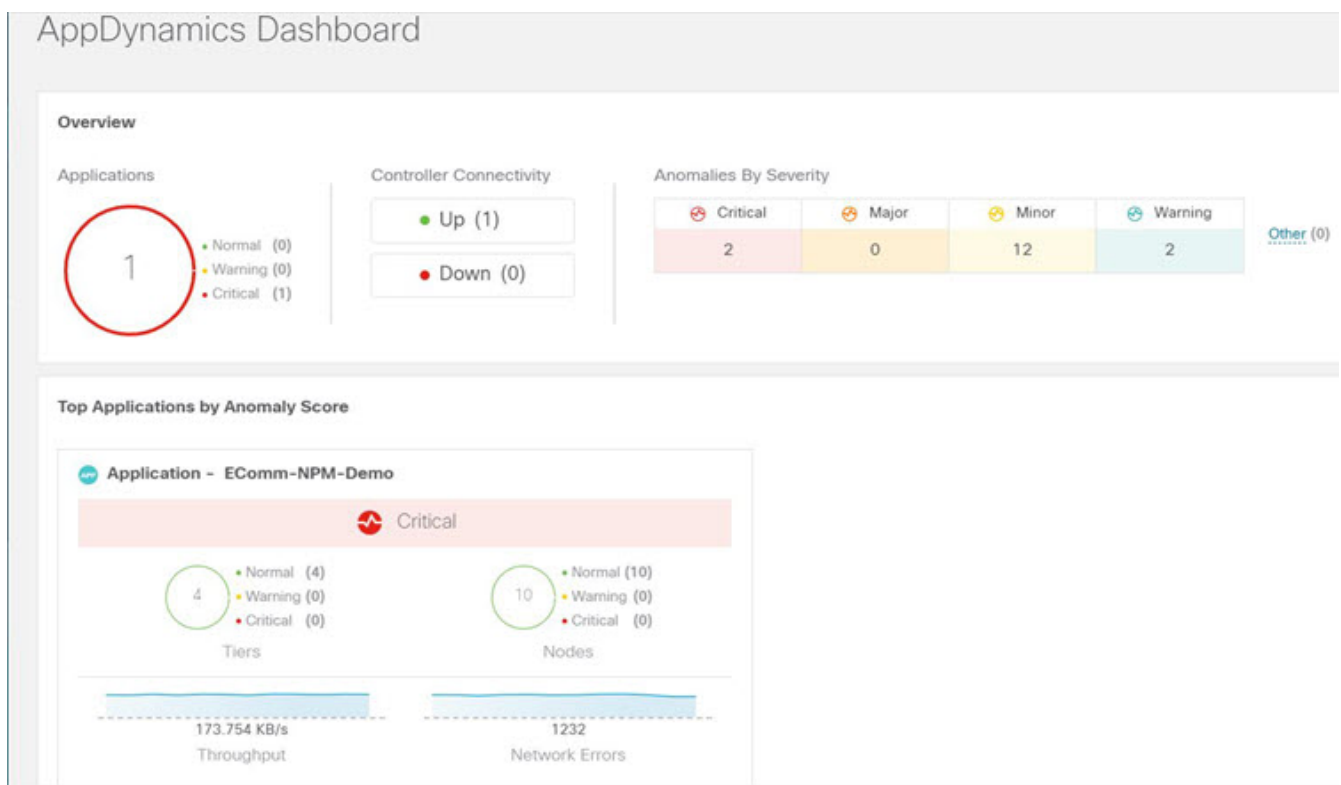
Click the widget for additional details about the monitored application.

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 Flow Records with the flow properties set in the filter.

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

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**.

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.

- Scale limits for AppDynamics integration:

  - Number of apps: 5

  - Number of tiers: 50

  - Number of nodes: 250

  - Number of net links: 300

  - Number of flow group: 1000

Topology View

The topology view represents the stitching between nodes where these nodes are connected to the 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** > **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 leaf nodes 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 displays the top 100 fabric flows ordered by the anomaly score for AppDynamics anomalies.

vCenter Integration

About VMware vCenter Server Integration

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 NDFC fabric.

Data collected from vCenter includes

- Virtual machine data
- Network data
- Virtual machine NIC data
- Host data
- Datastore data
- Standard switch information
- DVS information
- vCenter Alarms

Nexus Dashboard Insights collects data from vCenter every 15 minutes. A system anomaly is raised if Nexus Dashboard Insights is unable to reach vCenter.

