Cisco Network Assurance Engine Getting Started Guide, Release 5.1(1)

Table of Contents

First Published: 2020-11-13

Last Modified: 2021-04-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

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

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

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

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

Cisco Network Assurance Engine GUI

Overview of the GUI

The Cisco NAE GUI is a browser-based graphical user interface that communicates internally with the Cisco NAE software engine by exchanging REST API messages. At the top of the GUI are several tabs, and each tab expands to reveal subtabs. Choosing a subtab opens the respective inspector page. An inspector page provides information about the smart events for the respective portion of your network. Each inspector page generally has several areas and panes, and multiple dashlets in the areas.

On most pages, you can jump to the different areas by clicking the corresponding circular button in the middle of the right edge of the page. The blue circle is the currently-displayed area.

A dashlet is a small panel that provides a summary of a specific type of information that relates to the content of a page. The exact layout varies by inspector page.

The GUI contains the following pages:

> The tabs that you see listed below, depend upon the Assurance Group you are viewing in the GUI. If you are viewing an ACI Assurance Group, you will see all the tabs. If you are viewing a DCNM Assurance Group or an MSO Assurance Group, you will not have access to certain tabs. In addition, depending upon your Assurance Group there will be some differences in the content that you see within a tab. The table below displays information about which tabs are available for each Assurance Group. For further details, see **Cisco NAE Features Not Supported for NX-OS** and **Cisco NAE Features Not Supported for MSO** in the *Cisco Network Assurance Engine Installation and Upgrade Guide*.

- Dashboard tab—Provides a high-level overview of the health of the fabric.
- Explorer tab—Enables you to discover assets and their object associations in an easy-to-consume natural language query format.
- Change Management tab-
  - Policy Analysis—Provides information about the assurance on policy analysis changes.
  - Manage Pre-Change Analysis allows you to model the intended changes in Cisco NAE to verify if desired results are generated.
- Epoch Delta tab-Provides information about the state of the fabric between two epochs.
- Policy CAM tab—Provides information about the Policy CAM utilization in the Assurance Group.
- Compliance tab-Provides information about the state and health of the IT infrastructure.
- Smart Events tab—Provides information about all of the smart events.
- Global Search icon—Locates objects that you specify in the **Search** field, and the results appear below the **Search** field.
- Assurance Group drop-down list—Enables you to choose which assurance group to analyze.

Green color icon indicates an active Assurance Group.

- Settings menu—Enables you to perform various miscellaneous tasks, such as configure an assurance group, configure the log level settings, perform an offline analysis, manage users, view the REST API documentation, and see information about your installation of the Cisco NAE.
- User menu—Enables you to change your password, edit user account, or log out of the Cisco NAE.

Table 1. Cisco NAE GUI Menu Tabs Available in Release 5.1(0)

Tabs in GUI Menu	ACI Assurance Group Support	DCNM Assurance Group Support	MSO Assurance Group Support
Dashboard tab	Yes	Yes	Yes
Explorer tab	Yes	Yes	Yes
Change Management tab	Yes	No	No
Epoch Delta tab	Yes	Yes	No
Policy CAM tab	Yes	No	No
Compliance tab	Yes	No	No
Smart Events tab	Yes	Yes	Yes **Manage Event Rules** is not supported. Smart Events suppressed in the ACI epoch will not be propagated to the MSO epoch. Event suppression rules cannot be added in MSO epochs. Smart Event assignment is not supported in MSO epochs.

Cisco NAE GUI Icons

The following table provides a description of the Cisco NAE GUI icons.

Table 2. Cisco NAE GUI Icons

Icon	Description
+	A button that adds a virtual machine.
−	A button that removes a virtual machine.
⋮	A button that displays more options for a dashlet. In most cases, the options enable you to toggle a dashlet’s view between the grid view and chart view.
✕	A button that closes an overlay or removes data.
▾	An icon that indicates a drop-down list.
✎	A button that opens the form to edit data.
🗎	A button that opens the form to view details.
?	A button that provides helpful tips.
✓	An icon that indicates information events.
!	An icon that indicates minor events.
⚠	An icon that indicates major events.
✖	An icon that indicates critical events.
!	An icon that indicates warning events.
✕	A button that closes a mode.
▶	A button that plays or starts data fetching.
■	A button that stops data fetching.
↻	A button that refreshes a page or dashlet.
⚙	A button that opens the settings menu.
🔍	A button that opens the global search form.
⚠	An icon that indicates a server issue.
›	A button that expands the Policy CAM bar.
⌄	A button that expands the Events Trend dashlet.
⌃	A button that collapses the Events Trend dashlet.
i	A button in the **Settings** menu that opens a form that displays information about the installed Cisco NAE software build.
⚙	A button in the **Settings** menu that opens the assurance control configuration form.
☑	A button in the **Settings** menu that opens the appliance status form.
⚙	A button in the **Settings** menu that opens the appliance settings form.
⇪	A button in the **Settings** menu that opens the offline file management form.
📈	A button in the **Settings** menu that opens the offline analysis form.

Icon	Description
👥	A button in the **Settings** menu that opens the user management form.
LOG ⬇	A button in the **Settings** menu allows you to downloads tech support logs.
</> ⬇	A button in the **Settings** menu that allows you to download offline collection script.
●	An icon in the radial view of the visualization area that indicates an endpoint group.
ⓘ	An icon that you hover the mouse cursor over to see legend information.
↶	An icon in the Timeline area that goes back to the previous epoch selection.
▶|	An icon in the Timeline area that displays the oldest epoch.
|◀	An icon in the Timeline area that displays the latest epoch.
▶▶	An icon in the Timeline area that displays the next epoch.
◀◀	An icon in the Timeline area that displays the previous epoch.
☰	An icon that customizes the columns in a table.
⇕	An icon that indicates that the table can be sorted.
≡	An icon that indicates allows you to change the order of a column in a table.
✓	An icon that indicates a selected object.
☰	A button for Assurance Group List view
◌	An icon for Assurance Group In progress / running indicator
●	An icon for Assurance Group Status indicator
⊞	A button for Assurance Group Tile / Card view
◐	An icon for an epoch that was generated prior to Cisco NAE release 4.0(1)
◎	An icon for an epoch where the smart event is cleared
⊘	An icon for an epoch where the smart event is clearing
⬆	An icon for an epoch where the smart event is raised
>	A button to move to next
<	A button to move to previous
▼	An icon to indicate a filter
◓	An icon to indicate Policy CAM utilization > 90%
◓	An icon to indicate Policy CAM utilization 0% - 60%
◓	An icon to indicate Policy CAM utilization 75% - 90%
◓	An icon to indicate Policy CAM utilization 60% - 75%
📅	A button for date selection

Icon	Description
🕓	A button for time selection or scheduled
📄	A button to view the Cisco NAE Fundamentals Guide
⏻	A button to view the Cisco NAE Getting Started Guide
📦	A button to view the Cisco NAE Release Notes
{···}	A button to view the Cisco NAE Rest API Swagger Interface
⊗	A button to view the Cisco NAE Smart Events Reference Guide
API	A button to view the Cisco NAE REST API User Guide
⊞	A button to view the Cisco NAE Installation and Upgrade Guide

> ℹ Occasionally, on slower links, accessing Cisco NAE using IP address may result in the UI not displaying all the icons. Use the Fully Qualified Domain Name to display the icons.

Settings Menu

The **Settings** menu enables you to perform various tasks, such as configure an assurance group, configure the log level settings, perform an offline analysis, manage users, view the REST API documentation, and see information about your installation of the Cisco NAE. The menu contains the following items:

- **Assurance Groups**—Enables you to add, delete, or modify an assurance group.
- **Download Offline Collection Script**—Downloads the offline collection script.
- **Offline File Management**—Enables you to upload previously-downloaded fabric data so that you can use the Cisco NAE in offline data analysis mode. You can also delete offline data.
- **Offline Analysis**—Enables you to perform offline data analysis. Cisco NAE provides one-time assurance of the offline data.
- **Appliance Administration**—Displays details of the Cisco NAE appliance cluster such as information about each individual virtual machine in the cluster, software version installed, the configured log level settings for the appliance, the disk usage, and authentication domain details.
- **Appliance Status**—Displays the smart events that relate to the appliance.
- **User Management**—Enables you to create user accounts and change the password of the accounts.
- **Download Tech Support Logs**—Downloads the tech support logs as a .tar file to your local system.
- **License**—Enables you to register your Cisco NAE smart license.

- **Appliance Documentation**—Enables you to view and download Cisco NAE documentation.
- **About Cisco Network Assurance Engine**—Displays information about your installation of the Cisco NAE.

Timeline

The timeline is located near the top of the inspector pages. The timeline shows the date and time of data collection (not analysis). Data is represented by dots on the timeline, which are referred to as epochs.

An epoch is a period of time in your network's history during which the Cisco NAE collected and analyzed data. The size of the epoch gives a rough indication of the quantity of smart events at that time, with a larger epoch indicating more smart events.

An epoch can be one of the following colors:

- Gray—This indicates normal operation containing info events.
- Flashing Blue—This indicates that the Cisco NAE is currently running an analysis on the data.
- Red—This indicates critical errors are detected for an EPOCH during online analysis.
- Blue—This indicates an analysis based on offline data collection.

By default, the timeline shows a time range of 2 hours and 45 minutes with markings at 15 minute intervals to give you an estimate of when the data collection occurred. You can hover the mouse cursor over an epoch to see the exact time that the data collection occurred.

To export data, click **Export Data**. This allows you to save the data collected for a selected EPOCH during online analysis for offline analysis at a later time.

You can change the time range by clicking one of the preset time durations under the timeline, or you can click **Custom** to specify a time range of your choice. Optionally, you can hover over an epoch to highlight it (do not click the epoch), then click and drag the mouse cursor over the timeline to choose that area as the custom time range. You can scroll backward or forward in time by intervals of the chosen time range (with a default of 2 hours and 45 minutes) by clicking the left or right arrow buttons that are located at either end of the timeline.

The date and time displayed to the right of the timeline represents the date and time of the currently chosen epoch. Use the arrows under the timeline to go to the first epoch, go to the previous epoch, go to the next epoch, or go to the last epoch. The **Live Updates** button sets the timeline to display the current date and time. The **Epochs with my events** button sets the timeline to display the epochs that contain one or more events that have been assigned to a particular user.

> When you assign an event from one user to another, the events are not reflected in the **Epochs with my events** timeline immediately. To view the epochs with reassigned events you must either refresh the page or select a different Assurance Group.

We recommend that you view less than 500 epochs at one time. If you have a lot of epochs in a selected time-range, you can drag on the timeline to zoom into a smaller time window.

Summary Boards Area

The summary boards area provides a broad view of the issues that the Cisco NAE discovered in the fabric. For most pages, the summary boards area consists of the first two rows of dashlets. The exact composition of the summary area varies by page.

For example, when viewing an ACI Assurance Group, the **Policy CAM** page has one row for Summary Board, while the **Policy Analysis** page under **Change Analysis** has more rows.

For most pages, the dashlet in the first row provides the number of each type of smart event. The following list provides the types of events:

- **Critical**—Critical smart events indicate issues that you must address as soon as possible.
- **Major**—Major smart events indicate serious issues that do not stop your Assurance Group from functioning, but you should address them as soon as possible.
- **Minor**—Minor smart events indicate issues that are not serious, but you should address them eventually.
- **Warning**—Warning smart events indicate things that are not issues now, but they have the potential to become issues later.
- **Info**—Info smart events generally indicate objects that are healthy. A low number of info smart events can indicate that there are issues in the fabric, while a high number of info smart events can indicate that most objects are healthy.
- **Total**—The total number of smart events of all types on the page.

The second row usually contains two dashlets. The second row provides a different way (compared to the first row) of categorizing the issues.

Hot Topics Area

The hot topics area usually consists of a group of two or three dashlets. The exact number of dashlets varies by page.

The hot topics area helps you to determine which issues to resolve first by listing the objects of a particular type that have the most issues.

For the inspector pages with dashlets, the dashlets display the top four or five objects that have the most issues of the type indicated by the dashlet title. The title of each dashlet is a drop-down list that you can use to change the type of object for which the dashlet displays data.

You can click a violations count in a dashlet to go to the Smart Events area and have the area display more information about Smart Events of the appropriate severity type for the appropriate type of object.

Expanded Dashlet View

At the bottom of each dashlet is a link that opens a page with an expanded dashlet view. The expanded view displays the same data for all objects (not just the top four or five) of the type that is appropriate for the dashlet. You can choose the type of object using the title drop-down list.

Some of the columns have a search field in which you can type a string, which narrows the table to only those objects whose values contain the string for that column's parameter.

You can sort the table by one of the columns in descending or ascending order by clicking the **Sort** button next to the column's header. Clicking the button multiple times cycles through the sort options, and clicking on a different column's sort button resets the previous column's sort order and sorts the table by the new column. Optionally, you can hold **Shift** and click more than one of the **Sort** buttons to sort by multiple columns.

You can click a violations count to close the expanded dashlet view, go to the Smart Events area, and have the area display more information about Smart Events of the appropriate severity type for the appropriate type of object. Also, in the visualization area, the filter becomes set to filter for the Smart Events of the object that you clicked and the **View Control** options get set based on what you clicked. You can use this functionality only if the violation count is greater than 0.

Global Search

Global Search searches for objects (across multiple epochs) that you specify in the **Search** field.

When you click in the **Search** field, you can search by resource name or DN. Clicking again in the **Search** field, allows you to add additional resource names or DNs to further qualify your search.

When you perform a search, auto-completion is not supported for some of the search terms in some of the Inspector pages. If you do not receive any visual feedback when you enter a value for a search term, then you must enter the full search string or value.

The results of the Global Search appear in tables below the **Search** field.

- All Smart Events: Contains Smart Events data.

The following results apply for ACI Assurance Group only:

- Tenant Endpoint Details: Contains endpoint data.
- Prefix Table: Contains L3 forwarding data.

> ℹ Global Search does not support searches of a Pre-Change Analysis epoch.

Performing Global Search

Use the following procedure to perform a global search.

Procedure

1. Launch Global Search by clicking the global search icon 🔍 (located in the upper right of the NAE GUI)
2. Click date/time (left of the **Search** field) to display the the pop-up window to configure the From date/time or To date/time period for the search.
   - You can configure the date by clicking a specific day in the calendar that appears.
   - You can configure the time by clicking the time field and adjusting the time of day in the time pop-up window. The number of epochs that exist in the configured time period appears below the calendars.
3. Click **Apply** to save your From date/time and To date/time specifications.
4. Click the **Search** field to specify the objects to search for. You can select the type of object and its specific instance from the menus that appear. You can also enter a partial identifier of an instance to filter the menu of available instances.
   - Each additional unique object adds a logical AND condition to the global search.
   - Each additional non-unique object adds a logical OR condition between the same object type to the global search.
   - As each object is added to the search field, the global search feature provides search results dynamically.
   - You can clear all the search objects from the **Search** field by clicking the remove data icon ✕ (located at the right side of the search field).

Guidelines and Limitations

The following apply to performing a global search:

- The maximum number of search parameters is 25.
- The default From date/time through To date/time period is one day.
- The maximum number of epochs that global search supports is 288 epochs or up to 3 days.
- A search for all objects (blank search) is done by not specifying search objects, clicking the search field, and pressing the Enter key.

Guidelines and Limitations for ACI Only

- Global Search (Cisco NAE release 4.0(1) and later) supports searching for Cisco ACI GOLF routes by specifying the Route object. The results of the global search appear in the Prefix Table with an External dynamic (golf) subnet type.
- Depending on the global search results, multiple rows may be displayed for same event, prefix or endpoints in the global search result tables.

Guidelines and Limitations for NX-OS Only

Global Search currently supports **All Smart Events** only.

Guidelines and Limitations for MSO Only

When viewing the **Global Search** screen for MSO, in the **All Smart Events** table under the **Individual** tab, you can view aggregated ACI event details in MSO by choosing the ACI fabric from the **Epochs** column. You can view MSO Infra event details by clicking an epoch in the **Epochs** column. **Sites** and **AG** (Assurance Group) name columns are also available in the table.

Viewing Global Search Results

The tables below the **Search** field contain the global search results:

Table	Description
All Smart Events	Smart Events data
Tenant Endpoint Details	Endpoint data (Currently, this is supported for ACI Assurance Group only.)
Prefix Table	L3 forwarding data (Currently, this is supported for ACI Assurance Group only.)

Guidelines and Limitations

The following apply to viewing results of a global search:

- You can filter the Global Search results by clicking specific filter icons located in the row above the timeline. A highlighted icon enables the filter, such as for a specific severity or for a specific event category. Clicking the filter icon at the beginning of the row de-selects all filter selections.
- You can select an epoch by clicking an indicated epoch located on the timeline below the **Search** field.
- The timeline that appears with Global Search does not have the zoom in/zoom out controls as the timeline that appears in each of the tabs of the NAE GUI. Instead, highlighting a group of adjacent epochs on the Global Search timeline magnifies the scale of the timeline (zoom in). Clicking the dates to the right of the timeline resets the timeline scale.
- Epochs that appear on the timeline as a solid color icon indicate epochs that were created with Cisco NAE release 4.0(1) or later releases. Epochs that appear on the timeline as a 2-color icon (◐) indicate epochs that were created with Cisco NAE release 3.1(1) or earlier releases.
- Global search does not support configuring a search containing epochs that were created with Cisco NAE release 3.1(1) or earlier releases with epochs that were created with Cisco NAE release 4.0(1) or later releases.
- When viewing All Smart Events:
  - Click **Aggregated** to view the aggregated Global Search results organized by smart events in the Event Name column.
    - Click a smart event in the Event Name column to view every individual occurrence of the smart event across epochs.
  - Click **Individual** to view every individual occurrence of the smart event across epochs.
    - Click a timestamp in the Epochs column to view the lifecycle and details of the smart

event that occurred in that epoch.