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**.

- Host, VM, and Datastore alarms from vCenter
- Baseline anomalies for checks such as CPU, memory, storage
- Threshold anomalies

See Analyze Anomalies.

Prerequisites

- You have installed VMware vCenter 6.5 and later.
- You have read-only privileges for VMware vCenter.

Guidelines and Limitations

- No of VMs supported for VMware vCenter integration is 1000.
- No of vNIC hosts supported for VMware vCenter integration is 10,000.

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. 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.

vCenter Server Dashboard

The vCenter Dashboard presents a view of the of the **Top Virtual Machines by Anomaly Score** or **Hosts 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.

- From the navigation pane choose **Browse** > **vCenters** to access the vCenter dashboard.

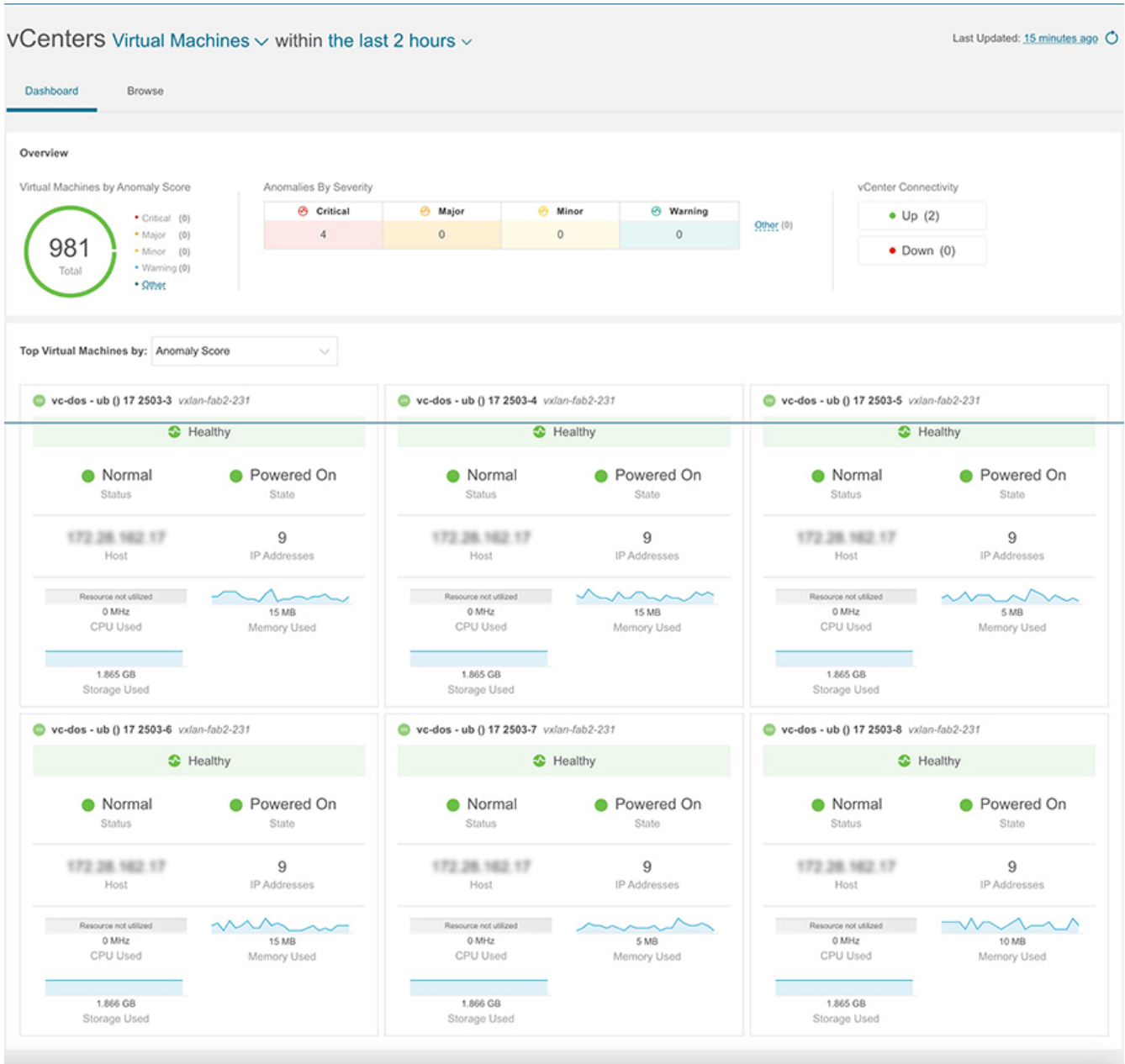- From the drop-down list, select **Virtual Machines** or **Hosts**.

vCenter Virtual Machine Dashboard

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 plotted on a timeline. From the drop-down list, select CPU, memory, storage, 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 IP, vCenter Controller, VM, host, state, status, guest OS, DNS name, datacenter, network adapter, network usage, CPU, memory, and storage.

   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 in a tabular format.

   The **Virtual Machines** table displays information such as Anomaly score, vCenter IP address, virtual machine IP address, state, number of network adapters, IP address, network usage, CPU , memory, and storage.

   > ℹ️ The information displayed for CPU, memory, and storage match the information displayed in the VMware vCenter VM Summary page.

   a. Click the **Settings** menu to customize the columns to be displayed in the **Virtual Machines** or **Hosts** table.

   b. Select any item in the table for the side pane to display additional details.

   c. Click the ⤴ icon to view the details page for the item selected.

Dashboard   Browse

Filters   ✎ ⊗

Top Virtual Machines by: CPU   ⌄   ︿
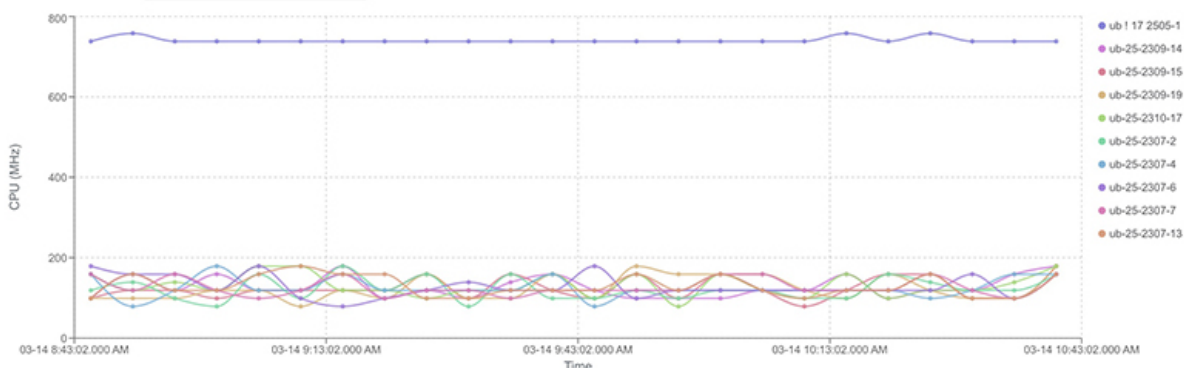
Virtual Machines

Anomaly Score	vCenter	VM	State	Network Adapters	IP Addresses	Network Usage	CPU	Memory	Storage	⚙
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-3 172.28.162.17	● Powered On	1	2001:172.31.3:1095:a6 d2:7011:1dda, 2001:172.31.3:956c:92 bd:46a3:13a + 7 More	-	-	15 MB	1.865 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-4 172.28.162.17	● Powered On	1	2001:172.31.3:794d:2b 3f:3230:75ac, 2001:172.31.3:250:56ff :fe85:6312 + 7 More	-	-	15 MB	1.865 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-5 172.28.162.17	● Powered On	1	2001:172.31.3:a467:90 77:851c:5176, 2001:172.31.3:219e:b3 eb:62d8:3d9a + 7 More	-	-	5 MB	1.865 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-6 172.28.162.17	● Powered On	1	2001:172.31.3:e92d:48 26:19b2:a8a0, 2001:172.31.3:4db:361 c:bf14:29ba + 7 More	-	-	15 MB	1.866 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-7 172.28.162.17	● Powered On	1	172.31.3.14, 2001:172.31.3:250:56ff :fe85:3897 + 7 More	-	-	5 MB	1.866 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-8 172.28.162.17	● Powered On	1	2001:172.31.3:2975:b5 79:6539:2d0c, 2001:172.31.3:250:56ff :fe85:6e28 + 7 More	-	-	10 MB	1.865 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-9 172.28.162.17	● Powered On	1	2001:172.31.3:f181:18 b0:d27e:6ddb, 2001:172.31.3:250:56ff :fe85:8e27 + 7 More	-	-	5 MB	1.864 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub () 17 2503-10 172.28.162.17	● Powered On	1	172.31.3.11, 2001:172.31.3:80b2:ae 36:20dd:e5d2 + 7 More	-	-	5 MB	1.865 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub ! 17 2505-1 172.28.162.17	● Powered On	1	172.31.5.20, 2001:172.31.5:711f:12 1:da99:a65e + 7 More	-	738 MHz	10 MB	1.869 GB	
✪ Healthy	vc-dos mageshk-162-216.cisco.com	ub ! 17 2505-2 172.28.162.17	● Powered On	1	2001:172.31.5:4de:63c 1:865d:a1a9, 2001:172.31.5:1013:3e 27:fa5f:7d11 + 7 More	-	-	15 MB	1.874 GB	