- You can export detailed information about all the entries displayed in a table (All Smart Events) to a file formatted as comma separated variables (csv) or JSON. Click the **Settings** icon and select Export to CSV or Export to JSON to export to the desired file type. The exported file is available as a download from your browser.

Guidelines and Limitations for ACI Assurance Group Only

- Search results that contain smart events related to Cisco ACI GOLF routes (Cisco NAE release 4.0(1) and later), can be displayed by entering GOLF in the filter field of the Subnet/Route column in the Prefix Table.
- You can export detailed information about all the entries displayed in a table for Tenant Endpoint Details and Prefix Table to a file formatted as comma separated variables (csv) or JSON. Click the **Settings** icon and select Export to CSV or Export to JSON to export to the desired file type. The exported file is available as a download from your browser.

Viewing Search Results of a Specific Smart Event

Clicking a specific smart event in the search results displays all occurrences of the smart event in the specified time range. The occurrences are displayed in a table with information about the Epoch, Leaf, Interface, and Event ID for each of the occurrences. You can filter the entries of the table by entering a string of characters in the filter fields of the table to show only those entries that contain the specified characters. The filter fields are located below the headings of the columns of the table.

For example, if the character "3" is entered into the filter field of the Interface column, only those occurrences that contain "3" in their Interface would be displayed.

> The filtering of Event IDs is not supported outside the display of Global Search results.

> The filtering of Event ID supports only smart event occurrences that are associated with Epochs that occurred with Cisco NAE release 4.1(1) and later. Filtering Event IDs is not supported in earlier Cisco NAE releases.

You can export detailed information about all the entries displayed in the table to a file formatted as comma separated variables (csv) or JSON. Click the **Settings** icon and select Export to CSV or Export to JSON to export to the desired file type. The exported file is available as a download from your browser.

Smart Events Area

By default, the smart events area lists all of the smart events that are relevant to the inspector page. The title of the table indicates the total quantity of smart events that are on the table. The columns of the smart events table vary depending on the inspector page, although all smart events tables have the following columns:

- **Severity**—The severity type of the smart event, represented by the icon for that severity type.

This column has a search field that enables you to filter for smart events of the severity type that you specify. Enter the severity type as a string in the field. The possible severity types are as follows:

  - Critical
  - Major
  - Minor
  - Warning
  - Info

- **Event Category**—The Category for the smart event.
- **Event Subcategory**—The subcategory for the smart event.
- **Event Name**—The code for the smart event.
  - You can click a code to expand the row to display the additional information about the smart event. Depending on the settings for displaying smart event attributes, a table with Epochs information is displayed for each instance of the smart event.

> When navigating through the Cisco NAE GUI, we recommend that you wait for the page to finish loading before navigating to another page in the GUI. The more Smart Events that are required to be rendered, the slower the page will load.

You may export the information in the smart events table. Clicking the **Settings** icon ⚙ allows you to specify an export to CSV or to JSON.

At the bottom right of the smart smart events area, you can choose how many rows to display on a page.

See the *Cisco Network Assurance Engine Smart Events Reference Guide* for more information.

> If the event suppression feature is activated, the smart event count and the smart events listed take into account the event rules.

See About Smart Event Suppression for more information.

Exporting Data from the GUI

Starting from Cisco NAE release 2.1(1), you can export the data from certain tables in the GUI to JSON and CSV format.

Exporting the data from all the **Smart Events** tables in the GUI is supported.

> For ACI Assurance Group only: The export of the Prefix table or the Endpoint Details table in the GUI is not supported in Cisco NAE release 4.0(1). You can however export the data using REST APIs. We recommend that you use the REST APIs to export the data only for debugging and not in a production environment.

REST API for exporting the data from the **Prefix** table

```
{{host_ip}}/api/v1/event-services/assured-networks/{{fabric_id}}/model/aci-
routing/tenant-forwarding/prefix?$epoch_id={{epoch_id}}&$page=0&$size=1000&$sort=-
severity&exportCategory=PREFIX_TABLE&fileName={{file_name}}&mediaType={{media_type,
eg: json/csv }}
```

REST API for exporting the data from the **Endpoint** table

```
{{host_ip}}/api/v1/event-services/assured-networks/{{fabric_id}}/model/aci-
routing/endpoints/?$epoch_id={{epoch_id}}&$page=0&$size=1000&$sort=-
maxSeverity&exportCategory=ENDPOINT_DETAILS&fileName={{file_name}}&mediaType={{media_t
ype, eg: json/csv }}
```

To export data to the JSON format, navigate to the table in the inspector page and then choose **Table Settings** > **Export to JSON**.

To export data to the CSV format, navigate to the table in the inspector page and then choose **Table Settings** > **Export to CSV**.

Important Notes

- The data from all the columns in the table are exported irrespective of the columns selected in the **Column Customization** setting for the table.
- Ordering the table columns using the **Column Customization** setting does not affect the order of the columns when the data is exported.
- In each export instance you can export the data contained in 10,000 rows. To export the data from a table containing more than 10,000 rows, you must select the rows containing the dataset to be exported.
- In the Cisco NAE release 4.0(1), you cannot export the data from the **Prefix** and **Endpoint** tables using the GUI. You can however export the data using REST APIs. We recommend that you use the REST APIs to export the data only for debugging and not in a production environment.

REST API for exporting the data from the **Prefix** table

```
{{host_ip}}/api/v1/event-services/assured-networks/{{fabric_id}}/model/aci-
routing/tenant-forwarding/prefix?$epoch_id={{epoch_id}}&$page=0&$size=1000&$sort=-
severity&exportCategory=PREFIX_TABLE&fileName={{file_name}}&mediaType={{media_type,
eg: json/csv }}
```

REST API for exporting the data from the **Endpoint** table

```
{{host_ip}}/api/v1/event-services/assured-networks/{{fabric_id}}/model/aci-
routing/endpoints/?$epoch_id={{epoch_id}}&$page=0&$size=1000&$sort=-
maxSeverity&exportCategory=ENDPOINT_DETAILS&fileName={{file_name}}&mediaType={{media_t
ype, eg: json/csv }}
```

Perform Analysis

Assurance Control Modes

Cisco NAE assurance control capability enables you to analyze the Assurance Group in two modes, online analysis and offline analysis.

ACI Assurance Group: An ACI Assurance Group is comprised of the entire ACI fabric. An ACI fabric is made up of the APIC host and all leaf switches and spine switches controlled by the APIC controller. All the network nodes (APIC controller, leaf switches and spine switches) are analyzed together as part of the Assurance Group. Optionally, an Assurance Entity (if it exists in the ACI fabric) can be included in the Assurance Group. An Assurance Entity is an ancillary item in the ACI fabric that provides support to the overall fabric. For example, a load balancer would be considered an ancillary item in an ACI fabric and could be included in an Assurance Group.

DCNM Assurance Group: A DCNM Assurance Group is comprised of a fabric running NX-OS, either fully managed or only monitored by DCNM. All of the switches in the fabric are analyzed as a part of the Assurance Group. With a NX-OS based fabric, the fabric could be a DCNM managed fabric or it could be configured using other means such as CLI, Ansible, or any other configuration automation mechanism. For fabrics not using DCNM for configuration management, DCNM must be installed and the fabric must be discovered in read-only or monitor mode. Cisco NAE uses DCNM for topology discovery and to identify the role of the switch in the fabric.

MSO Assurance Group: An MSO Assurance Group is supported by Cisco NAE. Cisco NAE queries the sites that Cisco Multi-Site Orchestrator (MSO) manages and controls the configurations. To provide MSO assurance, Cisco NAE aggregates all the ACI sites that are on-boarded as individual assurance groups, and the associated Smart Events are also aggregated. Data from all the ACI sites are aggregated to create a consolidated set of events. Each object is uniquely identified by its DN across sites. In addition, Smart Events are provided for site-to-site connectivity for the MSO Assurance Group.

Assurance control involves collecting data from the Assurance Group, running the analysis to create a model with the collected data, and generating the results. The results are then displayed on the **Dashboard**.

Online analysis provides assurance on the Assurance Group in real time. In online analysis data collection, model generation, and results generation are carried out simultaneously. In the online mode the collected data is analyzed immediately after collection followed by result generation. This is repeated after a fixed time interval as specified by the operator.

Offline analysis provides a one-time assurance of the Assurance Group. Offline analysis offers the flexibility of decoupling the data collection stage from the analysis stage. In offline analysis data is collected using a Python script and the collected data is then uploaded to Cisco NAE to provide one-time assurance. The collected data can also be analyzed at a later time. It enables the operator to collect the data during change management windows and then perform the analysis. It also fulfills compliance requirements of an organization.

Beginning with release 4.0(1), you can analyze multiple Assurance Groups. See Schedule Assurance

Group Analysis for more information.

Supported Topology for Load Balancer Assurance Entity

This feature is currently not available for DCNM Assurance Group.

If an Assurance Entity such as a load balancer is included in an Assurance Group, Cisco NAE provides assurance for the load balancer by validating the APIC configurations related to the Application Delivery Controller (ADC) and verifying if the servers, virtual IP addresses (VIPs), and Self IP addresses are reachable. Cisco NAE performs the reachability checks and raises ADC smart events. See the *Smart Events Reference Guide* for information regarding the ADC smart events.

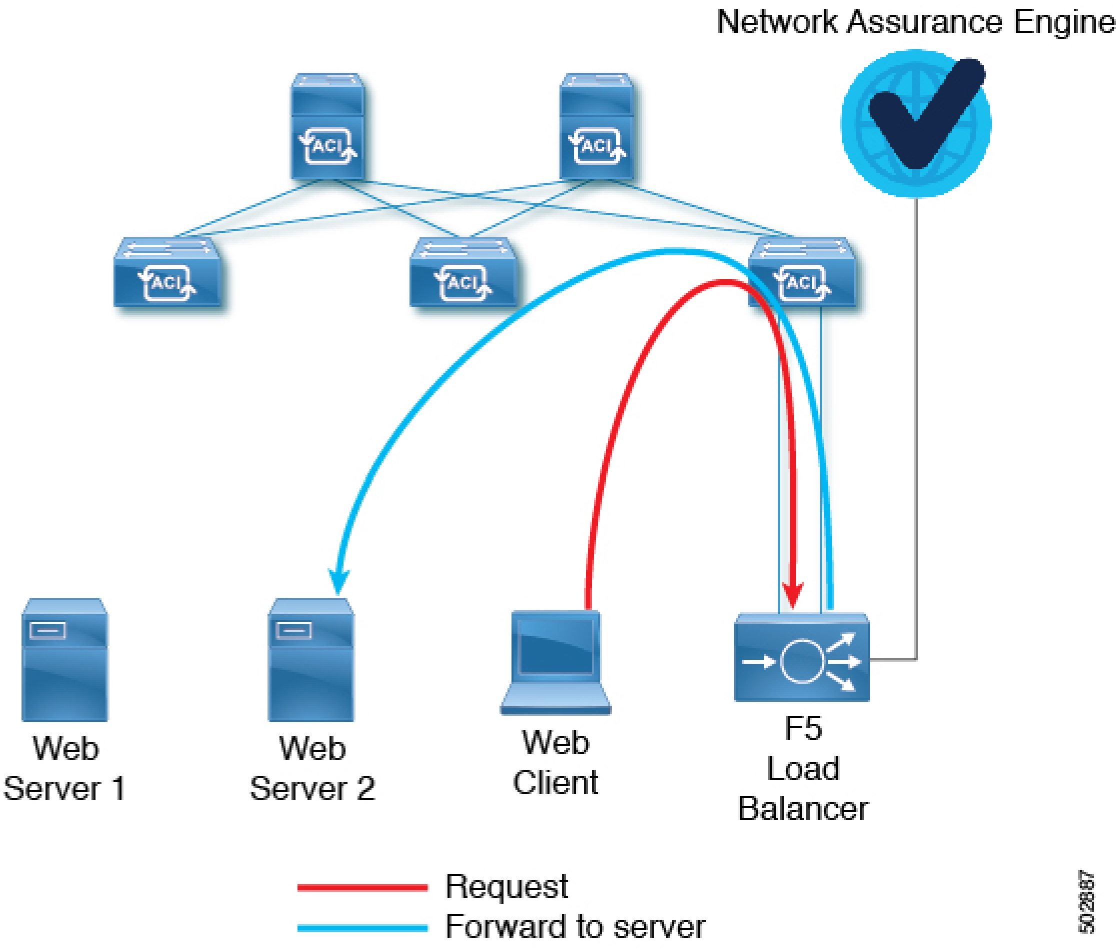

Figure 1. Topology for F5 Load Balancer

Guidelines and Limitations

Guidelines and Limitations for Assurance Groups

In Cisco NAE, with DCNM/NX-OS assurance groups and classical Layer2/Layer3 networks, support for assurance is limited to Layer1 smart events for access and fabric interfaces. Additionally, there are known false positives with respect to VPC smart events.

Guidelines and Limitations for Assurance Entities

- Assurance of F5 load balancer is supported only in unmanaged mode.
- Assurance of F5 load balancer is not supported if the F5 is used in a Service Graph.
- To assure a load balancer, enter the VRF information in the **Onboarding Info** field from the VRF DN. For example, for a VRF DN `uni/tn-TenantA/ctx-WebserverVRF`, in the **Onboarding Info** enter `WebserverVRF`. VRF with the same name in different tenants are not supported.
- You must configure Big IP without route domain.
- Assurance of F5 load balancer is supported in one-arm and two-arm deployment modes.

Performing Online Analysis

An Assurance Group provides Intent Assurance for a group of entities at the same time. Assurance Group configuration allows you to configure the entities that need to be analyzed together. Performing online analysis allows the Cisco NAE to collect data from the Assurance Group, build a model with the collected data, and generate results. The results are displayed on the **Dashboard** as Epochs.

Performing Online Analysis for ACI Assurance Group

If an Assurance Entity such as a load balancer is included in an Assurance Group, Cisco NAE provides assurance for the load balancer by validating the APIC configurations related to the Application Delivery Controller (ADC) and verifying if the servers, virtual IP addresses (VIPs), and Self IP addresses are reachable. Cisco NAE performs the reachability checks and raises ADC smart events. See the *Smart Events Reference Guide* for information regarding the ADC smart events.

Use this procedure to perform ACI online analysis.

Before You Begin

- You must have the credentials to access the APIC hosts.
- APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure export policy.
- You must have the credentials to access the load balancer if you use a load balancer in the Assurance Group.

Procedure

1. Choose **Settings** > **Assurance Groups**.
2. Click **Create New Assurance Group**.
3. From the drop-down list, choose **ACI**.
4. Complete the following fields for **Create New ACI Assurance Group**.
    a. In the **Name** field, enter the name.
    b. In the **Description** field, enter the description.

c. Check the **Switch to online mode** check box, to automatically analyze the Assurance Group in real time. Ensure that **Switch to online mode** check box is selected.

d. In the **Username** field, enter the user name to access the APIC hosts.

e. In the **Password** field, enter the password to access the APIC hosts.

f. From the **Analysis Interval** drop-down list, choose the interval to run the analysis. Analysis interval includes the time to collect data from APIC and the switches, analyze the data to build a model, generate results, and display them on the Dashboard. For production environments, the recommended analysis interval is a minimum of 15 minutes. An interval below 15 minutes should be used only in lab environments or for testing.

g. From the **Analysis Timeout** drop-down list, choose the time the system needs to wait before terminating the analysis. This value should be greater than the **Analysis Interval**

h. In the **MSO Assurance Group** field, from the drop-down list you have the option to choose the name of the MSO Assurance Group if already available.

i. Check the **Start Immediately** check box, to start the analysis of the selected Assurance Group immediately.

5. Complete the following fields for **APIC Hosts**.

   a. In the **APIC Hostname 1** field, enter the APIC host name in the format apic1.example.com.

   b. Click + to add another APIC host name. We recommend that you add all the APIC hosts to the Assurance Group.

6. (Optional) Click the **Add New Load Balancer** link to add a load balancer to the Assurance Group, and complete the following fields for **Load Balancer**.

   a. In the **Load Balancer Name** field, enter the name of the load balancer.

   b. in the **IP Address/Hostname** field, enter the IP address or host name for the load balancer.

   c. In the **Username** field, enter the user name to access the load balancer.

   d. In the **Password** field, enter the password to access the load balancer.

   e. (Optional) In the **Chassis Serial Number** field, enter chassis serial number of the load balancer to validate if the Assurance Entity is a load balancer.

   f. (Optional) From the **Onboarding Info** drop-down list, choose SIP-VRF or VIP-VRF and in the **Onboarding Info** field, enter the appropriate identifier that exists in the ACI fabric . SIP-VRF and VIP-VRF is required to determine if the server IP (SIP) address and virtual server IP (VIP) address are present in the VRF and the servers are reachable. See Guidelines and Limitations for VRF syntax.

   g. Click **Save**.