Virtual Machine Details Page

- The **Overview** tab in the virtual machine page displays information such as anomaly score,

usage, host, datastore, and network adapters.

- The **Alerts** tab in the virtual machine page displays the alarms from vCenter. In Nexus Dashboard Insights, the alarms from vCenter are displayed as anomalies. From the **Actions** drop-down menu, select an action to configure properties on an anomaly. See Configuring Anomaly Properties.

- 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.

  When there is an intermediate switch between the host and the leaf switch, the leaf switch in the host topology view displays as detached. Nexus Dashboard Insights is unable to determine the attached leaf switch port in such topologies. This will affect Cisco UCS B Series Blade Servers that have fabric switches between host blades and leaf switches, and it will also affect any other topologies with intermediate switches.

vCenter Hosts Dashboard

The **Overview** area in the dashboard displays the the hosts 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 Hosts 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 hosts based on drop-down list selection.
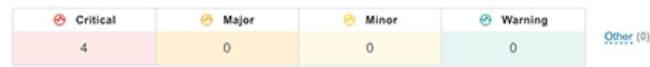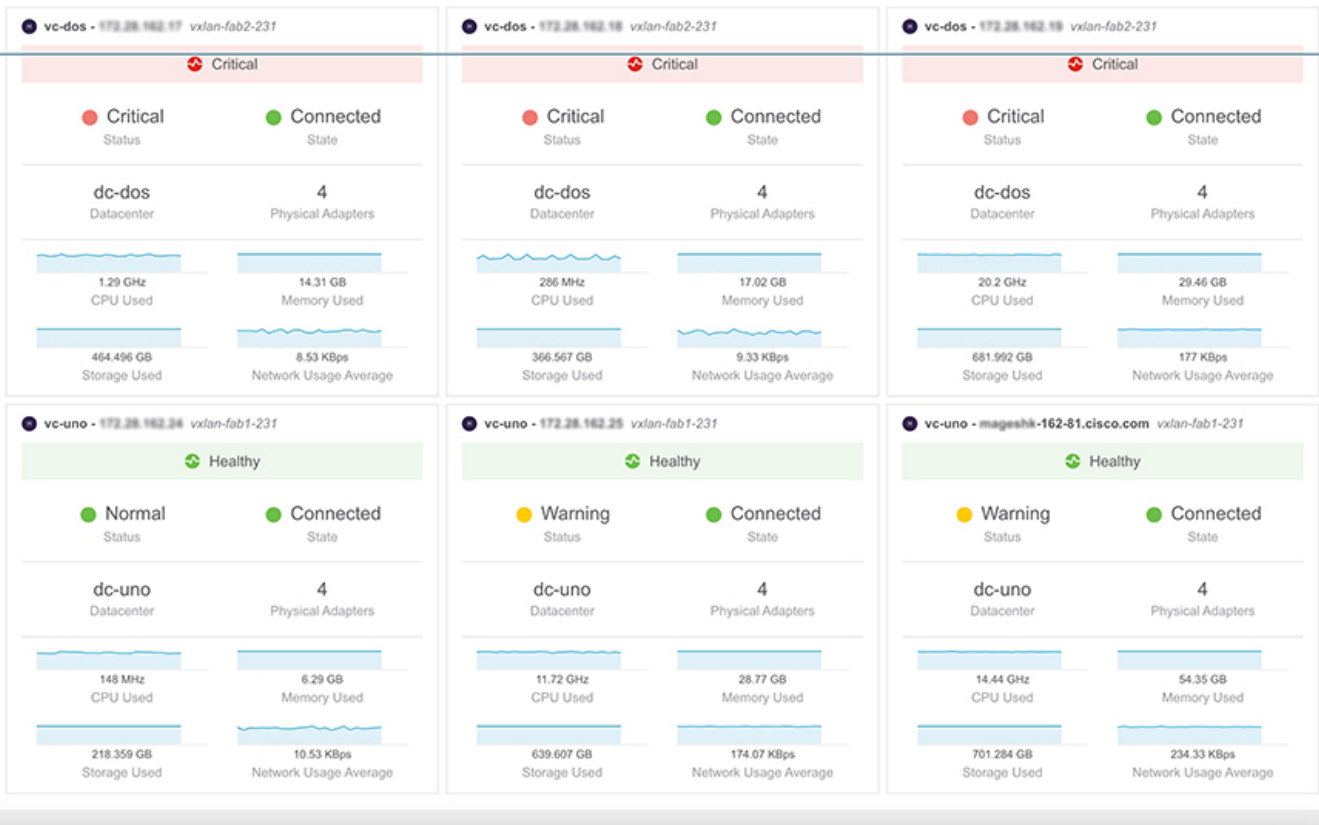
Browse

The browse page presents the **Top Hosts** by CPU plotted on a timeline. From the drop-down list, select CPU, memory, storage, or network usage to view the graphical representation of the top hosts based on drop-down list selection.

1. Use the filter bar to filter by vCenter IP, vCenter Controller, VM, host, datcenter, state, status, up time, virtual machines, cluster, hypervisor, model, processor type, logical processors, CPU, memory, and storage.

   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 hosts in a tabular format.

The **Hosts** table displays information such as Anomaly score, vCenter IP address, host IP address, sate, virtual machines, cluster, CPU , memory, and storage.

> ℹ️ The information displayed for CPU, memory, and storage match the information displayed in the VMware vCenter Host Summary page.

a. Click the **Settings** menu to customize the columns to be displayed in the **Virtual Machines** or **Hosts** table.

b. Select any item in the table for the side pane to display additional details.

c. Click the ⬀ icon to view the details page for the item selected.
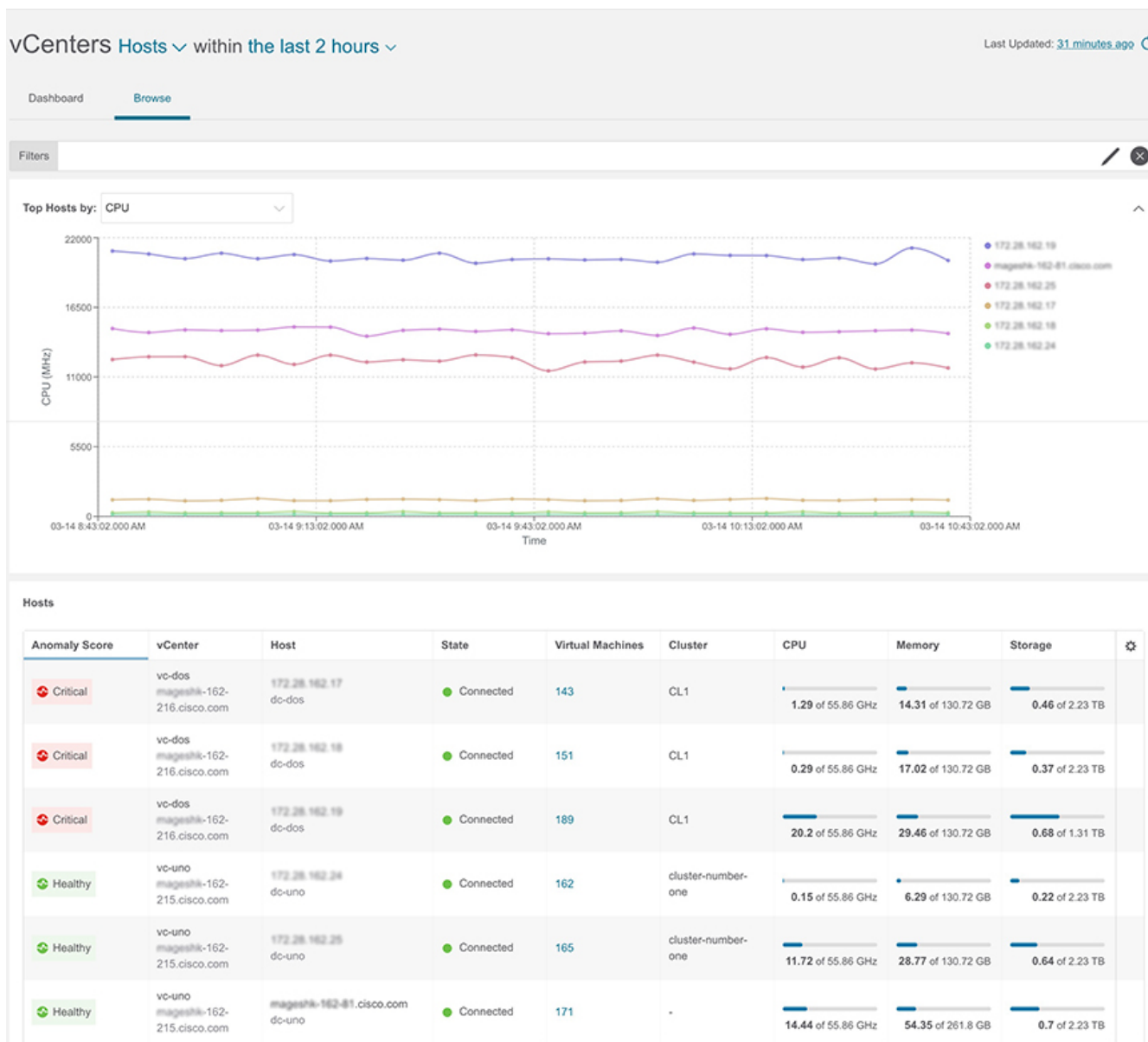
Hosts Details Page