7. Complete the following fields for **Collection Settings**. Collection settings are required for NAT and epoch delta analysis. See Creating Epoch Delta Analysis. See Management and Network Connectivity.

   a. Check the **Use APIC Configuration Export Policy** check box, to export configuration policy for policy delta.

   b. Click **Show**.

c. Select the **Export Format**.

d. In the **Export Policy Name** field, enter policy name.

e. Check the **Use NAT Configuration File** check box, to upload a file that has the Network Address Translation (NAT) table.

f. Click **Show**.

g. Click **Download NAT Configuration File Template**.

h. Enter the public and private IP address mapping in the NAT configuration CSV file to indicate the NAT translation that needs to be used to access the APIC hosts.

i. Click **Browse** to upload the CSV formatted NAT configuration file containing the public and private IP address mapping to be used to access the Assurance Groups.

j. In the **File Name** field, enter the file name and click **Upload**.

8. Click **Save**.
9. The status of the analysis is displayed in the Data Collection form. Cisco NAE performs analysis on only one fabric at a time. To perform analysis on another fabric, you must stop the analysis on the current fabric and then start the analysis on another fabric. You can perform the following actions:
   - Click the play icon to start the analysis.
   - Click the stop icon to stop the analysis.
   - See Managing Assurance Group.
10. To view the results of the analysis, click **Dashboard**. See Timeline. Ensure that you have the correct Assurance Group selected to view the results. Click **Assurance Group** and select the Assurance Group from the drop-down list.
11. To export data, select a epoch dot on the timeline and click **Export Data**.

Performing Online Analysis for DCNM Assurance Group

Performing online analysis allows the Cisco NAE to collect data from the DCNM Assurance Group, build a model with the collected data, and generate results. The results are displayed on the **Dashboard** as Epochs.

There are DCNM credentials for the DCNM controller and the LAN credentials which extends to the rest of the network which is the leaf and spine switches.

Use this procedure to perform DCNM online analysis.

Before You Begin

- You must have the credentials to access the DCNM hosts.

Procedure

1. Choose **Settings** > **Assurance Groups**.
2. Click **Create New Assurance Group**.

3. From the drop-down list, choose **DCNM**.
4. Complete the following fields for **Create New DCNM Assurance Group**.
    a. In the **Name** field, enter the name.
    b. In the **Description** field, enter the description.
    c. Check the **Switch to online mode** check box, to automatically analyze the Assurance Group in real time. Ensure that **Switch to online mode** check box is selected.
    d. In the **DCNM IP address** field, enter the IP address to access your DCNM.
    e. In the **DCNM Password** field, enter the DCNM password.
    f. In the **Site Name** field, enter the site name for the site that DCNM in your Assurance Group manages.

    > ℹ DCNM can manage multiple sites. For NAE support, one assurance group maps to one such site.

5. In the **Default LAN Credentials** area perform the following actions:
    a. In the **LAN Username** field, enter the username.
    b. In the **LAN Password** field, enter the password.

    > ℹ In the following steps, add switches to the list and specify their credentials only if the switch credentials do not match the default credentials provided above. If that login fails, Cisco NAE will log an event stating the login failure. In this context, switch refers to leaf and spine switches.

6. In the **Switch Credentials to Override the Default Credentials** area, click **Add Switch**, and perform the following actions.
    a. In the **Switch Name** field, enter the name for the switch.
    b. In the **Switch IP Address** 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. Click **Add Switch** to add credentials for additional switches if required.
7. Click **Save**.

Performing Online Analysis for MSO Assurance Group

To provide MSO assurance, Cisco NAE aggregates all the ACI sites that are on-boarded as individual assurance groups, and the associated Smart Events are also aggregated. Data from all the ACI sites are aggregated to create a consolidated set of events.

Use this procedure to perform MSO online analysis.

Before You Begin

- You must have an MSO instance identified for Cisco NAE assurance.

Procedure

1. Choose **Settings** > **Assurance Groups**.
2. Click **Create New Assurance Group**.
3. From the drop-down list, choose **MSO**.
4. Complete the following fields for **Create New MSO Assurance Group**.
    a. In the **Name** field, add a name for the MSO Assurance Group.
    b. In the **MSO hostname1** field, enter the IP address for the MSO hostname.
    c. In the **MSO Username** field, enter the username for the MSO hosts to which you want access.
    d. Modify the **Analysis Interval** field, if required. The default value is 15 minutes.
    e. Modify the **Analysis Timeout** field, if required. The default value is 60 minutes.
5. Click **Save** to create the MSO Assurance Group.

Important Guidelines for MSO Assurance Groups

- When creating an MSO Assurance Group and after you enter the MSO hostname, MSO Username, and MSO Password, Cisco NAE fetches the sites that MSO is managing. These are displayed in **Associated ACI Assurance Groups** area of the screen. Cisco NAE correlates these sites with the sites that are available. If there are any sites that are managed by MSO but are not available as an ACI Assurance Group, Cisco NAE displays them so you have the option to include the missing site/s into the MSO Assurance Group.
- You can create an MSO Assurance Group without associating an ACI Assurance Group to it right away. You can associate the desired ACI Assurance Group/s later. However, in order to start an MSO Assurance Group analysis, you must have at least one ACI Assurance Group associated with it.
- When scheduling an analysis for ACI and MSO Assurance Groups, in the Assurance Groups screen, you must choose the items in a specific running order. Choose the appropriate ACI Assurance Group/s one by one first, and then choose the appropriate MSO Assurance Group/s. The running order will be sequentially displayed.
- You cannot delete an ACI Assurance Group that is associated to an MSO Assurance Group, but you can disassociate the ACI Assurance Group from the MSO Assurance Group.
- If an ACI Assurance Group is associated with an MSO Assurance Group, and an analysis has been completed, the ACI Assurance Group cannot be deleted even after disassociating it from the MSO Assurance Group. This is because MSO epochs will have cross references to the ACI Smart Events.
- You cannot associate an ACI Assurance Group with another MSO Assurance Group if it was previously associated to an MSO Assurance Group and has epochs present in the database. For example, if ACI-1 is associated with MSO-1 and an analysis has been completed, the user can

disassociate ACI-1 from MSO-1 but cannot associate ACI-1 with another MSO Assurance Group, such as MSO-2. This is because MSO-1 has the aggregated events from ACI-1 which will continue to be used to get the details of the Smart Events. You can associate ACI-1 back with MSO-1 if required. You can associate ACI-1 with MSO-2 only after MSO-1 has been deleted because this would result in ACI-1 references not being required by MSO-1 any longer, and therefore ACI-1 is ready to be associated to a new MSO.

- You can delete an ACI Assurance Group or associate it with a new MSO Assurance Group only after the first MSO Assurance Group that was associated with the ACI Assurance Group has been deleted.

Performing Offline Analysis

Use the procedure to perform offline analysis. See the Offline Data Collection Script for information about the Offline Data Collection Script.

Procedure

1. Choose **Settings** > **Download Offline Collection Script** to download the python script.
2. Run the downloaded script to collect the data for assurance. See README for more information.

> ℹ 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 NAE will indicate that the APIC version is unsupported.

3. Choose **Settings** > **Offline File Management** to upload the collected data.
4. Click **Create New Upload**.
5. In the **Create New Upload** form, complete the following fields.
   a. Click **Browse** to upload the collected data to provide one-time assurance.
   b. In the **Name** field, enter the name of the file.
   c. In the **Description** field, enter the description.
6. Click **Submit**. After the file has been uploaded successfully, it is displayed in the Upload table.
7. Choose **Settings** > **Offline Analysis**.
8. In the **Create New Offline Analysis** form, complete the following fields.
   a. In the **Analysis Name** field, enter the name of the offline analysis.
   b. From the **File** drop-down list, choose the file with the collected data.
   c. From the **Assurance Group** drop-down list, choose the Assurance Group.
   d. (Optional) Click **Create New Assurance Group** to add another Assurance Group. Use this form if you want to define a new Assurance Group with different attributes.
   e. From the **Analysis Timeout** drop-down list, choose the time the system needs to wait before terminating the analysis. You can also enter the time the system needs to wait before terminating the analysis.

9. Click **Run** to run the offline analysis. After the offline analysis is completed, the status is displayed in the **New Offline Analysis** form. Cisco NAE performs analysis on only one fabric at a time. To perform analysis on another fabric, you must stop the analysis on the current fabric and then start the analysis on another fabric.
10. To view the results of the analysis, click **Dashboard**. See Timeline.

Offline Data Collection Script

Offline Data Collection Script for ACI Assurance Group

The Cisco NAE offline data collection script is a Python script that polls the Cisco Application Policy Infrastructure Controllers (APICs), spine switches, and leaf switches for a series of REST API and CLI calls. For information about the REST API calls and CLI calls, see the readme.md file that is included with the script.

The script has the following dependencies:

- Python 2.7.11+
- Ubuntu/OS X /Cent OS
- Python dependencies
  - Requests (Python REST library)
  - Paramiko (Python SSH library)
  - Setuptools (Python packaging library)

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

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

The readme.md file provides the syntax for using the script. By default, the script will run 3 iterations of the data collection at a 5 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 epochs 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.

Offline Data Collection Script for DCNM Assurance Group

The Cisco NAE offline data collection script for DCNM supports only out-of-band management connectivity.

Offline Data Collection Script for MSO Assurance Group

Cisco NAE must gather data from the ACI fabrics an MSO is monitoring and to which MSO is pushing configurations. This data must be collected from MSO using the offline data collection script. After this data is populated in Cisco NAE, then the data for individual ACI fabrics that the MSO is monitoring must also be collected in an offline manner. When uploading the dataset collection, the ACI fabrics must first be uploaded for offline analysis.

For offline analysis, you must associate the ACI fabrics to the MSO fabric during on-boarding, and then run the analysis on each ACI fabric followed by analysis on the MSO fabric.

The procedure for Cisco NAE offline data collection script for MSO is as follows:

1. Using the command option `--iteration 1`, collect the offline dataset from the ACI APICs that are managed by MSO using the offline script as described in the preceding section titled **Offline Data Collection Script for ACI Assurance Group**.
2. Run the offline analysis for ACI datasets with the respective offline assurance groups.
3. Collect the offline dataset from MSO using the command option `-cnaeMode MSO`. (See the readme.md file that is available inside the same zip file with the offline analysis script file.)
4. Create an MSO offline Assurance Group, and associate the respective offline ACI Assurance Groups with the MSO Assurance Group.
5. Start the analysis with the MSO dataset which will aggregate the data from the ACI Assurance Group, and complete the analysis.

> One iteration is recommended per dataset collection. In addition, make sure that the DNS resolution enables you to obtain the mapping between the ACI site name and the Assurance Group name correctly.

Schedule Assurance Group Analysis

Starting with Cisco NAE release 4.0(1), you can schedule an analysis for multiple Assurance Groups sequentially. When you schedule an analysis for multiple Assurance Groups, the analysis is performed using the round-robin scheduling algorithm.

Important Notes

- Scheduling analysis for multiple Assurance Groups is only supported for online analysis.
- The Assurance Groups must be located in the same data center.
- You can schedule the analysis for up to five Assurance Groups.
- Stop any analysis on the Assurance Group before creating a schedule.
- When scheduling an analysis for ACI and MSO Assurance Groups, in the **Assurance Groups** screen, you must choose the items in a specific running order. Choose the appropriate ACI Assurance Group/s first, and then choose the appropriate MSO Assurance Group/s. The running

order will be sequentially displayed.

Procedure

Use this procedure to schedule the analysis for Assurance Groups.

1. Choose **Settings** > **Assurance Groups**.
2. (Optional) In the Assurance Group page, click the **Sort** icon to sort the Assurance Groups by Name, Operational Mode, or Schedule.
3. Click **Schedule** located on the right side of the **Assurance Groups** page.
4. In the **Analysis Interval** field, choose the desired interval. The analysis interval enables you to schedule the wait time between the scheduled Assurance Group runs. The default analysis interval is 15 minutes. The interval value must be between 5 mins to 24 hours in multiples of 5 mins.
5. Select the Assurance Groups. You cannot schedule an analysis for Assurance Groups running offline analysis.
6. In the **Timeline**, the scheduled order of the Assurance Groups and the approximate time to run the analysis is displayed. Review the schedule and click **Activate**.

Cisco Network Assurance Engine User Access and Authentication

User Access and Authentication

In Cisco NAE, an administrator can choose to configure users on the Cisco NAE appliance itself and not to use external AAA servers. These users are called local users. To configure local users, see Creating a User Account.

Cisco NAE also allows administrators to grant access to users configured on externally managed authentication servers such as Lightweight Directory Access Protocol (LDAP) and Terminal Access Controller Access Control System Plus (TACACS+). Users can belong to different authentication systems and can log in simultaneously to the Cisco NAE. To authenticate users with an LDAP or TACACS+ server, see Creating a New Authentication Domain.

A login domain defines the authentication domain for a user. Login domains can be set to the Local, LDAP, or TACACS+. When accessing the GUI, the Cisco NAE offers a drop-down list of domains to enable the user to select the correct authentication domain.

By default, the Local domain is set as the default authentication domain. The domain marked as the default authentication domain will appear at the top of the dropdown and be automatically selected on the login page. The default authentication domain is a system wide setting that affects all users. Login domains such as LDAP or TACACS+ can also be set as the default authentication domain.

> ℹ For remote authentication of the Cisco NAE app on Cisco Nexus Dashboard, if the remote server is reachable only from the management network, you must configure a route for the remote server by navigating to **Nexus Dashboard** > **Infrastructure** > **Cluster Configuration** > **Routes** > **Management Network Route**.

Session Management

In Cisco NAE, you can view or delete active user sessions using the REST API. These operations cannot be performed using the GUI.

See the *Cisco Network Assurance Engine REST API User Guide* for more information.

Creating a User Account

Use this procedure to create a new user account. Only an administrator can create a user.

Procedure

1. Choose **Settings** > **User Management**.
2. Click **Create New User Account**.

3. Complete the following fields for **Create New User Account**.
    a. In the **Email** field, enter the email address of the user.
    b. In the **Username** field, enter the username of the user account.
    c. In the **Password** field, enter the password to access the user account.
    d. Click **Save**.

Prerequisites

LDAP has the following prerequisites:

- You have configured the LDAP server.
- You have the created the Cisco NAE users on the LDAP server.
- You have created a group for Cisco NAE users.
- You have added the Cisco NAE users to the group.
- You have the base DN, bind DN, and group DN of the LDAP server.

TACACS+ has the following prerequisites:

- You have configured the TACACS+ server.
- You have the created the Cisco NAE users on the TACACS+ server.
- You have the host name or IP address, port number, authorization protocol, and key of the TACACS+ server.
- You may need to register all three Cisco NAE VMs as client devices if using Identity Service Engine (ISE).

Creating a New Authentication Domain

Use this procedure to create a new authentication domain. Only an administrator can create an authentication domain.

Before You Begin

- You have the host name or IP address, port number, bind DN, base DN, and group DN of the LDAP server.
- You have the host name or IP address, port number, authorization protocol, and key of the TACACS+ server.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Authentication Domains** tile.
3. Click **Create New Authentication Domain**

4. Complete the following fields for **Create New Authentication Domain**.
    a. In the **Name** field, enter the name of the authentication domain.
    b. (Optional) In the **Description** field, enter the description of the authentication domain.
    c. From the **Authentication Type** drop-down list, choose the authentication type such as LDAP or TACACS+.
5. Complete the following fields for **LDAP Server Configuration**.
    a. In the **Hostname** field, enter the hostname or the IP address of the LDAP server.
    b. (Optional) Click + to add another hostname. You can configure a maximum of 3 LDAP servers.
    c. Check **LDAPS** check box to connect to the LDAP server using a secure connection.
    d. In the **Port Number** field, enter the port number of the LDAP server. The valid port range is 0-5535.
    e. (Optional) In the **Bind DN** field, enter the bind DN in the format `cn=NAE User,ou=Systems,ou=IT,ou=Departments,dc=nae_customer,dc=com`.
    f. (Optional) In the **Bind Password** field, enter the bind DN password.
    g. In the **Base DN** field, enter the base DN in the format `dc=nae_customer,dc=com`.
    h. In the **Timeout** field, enter the timeout in seconds. The valid timeout range is 0-15 seconds for each host.
    i. In the **Group DN** field, enter the group DN for the Cisco NAE users in the format `cn=NAE group,ou=groups,dc=nae_customer,dc=com`. Only the users belonging to the LDAP group will be granted access to the appliance.
    j. In the **Filter** field, enter the filter in the format `(&(objectclass=person)(cn=$userId))`. Filter is used as a criteria to search for the user in the LDAP server.
    k. The **Attribute** field, is pre-populated.
    l. Click **Test Connection** to test the connection for the LDAP server.
        i. From the **LDAP Server** drop-down list, choose the LDAP server.
        ii. Enter the username and password to test the credentials on the LDAP server.
        iii. Click **Test**.
6. Complete the following fields for **TACACS+ Server Configuration**.
    a. In the **Hostname** field, enter the hostname or the IP address of the TACACS+ server.
    b. In the **Port Number** field, enter the port number of the TACACS+ server. The valid port range is 1-6553.
    c. From the **Authorization Protocol** drop-down list, choose the protocol type such as PAP, CHAP, or MS-CHAP.
    d. In the **Key** field, enter the shared secret used by TACACS+ client to authenticate with the TACACS+ server.
    e. In the **Confirm Key** field, enter the shared secret key again.
    f. In the **Retries** field, enter the maximun number of retries to connect to the TACACS+ server.