- The **Overview** tab in the hosts page displays information such as anomaly score, usage, virtual machines, datastore, distributed switch, and standard switch.

- The **Alerts** 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.

Supporting Third-Party Nodes for Cisco Nexus Dashboard Insights

About Third-Party Nodes Support for Nexus Dashboard Insights

Cisco Nexus Dashboard Insights provides a way to gather data from third-party nodes.

The data is acquired through the third-party collector service using REST based EAPI method calls provided by the collector service.

The following telemetry information is collected from third-party nodes in the site:

- Environmental Statistics—This includes monitoring environmental statistics such as CPU, memory, fan, temperature, and power usage, and storage details of the site nodes.
- Interface Statistics—This includes monitoring of nodes, interfaces, and protocol statistics on Cisco NDFC and site nodes using LLDP and LACP.
- Resource Statistics—This includes monitoring software and hardware resources of site nodes on {CiscoNDFChortName} using IPv4 unicast, IPv4 multicast, and MAC.

Third-Party Hardware Support for Cisco NDFC

Nexus Dashboard Insights supports Arista 7050SX and 7280SR platform switches.

Third-Party Nodes Limitations for Nexus Dashboard Insights

- The Interface Statistics for LLDP and LACP do not support *Flap Count*, *Entries Aged Count*, and *PDU Timeout Count*.
- The Interface Statistics for MAC do not support local and static endpoints.
- Third-party nodes are discovered in a separate fabric.
- Third-party nodes are supported only on Monitored mode.
- Third-party nodes are accessible in non-privileged mode for data to be streamed.

Enabling Third-Party Nodes for Data Collection

Adding or removing the third-party nodes from the site will generate a control message, which triggers the third-party collector service present in the UTR pipeline to start or stop collecting data from the specific node.

To discover and enable third-party nodes to Cisco NDFC site:

- Create an external site to discover the third-party nodes, refer to Creating an External Fabric for details.

- To discover the third-party nodes, refer to Discovering New Switches for details.

- Add the third-party nodes to the external site, see Adding non-Nexus Devices to External Fabrics for details.

Configuring Third-Party Nodes in Cisco NDFC

Before you begin adding the third-party nodes to the site on Cisco NDFC, make sure the following requirement is met:

- You must have administrator credentials for doing the third-party node discovery.

Most of the Interface Statistics data is obtained with out any specific configuration for the third-party nodes. The following configuration is required for collecting port channel and storage statistics.

1. Setup the port channel for LACP. See Port Channel Configuration Procedures for details.

2. Execute the `aaa authorization exec default local` CLI command to collect storage statistics.