The valid retries range is 0-5.

g. In the **Timeout** field, enter the timeout in seconds. The valid timeout range is 1-15 seconds.

h. Click **Test Connection** to test the connection for the TACACS+ server.

7. Click **Save**.

Manage Pre-Change Analysis

Manage Pre-Change Analysis

> ℹ Currently this is supported for ACI Assurance Group only.

The **Manage Pre-Change Analysis** screen is under the **Change Management** tab.

When you want to change a configuration in an assurance group, a pre-change analysis allows you to model the intended changes in Cisco NAE, perform a pre-change analysis against an existing base epoch in the assurance group, and verify if the changes generate the desired results.

After you model the changes for a Pre-Change Analysis, you can choose **Save** or **Save And Run**. By choosing **Save**, you can save the Pre-change Analysis job without having to start the analysis right away. You can return to the job later, edit the changes if required, and then run the analysis later. The **Save** option is supported only for a Pre-Change Analysis with manual changes. If you choose **Save And Run**, you initiate the Pre-change Analysis job, and the operation results in Smart Events being raised as part of the analysis.

When you save and run the job, the changes are applied to the selected base epoch, the analysis is performed, and results are generated. When the analysis is completed, the pre-change analysis instance is listed in the **Manage Pre-Change Analysis** table. For every pre-change analysis listed in the **Manage Pre-Change Analysis** table, a delta analysis is generated between the pre-change analysis and the base epoch. When you click **View Epoch Delta**, it displays the delta analysis screen where you can view the differences in the smart events.

The pre-change analysis is also displayed in the Timeline as an icon above the associated base epoch. When you hover over this icon, you see a list of all pre-change analysis that have been run on that epoch.

If smart events are raised in the analysis, make the required modifications based on the results and re-run the analysis until you obtain satisfactory results.

The download option in a Pre-Change Analysis job allows you to download a JSON file that can be uploaded to Cisco APIC. However, you can upload a JSON or an XML Cisco APIC configuration file to run a Pre-Change Analysis job if you choose the file upload approach. If you run a Pre-Change Analysis job by manually providing modifications, in order to get the configuration JSON, your Assurance Group must have the **APIC Configuration Export Policy** field selected at the time of the base epoch creation. Otherwise, the download option will be disabled. If the download option is disabled, in the case of an online analysis, navigate to **Settings** > **Assurance Group**, choose the desired ACI Assurance Group, and choose **Edit**. Under **Collection Settings**, check the checkbox for the **Use APIC Configuration Export Policy** field. Then create a new online epoch, and then run the Pre-Change Analysis. This will enable the **Download** option. In the case of an offline analysis, at the time of data collection, the **-apicConfigExportPolicyName** , **-apicConfigExportFormat** arguments must be passed.

Once the analysis starts, the status of the job will be shown as **Running**. During this time, the specified changes will be modeled on top of the base epoch, and complete logical checks will be run, including Policy Analysis and Compliance. No switch software or TCAM checks will be performed. The status of the Pre-Change Analysis job is marked **Completed** when the entire analysis including Epoch Delta completes. The Epoch Delta is automatically triggered and the associated Pre-Change Analysis job us displayed as running during that time. The Epoch Delta is performed only on checks supported in Pre-Change Analysis job.

You can view the changes applied by a user to a specific Pre-Change Analysis job by clicking the Pre-Change Analysis job in the **Manage Pre-Change Analysis** table. This action displays the Pre-Change Analysis details for that job. If the changes in the Pre-Change Analysis job were applied manually, you can view the different changes selected by the user. If the Pre-Change Analysis job is created using a JSON file, the **Change Definition** field displays the name of the JSON file from where the changes were imported.

Starting with Cisco NAE release 5.0(1), you can perform Pre-Change Analysis for supported Fabric Access Policies using JSON/XML upload files (only). In addition, if the user wants to add, modify, or delete certain Fabric Access Policy associations, they can do so in the JSON/XML file, and save the modified file. Cisco NAE will verify that the changes are valid after which the JSON/XML file can be uploaded to Cisco APIC. When you create a Pre-Change Analysis and upload a JSON/XML file, it verifies if there are any unsupported objects and provides the user an option to continue or stop.

A Pre-Change Analysis job can be cloned if the same set of changes are required to be verified on different base epochs.

The resulting data of an analysis are stored as a Pre-Change Analysis epoch, displayed as an annotation on top of the base epoch, in the epoch timeline. Clicking this annotation takes you to the Delta Analysis screen.

Manage Pre-Change Analysis Options

The following list specifies the options you can choose to add to your pre-change analysis job. Only the objects listed are supported.

1. Add, modify, or remove Tenant.
2. Add, modify, remove App EPG (supported attributes: preferred group member, intra EPG isolation; relations for App EPG: BD, provided, consumed and taboo contracts; export/import of contracts is not supported.)
3. Add, modify, or remove a VRF (Supported attributes: policy control enforcement preference, policy control enforcement direction, BD enforcement status, preferred group member, description).
4. Add, modify, or remove a BD (Supported attributes: description, optimize WAN bandwidth, type, ARP flooding, IP learning, limit IP learning to subnet, L2 unknown unicast, unicast routing, multi-destination flooding, multicast allow, L3 unknown multicast flooding).
5. Add, modify, or remove a contract (Supported attributes: scope, description).
6. Add, modify, or remove a contract subject (Supported attributes: reverse filter ports, description, priority, target DSCP, filter name, forward filter name, reverse filter name).
7. Add, modify, or remove subnets (Supported attributes: scope, preferred, description, primary IP

address, virtual IP address, subnet control).

8. Add, modify, or remove an App profile (priority, description).
9. Add, modify, or remove an L3Out (Supported attributes: description, VRF name, Target DSCP, route control enforcement).
10. Add, modify, or remove an L2Out (Supported attributes: description, BD name, encapsulation type, encapsulation ID).
11. Add, modify, or remove an L3 Ext EPG (Supported attributes: preferred group member, description, priority, and supported relations: VRF, provided contracts, consumed contracts, taboo, target DSCP).
12. Add, modify, or remove an L2 Ext EPG (Supported attributes: preferred group member, description, priority, target DSCP and provided contracts, supported contracts, taboo contracts).
13. Add, modify, or remove L3 Ext EPG Subnets (Supported attributes: description, scope).
14. Add, modify, or remove a Taboo Contract (Supported attributes: description).
15. Add, modify, or remove a Taboo Subject (Supported attributes: name, description, Supported relations: vzRsDenyRule).
16. Add, modify, or remove a Filter , Filter entries.

For Fabric Access Policies, you can choose to add the following to your pre-change analysis job:

1. Add, modify, or remove relationship between Tenant to a physical domain.
2. Add, modify, or remove relationship between physical domain and a corresponding VLAN pool.
3. Add, modify, or remove relationship between physical domain and Attachable Entity Profile.
4. Add, modify, or remove a leaf interface profile.
5. Add, modify, or remove a host port selector.
6. Add, modify, or remove a switch profile.
7. Add, modify, or remove a switch selector.
8. Add, modify, or remove an interface policy group.
9. Add, modify, or remove an interface policy for CDP and LLDP.

Pre-Change Analysis Guidelines and Limitations

When using Pre-Change Analysis follow these guidelines and limitations:

- Pre-change Analysis can be conducted for online and offline assurance groups.
- You can identify a Pre-Change Analysis epoch by a blue banner displayed on top of the screen that says **Pre-Change Analysis** and the name of the analysis.
- More than one Pre-change Analysis can be run on the same base epoch.
- Pre-Change Analysis cannot be run for a pre-change epoch being used as a base epoch. When you are on pre-change epoch, the **Create New Pre-Change Analysis** option is disabled from the **Manage Pre-Change Analysis** screen.

- Only logical configuration smart events are modeled and run in a Pre-Change Analysis. Switch software and TCAM changes are not modeled. After the analysis completes, an Epoch Delta job will be automatically started to compare the Pre-Change Analysis epoch with the base epoch. Epoch Delta is performed only on checks supported in the Pre-Change Analysis job.
- During a pre-change analysis, certain smart events that exist in the base epoch will not be analyzed in the pre-change analysis. As a result, these smart events will not appear in the Pre-Change Analysis epoch even though the violation continues to exist. The reason that such an event is not analyzed in a pre-change analysis is because these smart events require not just logical data, but they also require switch software and TCAM data.
- Compliance Analysis displays the results of compliance checks in the Pre-Change Analysis epoch.
- Connectivity Analysis works on the data available in the Pre-Change Analysis epoch (minus some data such as learned prefixes which cannot be modeled).
- Events from a Pre-Change Analysis epoch are not included in searches across a time-range and event lifecycle scope. A local search within the Pre-Change Analysis epoch is supported when the user navigates to the Delta Analysis screen from a Pre-Change Analysis job and filters the Smart Events for the Pre-Change Analysis using the **Search** field on that screen.
- Global Search is disabled for Pre-Change Analysis epochs. In the Global Search timeline, Pre-Change Analysis epochs are not visible.
- Pre-Change Analysis does not support or analyze any service chain related changes or objects.
- The **Delta Analysis** tab does not allow a Pre-Change Analysis epoch to be selected.
- When you attempt to run a pre-change analysis, if there is already an epoch analysis running, a dialog box displays where you can stop the analysis that is running and start the new pre-change analysis. If you stop an epoch analysis that is running, you must manually restart it after your pre-change analysis job is complete. Alternatively, you can wait for the analysis that is currently running to complete, and then run the new pre-change analysis.
- If configuration data does not exist for a base epoch, and you run a pre-change analysis job using this epoch, new logical configuration files will not be generated. For such pre-change analysis jobs, the **Download** option will be grayed out/disabled under the **Settings** icon in the **Manage Pre-Change Analysis** table. You will not be able to download a new logical configuration.
- The Pre-Change Analysis could go into a **Failed** state if an imported configuration has unsupported objects. Figure out the Cisco ACI objects that are unsupported by referring to the **Manage Pre-Change Analysis Options** section, remove the unsupported objects, and import the configuration again before starting another Pre-Change Analysis job. If there is a failed Pre-Change Analysis, the error message for the failure is displayed in the **Manage Pre-Change Analysis** screen under **Analysis Status**.
- The Pre-change Analysis feature is supported in Cisco APIC release 3.2 or later. If you attempt to run a Pre-change Analysis with a Cisco APIC release earlier than release 3.2, an ERROR message indicates that **Pre-Change verification is supported on APIC 3.2 or higher**, and you cannot run the analysis.
- When you hover on the Pre-Change Analysis icon in the epoch timeline, the **Export Data** and the **Export Policy** options are not available for download. Smart Events severities are also not

displayed.

- Currently, when you click the **View Delta Analysis** option for a Pre-Change Analysis displayed in the **Manage Pre-Change Analysis** table, it navigates to the **Delta Analysis** screen of the Pre-Change Analysis epoch. When you navigate in this manner, the **Dashboard** tab, the **Policy CAM** tab, and the **Smart Events** tab will not be clickable or available for use. The **Manage Delta Analysis** submenu under the **Epoch Delta** tab is disabled. The **Explorer** tab, the **Change Management** tab, the **Delta Analysis** sub-menu in the **Epoch Delta** tab, and the **Compliance** tab are clickable and available for use.

Creating New Pre-Change Analysis

Use this procedure to create a new pre-change analysis.

Before You Begin

- At least one assurance group must be created.
- At least one base epoch must be created.

Procedure

1. In the Cisco NAE GUI, in the Timeline, choose the base epoch against which you want to create and run the pre-change analysis.
2. Choose **Change Management** > **Manage Pre-Change Analysis**.
3. In the **Create New Pre-Change Analysis** screen, perform the following actions:
   a. In the **Pre-Change Analysis Name** field, enter a name for the analysis. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description. (Optional step)
   c. In the **Base Epoch** field, ensure that the base epoch you chose earlier is displayed.
   d. In the **Change Definition** field, choose the desired radio button from **Import JSON file** and **Specify Changes Manually**.

   > ⓘ If you choose to upload a JSON file, you must upload the file that specifies the details of your changes, and your analysis will be performed based on the details. The JSON format must be the same as the Cisco APIC JSON format. If you choose to manually upload the file, then you must specify details in the **Changes** area as described below. Depending upon the object you choose, the attributes that are related will display, and you must choose the appropriate attributes.

4. In the **Changes** area, from the drop-down options, modify the current choices to reflect your proposed changes such as **Action**, **Object**, DN for the parent object and such.

   > ⓘ Based upon your choices, additional fields will be available for you to populate.

5. To add additional objects, click **Add Change**, and choose the attributes. In a single Pre-Change

Analysis job, you can specify multiple changes.

> Currently, a maximum of 100 object type changes are allowed.

6. Click **Save** or **Save & Run**.

You can use save to save the Pre-change Analysis job without having to start the analysis right away. You can return to the job later, edit the changes if required, and then run the analysis later.

When you save and run the job, the changes are applied to the selected base epoch, the analysis is performed, and results are generated. When the analysis is completed, the Pre-Change Analysis instance is listed in the **Manage Pre-Change Analysis** table.

The Pre-Change Analysis is also listed in the Timeline as an icon above the associated base epoch. When you hover over the base epoch, the pre-change analysis name that was run on that epoch is listed.

After you save and run a pre-change analysis, you cannot edit it. You can use the results or you can delete it. For additional details about editing or deleting pre-change analysis, see Update Setup in Pre-Change Analysis.

Clone Pre-Change Analysis

You can clone an existing Pre-Change Analysis, and modify it to create a new Pre-Change Analysis as follows:

> The clone option is disabled for Pre-Change Analysis jobs with changes imported from a file.

1. In the **Pre-Change Analysis Name** field, enter a new name. The name must be unique across all the assurance groups.
2. In the **Description** field, enter the description. (Optional step)
3. In the **Changes** area, from the drop-down options, modify the current choices to reflect your proposed changes such as **Action**, Object, DN for the parent object and such.

> Based upon your choices, additional fields will be available for you to populate.

4. Click the **Add Change** button to add additional changes.
5. Click **Save** or **Save & Run**.

You can use save to save the Pre-change Analysis job without having to start the analysis right away. You can return to the job later, edit the changes if required, and then run the analysis later.

When you save and run the job, the changes are applied to the selected base epoch, the analysis is performed, and results are generated. When the analysis is completed, the Pre-Change Analysis instance is listed in the **Manage Pre-Change Analysis** table.

The table in the **Manage Pre-Change Analysis** screen displays the details about your Pre-Change

Analysis and the **Analysis Status** column displays the stages of the running job such as **Submitted** and **Running**. After the job is completed, the status changes to display **Completed**.

Download Pre-Change Analysis

You can download an existing Pre-Change Analysis as follows:

- In the **Manage Pre-Change Analysis** table, click the **Settings** icon next to the appropriate pre-change analysis and click **Download**.
- The pre-change analysis downloads as an offline tar file with the pre-change analysis contents displayed in JSON format.

> In the downloaded file, you can view all the attributes which include attributes that are modified and those that are not modified. If desired, the downloaded file can be uploaded to your Cisco APIC.

- The option to download a Pre-Change Analysis is not available if **Use APIC Configuration Export Policy** was not enabled for the assurance group before the base epoch was generated.

Known Issues for Pre-Change Analysis

- When Pre-Change Analysis scale limits are exceeded, the analysis can fail with no error message.
- For Pre-Change Analysis jobs, you must not modify configurations where the total number of EPGs, BDs, VRFs are greater than 16,000.
- When creating a new Pre-Change Analysis, note the following:
  - Pre-Change Analysis is limited to handling configuration files of no more than 15MB. This applies to the currently configured tenant and endpoints, and if a JSON file upload is used, it applies to the uploaded JSON file.
  - If you upload a file with unsupported objects, Cisco NAE will remove the unsupported object and run the job.
  - When Pre-Change Analysis API users attempt to upload a JSON/XML file larger than 100MB, using a client, the API throws an error as follows: **502 Bad Gateway**. If the JSON/XML file size being uploaded is less than 100MB but greater than 15MB, then the API validates the file and throws a validation error as follows: **Uploaded file size exceeds the 15MB maximum limit**. When users access the Cisco NAE portal, and try to create a Pre-Change Analysis job with a file size greater than 15MB, the UI throws the following error: **File size cannot be larger than 15MB**. Therefore, files larger than 15MB are not supported in Pre-Change Analysis.
- A Pre-change Analysis job may fail or return incorrect results if the Cisco ACI configuration has features that are unsupported by Cisco NAE.
- Pre-change Analysis is not supported in Cisco ACI configurations that contain service chains.
- Cisco NAE performs a limited set of checks on the JSON file uploaded for pre-change analysis. Cisco ACI may reject this file.

- Pre-change Analysis may incorrectly report errors for attributes of subnets of external routed networks.
- Pre-change Analysis is supported in the following Cisco APIC releases:
    a. For 3.2(x) release, 3.2(9h) and earlier are supported
    b. For 4.0(x) release, 4.0(1h) and earlier are supported
    c. For 4.1(x) release, 4.1(2x) and earlier are supported
    d. For 4.2(x) release, 4.2(4o) and earlier are supported
    e. For 5.0(x) release, 5.0(2e) and earlier are supported

Explorer

About Explorer for ACI and NX-OS

The **Explorer** feature in NAE analyzes a policy snapshot from the Cisco APIC or a configuration snapshot from Cisco NX-OS to enable data center operators and architects to:

- Explore the ACI object models and associations or the NX-OS networking assets
- Verify connectivity and segmentation between network assets

The **Explorer** 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 **Explorer** feature allows operators to easily discover associations between traditional networking constructs such as VRFs, EPs, and VLANs to the ACI object model as well as with Cisco NX-OS.

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

> Currently, to explore NX-OS networking assets that are available through DCNM Assurance Group, only 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 ACI:

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

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

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

Example:

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

sport: *10*

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

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

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

Example: View interfaces on leaf *X*.

Use Cases

- **Design verification**: Ad-hoc query model enables operators to quickly understand and reason about their infrastructure. The natural language query model returns search results and associations in an easy to understand tabular format. In a single concise view, operators are able to answer design verification questions or discover deviations from organizational best practices.
- **Lightweight book-keeping**: Administration and maintenance teams can provide on demand visibility into the current state of their policy and networking infrastructure allowing inventory, book-keeping, and asset tracking procedures to be lightweight.

Use Case for ACI Only

Connectivity and Segmentation: Easily answer connectivity questions between a pair of assets or containers of assets. For example, if a group of EPGs needs to be quarantined, the **Can** query can quickly answer if policy has been correctly setup.

Workflow

> ℹ The **Workflow** section applies for ACI Assurance Group only.

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

It enables you to explore the connectivity between entities by creating a query. The Can query determines if the entities can communicate with each other and the health of the connectivity. The default Can query, *Can Any talk to Any* displays the entire EPG to EPG connectivity. The How query displays the configuration used for communication between the entities and the health of the connectivity.

Can Query Results

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

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

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

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

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

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

> Starting from Cisco NAE release 4.1(1), connectivity health is displayed in the radial view. When you upgrade from Cisco NAE release 4.0(1) to 4.1(1), the older epochs will not contain the connectivity health information.

How Query Results

The results of the How query are displayed in the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** table. The connectivity can be healthy or unhealthy. If the connectivity is healthy, using the **Connectivity Table** you can determine the health of the connectivity. If the connectivity is unhealthy, you can use the **Policy**, **Forwarding**, and **Endpoint** tabs to determine the possible cause. The possible causes for unhealthy connectivity include security violations, forwarding violations, and endpoint point violations.

The color of the flow between the EPG pair indicates the maximum severity of smart events across the **Policy**, **Forwarding**, and **Endpoints** tab. The color of the icon in each tab indicates the individual severity of the smart events included in the corresponding tab.

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

The color of the icon in each tab will help you identify if the issues related to security violations, forwarding violations, and endpoint point violations.

For example if the issues are related to security violations, you can use the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** to determine the smart events associated with the security issue. In the **Prefix Table**, you can click **Subnet/Route** to see information regarding the prefixes. In the **Forwarding Smart Events** table you can click the smart event to determine the objects in your fabric that are affected by the issue, the Passing or Failing checks performed on the smart event and suggested steps to resolve the issue.

Guidelines and Limitations

- In the **Explorer** page, only four active epochs for exploring across all Assurance Groups is supported. The epochs can be used for exploration by either the same user or by multiple users. To explore additional epochs, you must offload an existing epoch before exploring. In the **Offload Epoch From Explorer** page you can select the epoch to offload.
- The Explorer feature is supported only for IPv4 prefixes.
- All queries created using the Explorer 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 **Explorer** and contact Cisco TAC to resolve the issue.
    a. Choose **Settings** > **Download Tech Support Logs** to download the tech support logs.
    b. On VM-3, navigate to */hadoop/log/* directory to locate the logs for explorer. If there are multiple explorer instances running, the logs for each instance is located in a separate directory.

```
explorerService-1/explorer.log
explorerService-2/explorer.log
explorerService-3/explorer.log
explorerService-4/explorer.log
connectivityAnalysisService/connectivityAnalysisService.log
```

Guidelines and Limitations for ACI

- Prefixes configured under L3extSubnet without their learnt route will not be listed as part of the auto-suggestions when you enter a query in the Search bar.
- To explore the APIC resources successfully using the Explorer feature, the APIC policy must contain either valid endpoints such as fv:CEp or valid EPGs.
- In the **Explorer** page, policy (contracts) and forwarding (subnets and learnt routes) are used to determine the connectivity analysis. In the **Compliance** page, the policy intent based on contracts is used to determine the compliance.

Guidelines and Limitations for NX-OS

- With the earlier Cisco NAE release 5.0(1), for NX-OS fabric assurance, the **Explorer** feature provided a switch-wide view of VRFs, VLANs, interfaces, endpoints and leaf switch resources in the fabric. Starting with Cisco NAE release 5.1(0), for NX-OS fabric assurance, Layer 2 VNI and Layer 3 VNI are added as resources.
- Starting with Cisco NAE release 5.1(0), 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 Explorer.
- When a VRF is not operational, Explorer 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 Explorer if you do not see endpoints or other network assets, look for system events in the associated epoch. 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 assurance with DCNM Assurance Group, only IPv4 endpoints support in Explorer is available. IPv6 endpoints support in Explorer is currently not available.

Creating a What Query

Use this procedure to create a What query using the Explorer feature.

> This procedure is supported in ACI and NX-OS.

Procedure

1. Choose **Explorer**.
2. In the **Timeline** select an epoch for analysis. When you select an epoch, the data to explore is loaded on demand.

   > You can only select an epoch created in release 4.0(1) and later to create a query.

3. Perform the following steps for a What query.
   a. On the **Search** bar, 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.
   b. For a What query, the results are displayed in the results table. The results table is only available for a What query.
   c. Click an entity in the **Query Results** table to view details. Click the number on the results table to view details about the entity in the ACI policy or the NX-OS networking assets.

Creating a Can Query

Use this procedure to create a query using the Explorer feature.

> This procedure is supported in ACI only.

Procedure

1. Choose **Explorer**.
2. In the **Timeline** select an epoch for analysis. When you select an epoch, the data to explore is loaded on demand.

   > You can only select an epoch created in release 4.0(1) and later to create a query.

3. Perform the following steps for a What or Can query.
   a. On the **Search** bar, enter a What or Can query. The query must include two groups of one or more entities from the ACI policy. See Supported Queries. By default, the Any to Any query view is displayed.
   b. For a What query, the results are displayed in the results table. The results table is only available for a What query. Click the entity on the results table to view the DN information. Click the number on the results table to view details about the entity in the ACI policy.
      i. Click **Source** and select one or more entities from the results table.

        ii. Click **Destination** and select one or more entities from the results table.

        iii. Click **Can they talk** to determine if the two entities can communicate with each other.

        iv. (Optional) Click **Reverse Query** to reverse the source and destination entities for a query.

    c. For a Can Query, the results are displayed in the **Which Entities Can Talk** Area.

        i. If the query results are large, the message “The query returned too much data to display” is displayed. Select a single resource from the **Would you like to check connectivity of a single resource** drop-down list to create a specific query.

        ii. (Optional) Click **Reverse Query** to reverse the source and destination entities for a query.

    d. In the **Which entities can talk** area, click **EPG** tab to view the the communication between the EPGs. The EPG view displays connectivity information between different EPGs as configured in the APIC policy. Click **Prefix** tab to view the the communication between the prefixes. The prefix view displays connectivity information between prefixes as configured in the APIC policy or learnt prefixes. In the radial view, the colors of the arced lines correspond to the severity of the smart events. See Workflow for information on the radial view visualization.

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

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

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

e. In the **Which entities can talk** area, click **Objects** tab to view the associations between the different objects such as tenants and VRFs. In the radial view, the colors of the arced lines correspond to the severity of the smart events. See Workflow for information on the radial view visualization.

f. In the **Which entities can talk** area, click **Both** tab to view the health of the connectivity. In the radial view, the colors of the arced lines correspond to the severity of the smart events. See Workflow for information on the radial view visualization.

g. Select the arc connecting the two entities and click **How do they talk** to view the the communication details.

h. See Viewing Can or How Query Results. for information about query results.

4. Perform the following steps for a View query.

    a. On the **Search** bar, enter a View query. The query must include two groups of one or more entities from the ACI policy. See Supported Queries.

b. The results of the table are displayed in the **Physical Interfaces** page. See Viewing View Query Results, for information about query results.

Viewing Can or How Query Results

> ℹ This procedure is supported in ACI only.

The **How do they talk** page displays the communication details between the entities from the ACI policy.

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

- Red Color indicates critical smart events
- Orange color indicates major smart events
- Yellow color indicates minor smart events
- Green color indicates warning and info events
- The **Policy** tab enables you to explore the security policy issues based on the query.
- The **Forwarding** tab enables you explore a prefix or pair of prefixes issues based on the query.
- The **Endpoints** tab to explore the endpoint issues based on the query.

Procedure

1. Click **Policy** to view the information regarding the health of the contracts between the EPG pairs. The **Policy** health information is displayed in the **Connectivity Table**, **Security Flow Table**, and **Security Smart Events** table.
   a. The **Connectivity Table** displays the connectivity details between the EPGs and prefixes.
   b. The **Security Flow Table** displays the communication details between the EPGs.
   c. The **Security Smart Events** table displays the security smart events based on the query.
2. Click **Forwarding** to view the the information regarding the health of the subnets between the EPG pairs. The **Forwarding** health information is displayed in the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** table.
   a. The **Connectivity Table** displays displays the connectivity details between the EPGs and prefixes.
   b. The **Prefix Table** displays detailed connectivity information about all the routes in the assurance group. This information shows which prefixes may communicate successfully, and which prefixes may have communication issues.
   c. The **Forwarding Smart Events** table displays the forwarding smart events based on the query.
3. Click **Endpoints** to view the the information regarding the health of the endpoints between the EPG pairs. The **Endpoints** health information is displayed in the **Connectivity Table**, **Tenant Endpoints Details**, table and **Endpoints Smart Events** table.

   a. The **Connectivity Table** displays displays the connectivity details between the EPGs and prefixes.

   b. The **Tenant Endpoints Details** table displays information about diagnosing endpoint learning errors for the fabric in the assurance group.

   c. The **Endpoints Smart Events** displays the endpoint smart events based on the query.

Viewing View Query Results

> This procedure is supported in ACI only.

Physical Interfaces page displays the physical interface health and provides the visual indication of the interface status for any leaf switch in the assurance group based on the query.

> The **Physical Interface View** area displays information about one leaf switch at a time.

Procedure

1. If an endpoint is attached to a particular interface, an image of the leaf switch is displayed as a two-dimensional image. The switch ports are color coded to display the status for each port. The color for each port matches its smart event severity by color.
2. Hover over the **i** icon located above the leaf switch image to view the legend for the status icons.
3. Click one of the switch ports in the switch image, to view the details of the smart event associated with that port, in the **Forwarding Smart Events** table.
4. For additional filtering, check or uncheck the tabs in the **View Control** area. View controls assist with fast navigation to the interfaces that are under your scrutiny.

   a. Under **Interface Usage**, the interfaces are classified into three types based upon intent.

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

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

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

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

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

Supported Queries for ACI

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

Supported What Queries

Table 3. Supported What Queries

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

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

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

Supported Can Queries

Table 4. Supported Can Queries

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

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

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

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

Table 5. Supported View Queries

Query	Entity
View interfaces on	Leaf `leaf_name`

Supported Queries for NX-OS

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

Supported What Queries

Table 6. 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

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

Query	Entity	Operator	Entity
What L2VNIs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI
What L3VNIs are associated with	• ? • Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI	• And • Or	• Any • EP • INF • LEAF • VLAN • VRF • L2VNI • L3VNI

About Explorer for MSO

The **Explorer** feature in Cisco NAE allows network operators to discover assets and their object associations in an easy-to-consume natural language query format. Explorer for MSO currently supports a **Can EPG talk to EPG** query where the query must include two groups of one or more entities from MSO policy to check their connectivity. Explorer for MSO enables you to navigate associations between EPGs, explore EPG to EPG communication, and enable visibility and troubleshooting across sites.

Examples:

- Can EPG_1_ talk to EPG_2_.
- Can any talk to any

Currently, only **Can** EPG to EPG queries are supported for MSO Explorer. **What** and **View** queries are not supported. For **Can** EPG to EPG queries, additional filtering based on protocols and port is not supported.

Examples:

- This is an example of a query that is supported: Can EPG: uni/tn-secure/ap-AP0/epg-B talk to EPG: uni/tn-secure/ap-AP0/epg-A
- This is an example of a query is **not** supported: Can EPG: uni/tn-secure/ap-AP0/epg-B talk to EPG: uni/tn-secure/ap-AP0/epg-A on tcp dport: 80

A user can choose from the auto-suggested query-list of all EPGs managed by the MSO Assurance Group. **Can** query results are available as aggregated for the MSO Assurance Group and not per ACI site. All queries in an MSO Assurance Group for Explorer are across-site queries, and the Maximum severity is max severity across all sites for assets and associations. For EPG severity, in addition to events considered in the ACI Explorer, `MSO_NAME_SPACE_NORMALIZATION_FAILED_FOR_EPG` is also considered. If this event exists, it will appear in the endpoint events table. `MSO_NAME_SPACE_NORMALIZATION_FAILED_FOR_EPG` and corresponding INFO events are supported only for Application EPGs.

Click the **How do they talk?** link, for more detail and to see the site-specific views.

Notes Related to Explorer for MSO

- When you click the **How do they talk?** link, the screen displays certain tabs and tables. When viewing the **Connectivity Table** and the **Security Flow Table**, in the **Source EPG** and **Destination EPG** columns a **shadow** tag to an EPG will be displayed if the EPG is a shadow in the corresponding site. For example, <epgname>(shadow). If an EPG is not a shadow, there will be no shadow tag after the EPG name. However, if you have a version of APIC/MSO that does not have the shadow annotation, the shadow tag will not display even for shadow EPGs.
- In the **Endpoints Smart Events Table**, **Forwarding Smart Events**, and the **Security Smart Events** tables, under the **Individual** tab, you can click a Site for specific Smart Event details and lifecycle information.
- The **Security Flow Table** and the **Connectivity Table** have a **Site** column. The **Prefix Table**

and the **Tenant Endpoint Table** have a **Sites** column that you can click for more information.

Creating a Can Query in MSO Only

Use this procedure to create a query using the Explorer feature in MSO.

Procedure

1. Choose **Explorer**.
2. In the **Timeline** select an MSO epoch for analysis. When you select an epoch, the data to explore is loaded on demand.
3. Perform the following steps for a Can query.
4. In the **Search** bar, enter a Can query. The query must include two groups of one or more supported entities. By default, the Any to Any query view is displayed.

> For a Can Query, the results are displayed in a radial in the **Which Entities Can Talk** Area. If the query results are large, the message “The query returned too much data to display” is displayed. Select a single resource from the **Would you like to check connectivity of a single resource** drop-down list to create a specific query.

5. (Optional) Click **Reverse Query** to reverse the source and destination entities for a query.
6. In the **Which entities can talk** area, click **EPG** tab to view the the communication between the EPGs. The EPG view displays connectivity information between different EPGs.
7. Click the **Prefix** tab to view the communication between the prefixes. The prefix view displays connectivity information between configured or learned prefixes. In the radial view, the colors of the arced lines correspond to the severity of the smart events.
8. Click the **How do they talk?** link, to see the color of the arc between the EPGs as the Maximum severity of the **Policy**, **Forwarding** and **Endpoints** tabs.

Use Cases For MSO

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

Workflow for MSO Assurance Group

> The **Workflow** section applies for MSO Assurance Group only.

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

It enables you to explore the connectivity between entities by creating a query. The Can query determines if the entities can communicate with each other and the health of the connectivity. The default Can query,`Can Any talk to Any` displays the entire EPG to EPG connectivity. The How query displays the configuration used for communication between the entities and the health of the connectivity.

Can Any (EPG) to Any (EPG) Query Results

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

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

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

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

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

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

Starting from Cisco NAE release 4.1(1), connectivity health is displayed in the radial view. When you upgrade from Cisco NAE release 4.0(1) to 4.1(1), the older epochs will not contain the connectivity health information.

How Query Results

The results of the How query are displayed in the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** table. The connectivity can be healthy or unhealthy. If the connectivity is healthy, using the **Connectivity Table** you can determine the health of the connectivity per site. If the connectivity is unhealthy, you can use the **Policy**, **Forwarding**, and **Endpoint** tabs to determine the possible cause. The possible causes for unhealthy connectivity include security violations, forwarding violations, and endpoint point violations.

The color of the flow between the EPG pair indicates the maximum severity of smart events across the **Policy**, **Forwarding**, and **Endpoints** tab. The color of the icon in each tab indicates the individual severity of the smart events included in the corresponding tab.

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

The color of the icon in each tab will help you identify if the issues related to security violations, forwarding violations, and endpoint point violations.

For example if the issues are related to security violations, you can use the **Connectivity Table**, **Prefix Table**, and **Forwarding Smart Events** to determine the smart events associated with the security issue on each site. In the **Prefix Table**, you can click **Sites** for information about the prefixes. In the **Forwarding Smart Events** table you can click in the **Sites** column to determine the objects in your fabric that are affected by the issue.

Supported Queries for MSO

The following table lists the queries supported by the **Explorer** feature for MSO.

Supported Can Queries

Table 7. Supported Can Queries

Query	Entity	Operator	Protocol	Destination Port	Source Port
Can EPG `epg_name` talk to	EPG	—	—	—	—
Can ANY talk to	• EPG • ANY	—	—	—	—

The **Operator Protocol**, **Destination Port** and **Source Port** are not supported.

Epoch Delta Analysis

Epoch Delta Analysis

Cisco NAE performs analysis of an Assurance Group at regular intervals called an epoch, and the epoch data is collected in 15-minute intervals.

> Cisco NAE support for Policy Delta with NX-OS switches and DCNM Assurance Group is a Beta feature. Currently, Cisco NAE does not support Epoch Delta Analysis for MSO.

At each epoch, Cisco NAE captures a snapshot of the controller policies and the fabric run time state, performs analysis, and generates smart events. The smart events generated describe the health of the network at that epoch.

Epoch delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two epochs. Epoch delta analysis consists of the following components:

- **Analysis Management**: Enables you to create a new delta analysis and manage existing analysis. See Creating Epoch Delta Analysis.
- **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 epochs. The results are displayed in the following areas:

- **Smart Event Count**: Displays the difference in smart event count per severity across the two epochs.
- **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.
- **All Smart Events**: The **Aggregated** view displays the delta status for each smart event name across the two epochs. The **Individual** view displays the delta status for each smart event across the two epochs and also the failing conditions for the event.

Policy Delta

Policy Delta for ACI

Policy Delta analyzes the differences in the policy between the two epochs 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 epochs.

- View the added, modified, and deleted policy configurations between the two epochs.
- Export the policy configuration for the earlier epoch policy and later epoch 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 epochs.

Policy Delta for DCNM

Policy Delta for DCNM Assurance Group analyzes the changed nodes or switches across two epochs 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 epochs.
- View the context around the modified areas in the policy delta.

To view the policy delta between the two epochs, you must configure the collection settings for an Assurance Group. See Performing Online Analysis.

Guidelines and Limitations

The following general guidelines are applicable to Epoch Delta Analysis:

While you are currently allowed to create more than one Epoch 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 assurance group analysis. The interdependency arises because the Epoch 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.

Guidelines and Limitations for ACI Assurance Group

> ℹ When you are viewing a Pre-Change Analysis epoch delta in the Delta Analysis tab page, you can identify it by a blue banner displayed on top of the screen that says Pre-Change Analysis and the name of the analysis.

The following guidelines and limitations are applicable for policy delta:

- The **APIC Configuration Export Policy** must be configured. See Performing Online Analysis.
- The **APIC Configuration Export Policy** must be of the same format (XML/JSON) for both the epochs.
- The policy delta will not be performed if there are any APIC configuration export policy collection errors.

Guidelines and Limitations for DCNM Assurance Group

- When you choose a switch in the **Changed Nodes** area, in the **Policy Delta** screen, the difference in the configuration between the two epochs is displayed.
- For Policy Delta, **Audit Logs** and **Search in Policy Viewer** are not currently supported.

Creating Epoch Delta Analysis

Use this procedure to create an epoch delta analysis.

Before You Begin

- You have configured the collection settings for an Assurance Group. See Performing Online Analysis.
- For ACI Assurance Group users, APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure the **APIC Configuration Export Policy**.

Procedure

1. Choose **Epoch Delta** > **Manage Delta Analysis**.
2. Click **Create New Delta Analysis**.
3. Complete the following fields for **Create New Delta Analysis**.
   a. In the **Name** field, enter the name. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description.
   c. From the **Earlier Epoch** drop-down list, choose the first epoch for the delta analysis. You can also use the timeline to select an earlier epoch. See Timeline for more information.
   d. From the **Later Epoch** drop-down list, choose the second epoch for the delta analysis. You can also use the timeline to select a later epoch.

> The two epochs selected for the delta analysis must belong to the same Assurance Group.

4. Click **Run**.
5. The status of the delta analysis is displayed in the **Delta Analysis** table. Cisco NAE performs 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. See Managing Epoch Delta Analysis.
6. To view the results of the delta analysis, select a delta analysis from the **Delta Analysis** table. From the Actions menu, choose **View Results**. See Viewing Delta Analysis Results.

Viewing Delta Analysis Results

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

- 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.

Viewing Health Delta Analysis

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

Procedure

1. Choose **Epoch Delta** > **Delta Analysis**.
2. Click **Health Delta** to view the results of the health of the fabric.
    a. **The Smart Event Count** displays the difference in the smart event count per severity across the two epochs. The first count represents the smart events found only in the earlier epoch. The second count represents the smart events common in both the epochs. The third count represents the smart events found only in the later epoch.
        i. Click the smart event count to view the smart event details.
    b. The **Health Delta By Resources** displays the health delta across various resource types. It also displays the count of the resources with issues, without issues, and the total resources.
        i. Click the resource count to view the resources associated with the resource count.
        ii. Hover on the resource name to view the resource DN.
        iii. Click the resource name to view the smart event details for that resource.
    c. In the **Search** bar use the multiple filters to search for smart events.
        i. Click **Add Filters** to filter by resources and then by resource name or DN.
        ii. Click the ◐ icon to filter by the epochs used for the delta analysis.
    d. The **All Smart Events** table displays the aggregated and individual view of the smart event delta.
        i. Click **Aggregated** to view the delta status for each smart event name across the two epochs. The **Count** column displays the consolidated number of events across the two epochs.
        ii. Click **Individual** to view displays the delta status for each smart event across both the epochs and also the failing conditions for the event. Click **Event Name** to view the smart event details.

Viewing Policy Delta Analysis for ACI

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

Procedure

1. Choose **Epoch Delta** > **Delta Analysis**.
2. Click **Policy Delta** to view the results of the policy changes across the two epochs. Policy Delta includes 3 panels, Changed Policy Object, Policy Viewer, and Audit Log.

3. The **Changed Policy Object** panel, displays the changed policy object tree across the two epochs.

    a. Drill down on a particular object to view the object types that have changed. The number indicates the number of changes to the object.

    b. Select the changed object type to view the smart events that have changed.

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

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

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

4. The **Policy Viewer** panel displays the policy configuration across the earlier and later epochs. The policy configuration for the earlier epoch is called the earlier epoch policy. The policy configuration for the later epoch is called the later epoch policy.

    a. Use the color coding to visualize the added, deleted, modified, and unchanged content across the two policies. Click the ⓘ icon for information about the color coding.

    b. The ◐ icon lists the line numbers for the content in the earlier epoch policy. The ◑ icon lists the line numbers for the content in the later epoch policy.

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

    d. Click the ⤓ icon to export the earlier epoch policy or to export the later epoch policy.

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

        i. Select **ALL** to search across all the content in the earlier epoch policy and later epoch policy.

        ii. Select **Changed** to search across the changed content in the earlier epoch policy and later epoch policy.

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

    a. In the audit log panel, green color indicates the audit log attributes such as VLAN that have been added. Red color indicates the audit log attributes that have been deleted. Yellow color indicates the audit log attributes that have been modified.

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

    c. Hover on an audit log entry to view when the changes were made and who made the changes. The timestamp on the audit log entry corresponds to the the timestamp on the APIC audit log.

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

Viewing Policy Delta Analysis for DCNM

Use this procedure to view the results of the policy delta analysis for the DCNM Assurance Group.

Procedure

1. Click **Policy Delta** to view the results of the policy changes across the two epochs. Policy Delta includes 2 panels for a DCNM Assurance Group, Changed Nodes and <*Switch Name*> Policy Viewer.
2. The **Changed Nodes** panel, displays the changed nodes or switches across the two epochs.
3. Click **Show Changes** to view the changes in the <***Switch Name***> **Policy Viewer** panel.
4. The <***Switch Name***> **Policy Viewer** panel displays the configuration across the earlier and later epochs. The switch configuration for the earlier epoch is called the earlier epoch policy. The switch configuration for the later epoch is called the later epoch policy.
    a. Use the color coding to visualize the added, deleted, modified, and unchanged content across the two epochs. Click the ⓘ icon for information about the color coding.
    b. The ●○ icon lists the line numbers for the content in the earlier epoch policy. The ○● icon lists the line numbers for the content in the later epoch policy.
    c. Click **Show More Above** or **Show More Below** to display more content.
    d. Click the ⤓ icon to export the earlier epoch or to export the later epoch.

Compliance Analysis

Compliance Analysis Tab

> Currently, this is supported for ACI Assurance Group only.

Every epoch verifies compliance analysis results. In each epoch, one event for every requirement that is analyzed is raised. For example, if an assurance group runs a compliance analysis on an epoch every 15 minutes, and there are two requirements associated with the epoch, two smart events will be raised.

When an epoch runs for a specific assurance group, all the active requirement sets that are associated with that assurance group are verified and validated.

> To be included as an active requirement set, you must associate your compliance requirement to the assurance group and activate the compliance requirement.

Manage Compliance

Manage Compliance Tab

> ℹ Currently, this is supported for ACI Assurance Group only.

The **Manage Compliance** tab enables the user to verify Segmentation Compliance and Service Level Agreement (SLA) compliance, traffic restriction compliance, and configuration compliance. Compliance can be used to set up regulatory compliance rules. With segmentation compliance, the user can establish walled areas around a set of entities that must not communicate with other entities. SLA compliance can also set up rules for entities that must talk with other entities. Traffic restriction compliance requirements allow the user to specify restrictions on protocols and ports for communication between objects.

In the NAE UI, the user specifies their compliance requirements. The NAE appliance, verifies in the subsequent epochs, whether the compliance requirements are satisfied by the policy that is configured on Cisco APIC. If satisfied, an event is raised stating that the compliance requirement is satisfied. One event per requirement per epoch is raised. For example, if an assurance group runs a compliance analysis on an epoch every 15 minutes, and there are two requirements associated with the epoch, two smart events will be raised.

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

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

Creating Object Selector

Use this procedure to create an Object Selector.

Before You Begin

At least one assurance group must be created.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Object Selectors**.
2. Click **Create New Object Selector**.
3. In the **Create New Object Selector** dialog box, **Object Selector Name** field, enter the name. The name must be unique across all the assurance groups.
4. In the **Description** field, enter the description. (Optional step)
5. In the **Object Selector Type** field, from the drop-down options, choose the appropriate object type. See the guidelines at the end of this section for guidelines about Object Selector Type and EPG selector.
6. In the Included and Excluded Object fields, from the drop-down options, choose the relevant objects.

   > You may use multiple match criteria, and the included objects will be a union and intersection of the criteria that you choose.

7. Click the **Preview** hyperlink to view objects selected by the new object selector. The objects displayed are based upon objects configured in the APIC in the last epoch. See the guidelines at the end of this section for guidelines about previewing objects.
8. Click **Save**. Your Object Selectors are created. The list of object selectors is displayed under the **Object Selectors** tab.

For additional details about editing or deleting object selectors, see Managing Object Selectors.

Guidelines When Creating Object Selectors

- Based on your object selector type (for example EPG, VRF, BD, Tenant, Contract, Filter, Subject), the relevant container object types are displayed. For example, EPGs can be selected directly or they can be based on the Tenant, VRF, BD, or App Profile to which they belong. Starting with Cisco NAE release 5.0(1), Tenant selectors are an Object Selector type supported in Segmentation requirements. Starting with Cisco NAE release 5.1(1), Contract, Filter, and Subject selectors are additional Object Selector types supported and Cisco NAE verifies if the name or a string in the name for contracts, subjects, or filters that are defined in Cisco APIC are compliant with the naming rules.
- If you had EPG selectors chosen in an earlier release of Cisco NAE, after the upgrade to Cisco NAE release 4.0(1), the EPG selectors will automatically display in the current Object Selector table and they will be associated with the EPG Selector type.
- When creating the new object selector, you can preview the objects that are included or excluded in the object selector before you save the newly created object selector with your selections. You can also filter the list by the object Distinguished Name/Name. If the preview list requires further modifications or filtering, close the preview dialog box and tweak your selections for included and excluded objects based upon your preference. Then preview the list once again. After you are satisfied with the preview list, close the dialog box.

Creating Traffic Selector

Use this procedure to create a traffic selector.

> You must configure the Traffic Selectors before configuring the Compliance Requirement and the Compliance Requirement Sets (in that order of sequence).

Before You Begin

- At least one assurance group must be created.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Traffic Selectors**.
2. Click **Create New Traffic Selector**.
3. Complete the following fields for **Create New Traffic Selector**.
    a. In the **Traffic Selector Name** field, enter the name. The name must be unique across all the analyses.
    b. In the **Description** field, enter the description. (Optional step)
    c. In the **Talk On** area, from the **EtherType** field drop-down options, choose the appropriate EtherType.

> Certain **EtherType** choices will require you to make additional choices from drop-down lists that appear based upon your selections.

4. To add additional EtherType options, click **Add On**, and choose additional EtherType options.
5. Click **Save**.

Your traffic selectors are created. The list of traffic selectors is displayed under the **Traffic Selectors** tab.

For additional details about editing or deleting traffic selectors, see Managing Traffic Selectors.

Creating Compliance Requirement

Use this procedure to create a compliance requirement.

Before You Begin

- At least one assurance group must be created.
- Your object selectors are created.
- Your traffic selectors are created.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Compliance Requirements**.
2. Click **Create New Compliance Requirement**.
3. Complete the following fields for **Create New Compliance Requirement**.
    a. In the **Compliance Requirement Name** field, enter the name. The name must be unique across all the analyses.

    b. In the **Description** field, enter the description. (Optional step)
4. In the **Compliance Type** area, perform the appropriate steps to specify the requirements depending on your preference.
    a. If you choose **Segmentation** perform the following steps:

        i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.

        ii. Choose the appropriate communication operator if available (**Must Not talk to** is chosen by default).

        iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.

> The Segmentation requirements occur between the EPGs that are in the Tenant Selector. Mixing EPG and Tenant selectors in a Segmentation requirement is not supported.

> If you use Tenant Selectors, you can decide to enable the aggregate event for tenants. If it is enabled, Cisco NAE will no longer raise info events for segmented EPG pairs. Instead, one event per segmented tenant will be raised. Enabling this event has scale implications. See the **Verified Scalability** section in the **Cisco NAE Installation and Upgrade Guide** for details.

b. If you choose **SLA** perform the following steps:

  i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.

  ii. Choose the appropriate communication operator if available (**Must Not talk to** is chosen by default).

  iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.

  iv. Click **Select Traffic Selector name** and choose a traffic selector name.

c. If you choose **Traffic Restriction** perform the following steps:

  i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.

  ii. Choose the appropriate communication operator if available (**Must Not talk to** is chosen by default).

ℹ When you choose the value **Must Not Talk To**, Cisco NAE verifies that the EPGs do not communicate with the specified protocol in the traffic selector field. When you choose the value **May Talk To**, Cisco NAE verifies that the EPGs cannot communicate on protocols other than the protocol specified in the traffic selector field.

iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.

iv. Click **Select Traffic Selector name** and choose a traffic selector name.

d. If you choose **Configuration** perform the following steps:

   i. Click **Enter Object Selector name** and choose an object selector name from the list.

   ii. The communication operator (for example **Must Have**) is displayed.

   iii. Click **Enter Attribute**, and choose the desired attribute from the list.

   iv. Choose the appropriate operator from **Equal to** or **Not Equal to**.

   v. Click **Enter Attribute Value**, and choose the desired attribute value from the list.

ℹ As part of object selectors for Configuration Compliance Type, BD, VRF, and EPG are supported. You can select more than one attribute in one configuration compliance requirement.

e. If you choose **Naming** perform the following steps:

   i. Click **Enter Object Selector name** and choose an object selector name from the list.

   ii. The operator (for example **Must Have**) is displayed.

   iii. Click **Enter Attribute**, and choose the desired attribute from the list.

   iv. Choose the appropriate operator. The syntax of regular expressions/operators used for naming are as follows:

a. Matches Regular Expression”, “

b. Contains”, “

c. Begins With”, “

d. Ends With”, “

e. Matches Exactly”, “

f. Does Not Contain”, “

g. Does Not Begin With”, “

h. Does Not End With”,

ℹ For further details about regular expressions and operators, search the internet for **Oracle Java Tutorials Regex character classes**.

v. Click **Enter Attribute Value**, and choose the desired attribute value from the list.

5. Click **Save**.

You have created a compliance requirement. For additional details about editing or deleting compliance requirements, see Managing Compliance Requirements.

For details about creating a configuration compliance containment check, see Configuration Compliance Containment Check.

For details about creating a BD to EPG relationship configuration compliance check, see BD to EPG Relationship Configuration Compliance.

Creating Compliance Requirement Set

Use this procedure to create a compliance requirement set.

Before You Begin

- At least one epoch analysis has been completed.
- Your object selectors and requirements are created.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Compliance Requirement Sets**.
2. Click **Create New Compliance Requirement Set**.
3. Complete the following fields for **Create New Compliance Requirement Set**.

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

    b. In the **Description** field, enter the description. (Optional step).

    c. In the **Associate to current Assurance Group** field, check the checkbox.

    > ℹ You can only associate with the current assurance group.

d. In the **Activate this Compliance Requirement Set** field, check the checkbox if you want to activate the requirement set.

> ℹ When an epoch runs for a specific assurance group, all the active requirement sets that are associated with that assurance group are verified and validated.

e. In the **Associated Requirements** area, click the **Associate** link to choose the requirements that you want to associate from the **Associate Requirements** table.

> ℹ Similarly, you can disassociate requirements by clicking the **Disassociate** link.

f. Click **Save**.

You have created a compliance requirement set. For additional details about editing or deleting compliance requirement sets, see Managing Compliance Requirement Sets.

Configuration Compliance Containment Check

Use this procedure to perform a configuration compliance containment check.

Starting with Cisco NAE release 5.0(1), you can perform a configuration compliance containment check against a specified configuration. You specify a configuration file or epoch, and Cisco NAE continuously checks against it and enables you to identify changes for the objects and configurable attributes defined in Cisco APIC. If the configuration deviates from the specified configuration, then compliance violations are raised. For every violation there will be a separate violation Smart Event displayed. Additionally, a single Smart Event will be raised that includes every variable for every object of the Tenant that is not a violation.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Compliance Requirements**.
2. Click **Create New Compliance Requirement**.
3. Complete the following fields for **Create New Compliance Requirement**.
   a. In the **Compliance Requirement Name** field, enter the name. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description. (Optional step)
   c. In the **Compliance Type** field, choose **Configuration**.
   d. In the **Base Configuration Settings** field, choose the appropriate option to specify your configuration compliance containment epoch or file. You can choose a base epoch, or import a JSON/XML configuration file, or enter the configuration settings manually.
   e. In the **Allow addition of new configuration objects** field, check the checkbox if appropriate. See the guidelines below for details about the behavior resulting from your selection in the **Allow addition of new configuration objects** field.
   f. If displayed, click the **Browse** button to browse and upload the golden configuration file.
4. Click **Save**.

Cisco NAE starts performing a containment check.

Guidelines and Limitations for Configuration Compliance Containment Check

- In the **Allow addition of new configuration objects** field, if you check the checkbox, no violation event will be raised for a new object that is missing in Cisco APIC. By default, the checkbox is not checked which enables Cisco NAE to perform bidirectional inspection to verify if the base epoch is contained in the current epoch and if the current epoch is contained in the base epoch. As a result, if an object is added or deleted in Cisco APIC, a violation event will be raised. If you had checked **Enabled equivalence check** in an earlier Cisco NAE release, and then you upgraded to release 5.1(1), the **Allow addition of new configuration objects** field checkbox will be automatically unchecked. Similarly, if you had unchecked **Enabled**

equivalence check in an earlier Cisco NAE release, and then you upgraded to release 5.1(1), the **Allow addition of new configuration objects** field checkbox will be automatically checked.

- If a user creates a Configuration Compliance Containment Check requirement and runs a Pre-Change Analysis job for that assurance group, Cisco NAE will not verify the Configuration Compliance Containment Check compliance requirement in the Pre-Change Analysis job. All other requirements such as SLA and segmentation are verified.
- In order to define a Configuration Compliance Containment Check with a base epoch, during the creation of that epoch, the **Use APIC Configuration Export Policy** must be checked, otherwise the user sees an error message stating that the base epoch does not have a policy configuration exported. If the **Use APIC Configuration Export Policy** is not checked and the analysis is started, a **COMPLIANCE_NOT_VERIFIED** event will be raised, describing what actions must be performed in order to run the analysis. To locate the checkbox for **Use APIC Configuration Export Policy**, navigate to **Settings** > **Assurance Group**, choose the desired ACI Assurance Group, and click **Edit** to view the **Collection Settings** area.
- If there is a backup job running in Cisco APIC, the analysis will raise a **CONFIGURATION_COMPLIANCE_NOT_VERIFIED** smart event. This is because the policy configuration file cannot be exported during that time and as a consequence, the actual comparison cannot be performed.
- The **status** attribute is not supported for any object type. XML or JSON files with this attribute cannot be uploaded to Cisco NAE.

BD to EPG Relationship Configuration Compliance

Use this procedure to configure a BD to EPG relationship compliance check.

Starting with Cisco NAE release 5.1(1), you can specify a BD selector to have a fixed number of EPGs. You can create a BD configuration compliance rule to set the maximum number of EPGs with which the BD can be associated.

When the requirement set is not satisfied a violation event will be raised. If the requirement is satisfied, it will raise an enforcement event. Only when the BD selector is not resolved, a warning event will be generated. The user can configure a requirement to verify that a specified number of EPGs are being associated to a BD. The supported operators for this requirement are **At least** /**At most** /**Equal to**. As an example, if a requirement is configured that the BD must have at least 5 EPGs associated, violation events will be raised if the BD has less than 5 EPGs (0-4). However, if the BD has >= 5 events, then an enforcement event will be raised.

Before You Begin

You must have a BD selector created under object selectors before you begin this procedure.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Compliance Requirements**.
2. Click **Create New Compliance Requirement**.
3. In the **Name** field, enter a name for the compliance requirement.

4. In the **Compliance Type** field, choose **Configuration**.
5. Under **Base Configuration Settings**, choose **Enter configuration settings manually**.
6. In the **Enter Object Selector Name** area, choose the previously created BD selector.
7. Upon choosing the **bd-selector**, the **Must Have** option changes to a drop-down menu from which you choose **Must Be Associated With**.
8. In the **Enter Operator** field, choose the appropriate operator (**At least** /**At most** /**Equal to**).
9. In the **Enter Attribute Value** field, specify the appropriate value.
10. Click **Save**, and after the requirement is created, associate and activate it with the appropriate Compliance Requirement Set.

After the compliance check is completed, the events generated will be available under the **Compliance Analysis** tab.

Smart Event Management

Smart Event Dashboard

In the **Smart Event Dashboard**, the smart events are organized by severity, category, subcategory, and name.

- Only static path EPGs are displayed for `LEAF_USED_INTERFACE` smart events. The smart event details do not contain information about static leaf EPGs and dynamic VMM EPGs.

You can manage the display of the smart events by:

- Clicking one of the icons in the Smart Events by Severity bar displays only the smart events of the specified severity. All the smart events are displayed when clicking Total in the Smart Events by Severity bar.
- Clicking one of the buttons in the row above the Smart Events by Severity bar displays only the smart events in the selected category. Clicking an additional button adds smart events of the additional category to the display. Clicking a previously selected button removes the smart events of that category from the display. When none of the buttons are clicked, smart events of all categories are displayed. Clicking the filter icon at the beginning of the row de-selects all filter selections.
- Clicking **Aggregated** displays groups of smart events identified by event name.
- Clicking **Individual** displays every instance of the smart event.

A smart event contains the following information:

- Description—A description of the smart event.
- Impact—The negative impact that the smart event has on your fabric.
- Affected Objects—The objects in your fabric that are affected by the issue. The primary affected objects are highlighted.
- Checks—The Passing or Failing checks performed on the Smart Event and suggested steps to resolve the issue. Every passing or failing condition has a check code associated with it. The same check code may be used for a passing or failing condition and may be reused across Smart Events with different event codes.
- Event ID/Code—The ID and code associated with the Smart Event.

Smart Events Dashboard Guidelines for MSO Assurance Group Only

When viewing the **All Smart Events** table in the **Smart Events Dashboard** screen for MSO, under the **Individual** tab, you can see the aggregated ACI event details in MSO by clicking a site from the **Sites** column. You can view MSO Infra event details by clicking the **Event Name** column. **Sites** and **AG** (Assurance Group) name columns are also available in the table.

Lifecycle of a Smart Event

The lifecycle of a smart event appears as an overview summary timeline when displaying the details of an individual smart event. The lifecycle of a smart event is a graphical representation of the individual smart event occurrences in the epochs on the timeline. The color of the epoch icons signify the severity of the smart event. The magnification of the lifecycle can be controlled with the Zoom Level controls below the timeline.

Zoom Level: Lifecycle

Selecting the Lifecycle Zoom Level (default magnification) displays the time when the smart event reached a certain state. (A gray color icon indicates the smart event did not reach the threshold for the state.)

Lifecycle State	Description
First Raised	Initial occurrence of the smart event and the affected object.
Last Raised	Last occurrence of the smart event and the affected object.
Clearing	Smart event and affected object did not occur in one subsequent epoch.
Cleared	Smart event and affected object did not occur in two subsequent epochs.

In addition to these four smart event states, the CONNECTED_EP_LEARNING_ERROR and the FABRIC_EP_LEARNING_ERROR smart events have a Raising state that precedes the First Raised state. If a CONNECTED_EP_LEARNING_ERROR and the FABRIC_EP_LEARNING_ERROR smart event occurs in an epoch, it is in the Raising state. If it occurs in the next consecutive epoch, it is then considered to be in the First Raised state.

Example

If you have four consecutive epochs with the earlier epochs containing the occurrence of a smart event, the lifecycle of the smart event would have the following chronology when displayed with the Lifecycle Zoom Level.

- The initial occurrence of the smart event is contained in Epoch1.
    - The First Raised state indicates Epoch1.
- The last occurrence of the smart event is contained in Epoch2.
    - The Last Raised state indicates Epoch2.
- The smart event did not occur in Epoch3.
    - The Clearing state indicates Epoch3.
- The smart event did not occur in Epoch4.
    - The Cleared state indicates Epoch4.

Zoom Level: Magnified

Selecting a more granular Zoom Level (or clicking one of the icons on the timeline) increases the magnification of the timeline and displays epochs where the smart event occurred.

With the increased timeline magnification, you can navigate among the epochs by clicking one of the epochs or by using the navigation controls (located below the timeline and to the right of the Zoom Level). The selected epoch displays the date/time for the epoch as well as detailed information for the smart event occurrence.

Clicking the settings icon ⚙ in the Action column opens a menu so that you can edit one of the following pieces of information for the smart event:

- Operation Status: [New, In Progress, or Closed]
- Assign to: Assign to a UserId
- Comment: Add a comment
- Tags: Add a metadata tag

Upon completion of editing these pieces of information, the updated information is displayed in the detailed information for the smart event. You can search the individual smart events by Operation Status, UserID, or Tag value by making these columns a visible attribute to the individual smart event by setting **Column Customization** ☰ and typing the desired search term in the filter field of the appropriate column.

For example, if you edit an individual smart event to have a metadata tag of "Rare event" and add the Tags column to the table of individual smart events using **Column Customization**; you can search for the smart event by typing "Rare event" in the filter field of the Tags column.

Previous Occurrence and Next Occurrence

If NAE has access to information about the lifecycle of the smart event that is contained in earlier or later epochs, you can click on **Previous Occurrence** or **Next Occurrence** to display these lifecycles.

> ℹ Lifecycle does not support epochs from Cisco NAE release 3.1(1) and earlier releases.

Smart Event Suppression

A smart event in Cisco NAE provides information about the state of your network at the time represented by the epoch. Smart events are categorized as either Critical, Major, Minor, Warning, or Informational. Smart event suppression feature enables you to suppress smart events in the Cisco NAE UI and view only the smart events that are relevant.

> Events suppressed in an ACI epoch are not propagated to MSO epoch. You cannot add event suppression rules in an MSO epoch.

Smart Event Suppression Workflow

Smart event suppression workflow includes the following steps:

1. Create event rules: An event rule enables you to match a smart event against a rule using the match criteria.
   - An event rule contains the match criteria required to match a smart event against the rule and the action that should be applied on the matched smart event.
   - You can use attributes such as severity, category, subcategory, event code, affected object, and check code to define the match criteria for the event rule.
   - A match criteria can contain one attribute or multiple attributes.
     - If a match criteria contains multiple attributes, then the events containing all the attributes will be matched. All attributes inside a row must be met (The **AND** operator will apply to the attributes).
     - If a match criteria contains multiple check codes, then the events containing any one check code will be matched.
     - If a match criteria contains multiple affected objects, then the events containing all of the affected objects will be matched.
   - If an event rule contains multiple match criteria, then the events containing the union of the match criteria will be matched. Any events that match any criteria row will apply the rule (The **OR** operator will apply to the criteria).
   - Each event rule can have only one action. The options include **Suppressed**, **Never Suppressed**, and **No Action**.
   - An event rule containing the option **Never Suppressed**, supersedes an event rule containing the option **Suppressed**.

See Creating New Event Rule for more information.

2. Add event rules to event rulesets: An event ruleset enables you to group event rules and associate them with an Assurance Group. The event rules are applied when you activate the event ruleset.
   - An event ruleset contains event rules.
   - An event rule can be part of multiple event rulesets.

    - An event ruleset can be associated with an assurance group or with multiple assurance groups.
    - An event ruleset can be activated or deactivated.
    - When the event ruleset it activated, the event rules are applied.

See Creating New Event Ruleset for more information.

Manage Event Rules

On the **Smart Events** inspector page, the user can create and manage event rules and event rulesets under the **Manage Event Rules** tab.

Event Rules Applied to Current Epoch

On the **Smart Events** inspector page, the user can view the event rules for the current epoch selected in the timeline under the **Event Rules Applied to Current Epoch** tab.

Click **Smart Events Count** to view the smart events that match the event rule.

Guidelines and Limitations

Starting with Cisco NAE release 5.0(1), Event Rules using **Match Criteria** with **Affected Objects** will only support the **Equals to** regex criteria. If you have existing Event Rules that use **Affected Objects**, then verify that these rules meet this new requirement.

Creating New Event Rule

Use this procedure to create a new event rule.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rule**.
2. Click **Create New Event Rule**.
3. Complete the following fields for **Create New Event Rule**.
    a. In the **Event Rule Name** field, enter the name.
    b. In the **Description** field, enter the description.
    c. In the **Customize Next Step Message** field, enter the suggested next step/s for the user to take. You can create multiple rules based on different matching criteria to have more than one customized suggestion displayed in the Smart Events details for a given epoch.
    d. From the **Suppression** drop-down list, choose, the action for the event rule. The default is **No Action**. An event rule containing the action **Never Suppressed**, supersedes an event rule containing the action **Suppressed**.
4. Click **Add New Match Criteria** to define the match criteria for the event rule.
    a. Select the attributes for the match criteria. You can use severity, category, subcategory, event code, affected object, and check code to define the attribute for the match criteria.

> If multiple affected objects are included in the match criteria, then the events containing all the affected objects will be matched. If multiple check codes are included in the match criteria, then the events containing any one check code will be matched.

b. Check the checkbox for the match criteria.

> If an event rule contains multiple match criteria, then the events containing the union of the match criteria will be matched.

c. Click **Save**.

The new event rule is displayed in the **New Event Rule** table below.

Creating New Event Ruleset

Use this procedure to create a new event ruleset.

Before You Begin

- You have created an event rule.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rulesets**.
2. Click **Create New Event Ruleset**.
3. Complete the following fields for **Create New Event Ruleset**.
    a. In the **Event Ruleset Name** field, enter the name.
    b. In the **Description** field, enter the description.
    c. Check the **Associate to Current Assurance Group** checkbox to associate the event ruleset to the current Assurance Group. To activate the event ruleset, it must be associated with an Assurance Group.
        i. To associate the event ruleset at a later time, see Managing Event Rulesets.
        ii. To associate the event ruleset with another Assurance Group, see Managing Event Rulesets.
    d. Check the **Activate this Compliance Requirement Set** checkbox to activate the event ruleset. To activate the event ruleset at a later time, see Managing Event Rulesets.
4. In the **Associated Event Rules** area, choose the event rules that you want to associate. Click **Associate**.

    > If you include a combination of Never Suppressed Event Rules and Suppressed Event Rules in your event ruleset, the Never Suppressed Event Rules will take precedence over the Suppressed Event Rules.

5. (Optional) To disassociate an event rule, select the event rule and click **Disassociate**.
6. Click **Save**.

Viewing Smart Event Details Using a URL

Use this procedure to view Cisco NAE smart event details using a URL.

Before You Begin

- You have the smart event UUID.
- The URL to the Cisco NAE domain.

Procedure

1. Login to the Cisco NAE instance.
2. Append `/smart-event-viewer` to the location of the Cisco NAE instance.

    ```
    ThirdPartyApplication-URL/smart-event-viewer
    ```

3. Choose one of the following:

a. Append the event UUID with forward slash.

```
ThirdPartyApplication-URL/smart-event-viewer/06ed58a0-4b9cb2ed-fc60-3328-afdd-
13fb71659018-3317c2c277ba59300c05a88c329bd9d8
```

b. Append a GET Parameter named `event_uuid`.

```
ThirdPartyApplicationL/smart-event-viewer?event_uuid=06ed58a0-4b9cb2ed-fc60-
3328-afdd-13fb71659018-3317c2c277ba59300c05a88c329bd9d8
```

4. The smart event details associated with the event UUID such as name, severity, description, affected objects details, event code are displayed.

Managing Cisco Network Assurance Engine

Managing User Accounts

Use this procedure to manage user accounts.

Procedure

1. Choose **Settings** > **User Management**.
2. Select the user account.
3. From the **Action** column, choose the **Settings** icon.
4. To change the password of the user, click **Change Password**. Complete the following fields for **Change Password**.
    a. In the **Current Password** field, enter the current password.
    b. In the **Password** field, enter the new password.
        i. The password must adhere to the password policy defined in the **Passphrase Configuration** page.
        ii. The password must have characters from the following characters types: lowercase, uppercase, digit, symbol.
        iii. The allowed symbols include: _ ! @ # $ % ^ & * ( )
    c. In the **Confirm Password** field, enter the new password again.
    d. Click **Save**.
5. To edit a user account, click **Edit User Account**. Complete the following fields for **Edit User Account**.
    a. In the **Email** field, update the email address.
    b. Click **Save**.
6. To delete a user account, click **Delete**. You cannot delete an Admin user.
    a. In the **Delete User** form, click **Delete**.

Managing Passphrase

In Cisco NAE, an administrator can define the password policy for users accessing the appliance.

Use this procedure to configure the password requirements for Cisco NAE.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Passphrase Configuration** tile.
3. Complete the following fields for **Passphrase Configuration**.

a. From the **Minimum passphrase length** drop-down list, choose the minimum length for the password. The default value for **Minimum passphrase length** is 15 characters. The default value for **Maximum passphrase length** is 256 characters.

b. From the **Password lifetime** drop-down list, choose the time (in days) before the user account is disabled if the password is not changed. The default value is 3650 days.

c. From the **Expiry warning period** drop-down list, choose the warning (in days) before the user account is given a grace period if the password is not changed. Expiry warning period is the number of days prior to the **Password lifetime**, when a user is warned that the password is about to expire. The default is 14 days. In addition to the **Password lifetime**, the user is also given a **Grace period** to change the password.

d. From the **Grace period** drop-down list, choose the grace period (in days) before the user account is disabled. Grace period is the number of days in addition to the **Password lifetime** to change the password before the user account is disabled. The default is 3 days.

> ℹ After the grace period expires, the admin user will be forced to change the password upon the next log in. Non-admin users will be locked out, and the admin user will have to reset their password.

e. From the **Passphrase generation** drop-down list, choose the option to generate an instant password.

Managing Appliance Settings

Use this procedure to manage the Cisco NAE appliance settings.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Appliance Settings** tile.
3. To modify the DNS server, complete the following fields for **DNS Server**.
   a. Enter the IP address of the primary DNS server.
   b. (Optional) Enter the IP address of the secondary DNS server.
4. To modify the NTP server, complete the following fields for **NTP Server**.
   a. Check **Use External NTP Server** check box to configure external NTP server.

   > We recommend that you use an external NTP server to configure NTP servers. We recommend you to set the NTP time in sync with the local time.

i. Enter the domain name of the primary NTP server.

ii. (Optional) Enter the domain name of the secondary NTP server.

b. Uncheck **Use External NTP Server** check box to configure local NTP server.

5. To modify the SMTP server, complete the following fields for SMTP server.
   a. Enter the host name of the SMTP server.
   b. Enter the port number. Examples include common default ports, SMTP port number 25, or secure SMTP (SSL) port number 465.
   c. (Optional) Check the **SSL** check box to configure SSL for SMTP.
      i. Enter the username and password to access the SMTP server.
6. Click **Submit**.

Managing Assurance Groups

The following sections enable you to manage assurance groups for online assurance group analyses and offline assurance group analyses.

You can display existing assurance groups or create a new assurance group by clicking **Assurance Groups** in the **Setting** menu.

Creating a New Assurance Group for Online Analysis

On the Assurance Groups page, click the **Create New Assurance Group** link to create a new assurance group. See Performing Online Analysis, to complete the information required for the new assurance group.

Creating a New Assurance Group for Offline Analysis

An assurance group for offline analysis requires data collected from a Python script and the collected data is then uploaded to Cisco NAE. See Performing Offline Analysis for more information.

Managing an Assurance Group for Online Analysis

You can manage an assurance group for online analysis by performing the following actions:

- Click the **Settings** icon in the desired online analysis tile to perform the following actions:
    - Click **View** to view details of the assurance group.
    - Click **Delete** to delete the assurance group. Stop the online analysis before deleting the assurance group.
        - The delete operation only deletes the assurance group settings in the Cisco NAE.
        - When you delete the assurance group, all the analyses corresponding to the assurance group will be deleted.
        - To delete an assurance group that is part of a schedule, you must first delete the assurance group from the schedule and then delete the assurance group.
    - Click **Edit** to edit an assurance group. Stop the online analysis before editing the assurance group.
        - For ACI Assurance Group users only, while editing the assurance group, you can add, modify, or delete an assurance entity.
            - To add an assurance entity, click the **Add New Load Balancer** link to add an assurance entity. For details about adding an assurance entity, see Performing Online Analysis.
            - To modify an assurance entity, click the **Settings** icon of the assurance entity and select **Edit**. For details about modifying an assurance entity, see Performing Online Analysis.
            - To delete an assurance entity, click the **Settings** icon of the assurance entity and select **Delete**. Alternatively, check the checkbox for the assurance entity and click

Remove.

> To edit a NAT configuration file, download the NAT configuration file template, update the file, and then upload it to the Cisco NAE appliance. See Performing Online Analysis.

- When scheduling an analysis for ACI and MSO Assurance Groups, in the Assurance Groups screen, you must choose the items in a specific running order. Choose the appropriate ACI Assurance Group/s one by one first, and then choose the appropriate MSO Assurance Group/s. The running order will be sequentially displayed.
- Click the **Start Online Analysis** icon to run the analysis. If the Assurance Group is part of an active schedule, the schedule will stop and the analysis will start on the selected Assurance Group.
- Click the **Run Analysis on Demand** icon to run the online analysis for a specified number of times. If the Assurance Group is part of an active schedule, the schedule will stop and the analysis will start on the selected Assurance Group.
- Click **Stop** icon to stop the analysis on the Assurance Group. If the Assurance Group is part of an active schedule, the analysis on the Assurance Group will stop.
- Click **Schedule** to create or modify a schedule. For details about creating or modifying an assurance entity, see Schedule Assurance Group Analysis.
- Click **View Current Schedule** to view the scheduled order of the Assurance Groups and the approximate time to run the analysis. Viewing the schedules allows you to perform the following actions:
    - Click the **Stop** button to stop running the schedule.
    - Click the **Delete** button (after stopping the schedule) to delete the schedule.
    - Click the **Close** button to hide the **Timeline** for the schedule.

Managing an Assurance Group for Offline Analysis

See Managing Offline Analysis for more information.

Managing Offline Analysis

Use this procedure to manage an assurance group for offline analysis.

Procedure

1. Choose **Settings** > **Offline Analysis** to add, modify, or delete offline analyses.
    - To create a new offline analysis, click **Create New Offline Analysis**. For details about creating an offline analysis, see Performing Offline Analysis.
    - To view epochs or to delete an offline analysis, locate the desired offline analysis and click its settings icon (⚙) in the **Action** column.

- Choose **View Epochs** to view the epochs.
- Choose **Delete** to delete the offline analysis and click the **Delete** button. You cannot delete an offline analysis while the analysis is in progress.

> When you delete an offline analysis all the epochs and the epoch delta objects associated with the offline analysis will be deleted.

Setting Log Levels

Use this procedure to set the log levels.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Log Level Settings** tile.
3. For each category, choose the log level from the drop-down list. By default, the log levels are set to **Error** setting.
4. Click **Save**.
5. (Optional) Click **Restore to Factory Default**, to reset the log level to the default value.
6. To download the logs, choose **Settings** > **Download Tech Support Logs**.

Viewing Data Storage Usage

In the Cisco NAE appliance, analysis data is auto purged once the usage is above 80% and the analysis will be stopped once the analysis is above 90%.

- Only the oldest analysis data is deleted when the data storage usage reaches 80% or above.
- Once the data storage usage is above 90%, the analysis will be stopped. Even if the analysis is stopped due to the 90% threshold, Cisco NAE will continue purging the oldest analysis data until the usage falls below 80%.
- In the rare event that Cisco NAE has stopped the analysis due to the 90% threshold safeguard, the administrator must manually restart the analysis once the usage falls below 80%.

Use this procedure to view the data storage usage of the appliance.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. The data storage usage is displayed in the **Assurance Data Controls** tile.

Deleting Bundle File

Use this procedure to delete the Cisco NAE bundle file.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Software Management** tile.
3. In the Upload table, select the bundle file.
4. From the **Actions** menu, choose **Delete**.

5. Click **Delete**.

Managing Authentication Domains

Use this procedure to manage authentication domains. Only an administrator can manage authentication domains.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Authentication Domains** tile.
3. Select the authentication domain.
4. Choose the **Settings** icon.
   a. To edit an authentication domain, click **Edit**. You cannot edit the name of the authentication domain.
   b. To delete an authentication domain, click **Delete**. You cannot delete the Local or Default authentication domain. The default authentication domain is a system-wide setting that will affect all users.

> ℹ When you delete an authentication domain, all the users in the authentication domain will be logged out from the appliance.

c. To set an authentication domain as default, click **Set as default**. By default, the Local domain is set as the default authentication domain.

Managing Import and Export of Configurations

Use the following procedures to import or export the configuration of the NAE appliance (Cisco NAE release 4.1(1) and later). Only an administrator can manage all operations for configuration import and export.

With this feature you can import and export individual parts of the configuration for:

- Assurance Groups
- Event Rules
- Compliance
- User Config

Exporting a Configuration

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. In the **Configurations Import/Export** tile, click **Start Import / Export Configuration** link.
3. In the **Import/Export Configuration** page, click **Export**.
4. Select which parts of the configuration to export.
    - All
    - Assurance Groups
    - Event Rules
    - Compliance
    - User Config
5. Click **Export**. The exported configuration is downloaded as a compressed file. The exported file is displayed in the **Configurations Import/Export** tile.

Downloading a Configuration

Available configurations for download are displayed in the **Configurations Import/Export** tile. When the selected configuration download has been imported, the imported configuration settings replace the existing settings of the appliance.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. In the **Configurations Import/Export** tile, click **Download** link of the exported configuration file, once the export job status has moved to **Complete**. Alternatively, click the details icon of the **Configurations Import/Export** tile to display all the available configurations for download, and click the **Download** link of the exported configuration file. The selected configuration is downloaded as a compressed file that you can store locally.

The display of available configurations allows you to delete a configuration by clicking the delete icon of the selected configuration.

Importing a Configuration

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. In the **Configurations Import/Export** tile, click **Start Import / Export Configuration** link.
3. In the **Import/Export Configuration** page, click **Import**.
4. Click **Browse** to select the downloaded compressed configuration file.
5. Click **Upload** to upload the selected configuration file. The import job details are displayed in the **Configurations Import / Export** table. Status of the import job is updated to **Validated**.
6. Click **Select configurations to import** link to select the configurations to import.
7. Select which parts of the configuration to import.
    - Assurance Groups
    - Event Rules
    - Compliance
    - User Config
8. Click **Import**. The status of the import job is now updated to **Complete**.

Notes About Importing a Configuration

- You must be a user with administrator authority to import or export a configuration.
- 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 replaces the existing configuration. However, only for the Assurance Group option, the imported configuration is appended and does not replace the existing assurance group configuration in the destination appliance. An Assurance Group import process is ignored under the following conditions:
    - If an Assurance Group name is the same in the source and destination appliances.
    - If the Assurance Group display name is the same in the source and destination appliances.
    - If the fabric UUID is the same in the source and destination appliances.
    - For ACI Assurance Group users, if the Cisco APIC name is the same in the source and destination appliances.

Even if an Assurance Group configuration is ignored due to a reason listed above, the remaining valid Assurance Group configurations will get imported. Other configurations such as event rules, compliance, and user configurations will also get imported.

- Importing a configuration does not affect existing epochs, existing offline analyses, or existing online analyses because the system does not delete previously existing assurance groups.
  - Existing epochs continue to exist after importing a configuration.
  - Existing offline analyses continue to exist after importing a configuration.
  - Existing online analyses continue to exist after importing a configuration. You are not required to restart existing online analyses after importing a configuration. However, you are required to start online analyses of the imported configuration.
- The NAE GUI alerts you when importing a configuration. The alert cautions that importing an NAE configuration overwrites the existing configuration. Host passwords from the imported configurations are not valid and must be re-entered to enable the imported Assurance Group configurations to work properly. We recommend that you create a backup configuration by exporting the existing configuration before importing a configuration. The load balancer configuration must also be re-entered for the assurance group configuration to work correctly. The NAT configuration is ignored and not exported with the Assurance Group configuration.
- Importing a compliance rule, event rule, or user rule configuration replaces the existing rule configuration. This means that if the imported configuration does not contain any compliance, event, or user rules, the existing rules are not preserved.
- When the selected configuration has been imported, the imported configuration settings replace the existing settings of the appliance.
- The user configuration for LDAP or TACACS+ configuration is present under **Appliance Administration** in the **Authentication Domains** tile. For LDAP configuration, the bind password is not exported, so it must be re-entered manually after the import. For TACACS+ configuration, the key is not exported, so it must be re-entered manually after the import.

Historical Data Import and Export

Historical Data Import and Export feature enables you to import epoch data from a remote location or export epoch data to a remote location for ACI and NX-OS fabrics.

> ℹ Historical Data Import and Export is not supported in MSO.

- You must have super administrator privileges to import or export epoch data.
- During an import or historical export, you cannot perform any other actions on Cisco NAE until the job is completed
- A running analysis or schedule may be interrupted by a historical export or import, and will be restarted after the job is completed. This does not apply to an online analysis that has 10 or less iterations to run, and also does not apply to an offline analysis. These jobs will not be restarted.
- Stop all the jobs on Cisco NAE before performing an import or historical export of epoch data.
- Imported epoch data cannot be exported.
- Every historical export job has a corresponding log file that details every epoch that fails. Historical export jobs are capped at 32Mb total, and if the logs reach a certain size, the older ones will be automatically deleted.
- Historical data import and export does not include import and export of the configurations such as Assurance Groups, event rules, compliance, and user configuration.
- Import and export of configurations will not export settings relating to the historical data import and export.
- When importing an epoch, the corresponding Event rules and Compliance configurations are not imported and hence they may not be visible in **Manage Event Rules** and **Manage Compliance** area.

Importing Epoch Data

Use this procedure to import epoch data.

> ℹ Data import is not supported in MSO epochs.

Before You Begin

- You have the IP address or hostname of the remote server.
- You have installed the RSA key on the remote server for a specified user.
- The specified user has permissions to read data from the folder specified in the remote path.
- You have the path to the exported epoch data in the remote server.

Procedure

1. Log in to Cisco NAE as a super admin.

2. Choose **Settings** > **Appliance Administration**.
3. Click the details icon on the **Import/Export Historical Data** tile.
4. In the **Schedule Import/Export Historical Data** page click **Import**.
5. In the **IP Address/Hostname** field, enter the IP address or hostname of the remote server.
6. In the **Username** field, enter the username to access the remote server.
7. In the **Remote Path** field, enter the path to the epoch data in the remote server.

Example of remote path format: `/path/to/backup/fabric name-uuid/EPOCH-2020-05-29-16-36-26-UTC`

8. Click **View Public Key**. Copy the RSA key and add it to the `~/.ssh/authorized_keys` file on the remote server.
9. If this fie is not present on the server, perform the following steps to create one and update the permissions.
   a. Create the .ssh directory.

      ```
      mkdir ~/.ssh
      ```

   b. Update the permission.

      ```
      chmod 700 ~/.ssh
      ```

   c. Create the authorized_keys file.

      ```
      touch ~/.ssh/authorized_keys
      ```

   d. Update the permission.

      ```
      chmod 600 ~/.ssh/authorized_keys
      ```

10. Click **Submit**.
11. (Optional) Click **Cancel** to stop the import epoch job.
12. (Optional) Click **Download Tech Support Logs** to download the logs.
13. The imported epoch job details are displayed in the **Import History Table**.
    a. Click the ⚙ icon and then choose **Delete** to delete the import epoch job.

Exporting Epoch Data

Use this procedure to export epoch data.

> Data export is not supported in MSO epochs.

Before You Begin

- You have the IP address or hostname of the remote server.
- You have installed the RSA key on the remote server for a specified user.
- You have the destination path for the exported epoch data in the remote server.
- The specified user has permissions to write data to the folder specified in the remote path.

Procedure

1. Log in to Cisco NAE as a super admin.
2. Choose **Settings** > **Appliance Administration**.
3. Click the details icon on the **Import/Export Historical Data** tile.
4. In the **Schedule Import/Export Historical Data** page click **Export**.
5. From the **Backup Option** drop-down list, select the backup option.
    - No Backup: Disables the inline export of epoch data.
    - Inline Data Only: Enables you to automatically export newly generated epoch data. To disable inline export, choose the **No backup** option.
    - Historical Data Only: Enables you to export the the data of epochs in a given time range.
    - Both Historical Data and Inline Data: Enables you to export the data of epochs in a given time range and also automatically export newly generated epoch data.
6. In the **IP Address/Hostname** field, enter the IP address or hostname of the remote server.
7. In the **Username** field, enter the username to access the remote server.
8. In the **Destination Path** field, enter the folder location to export the epoch data.
9. Select the date and time range for **Historical Data Only** and **Both Historical Data and Inline Data** options.
10. Click **View Public Key**. Copy the RSA key and add it to the `~/.ssh/authorized_keys` file on the remote server.
11. Click **Submit**. The epoch data is exported to the folder specified in the destination path. In the specified destination path, Cisco NAE will create a folder in the format `fabric name-UUID` and the epoch data will be exported using the UTC timestamp.
12. (Optional) Click **Cancel** to stop the job. The exported epoch job details are displayed in **Export History** table. Hover the mouse pointer over the **STOPPED** status of the job to view the details of the number of epochs exported.
13. (Optional) Click **Download Tech Support Logs** to download the logs.
14. The exported epoch job details are displayed in the **Export History** table.
    a. For historical exports, click the ⚙ icon and then choose **Download Failed Epoch Log** to download epoch logs if there were any failed epochs during the job.
    b. Click the ⚙ icon and then choose **Delete** to a delete historical export epoch job.

Managing Epoch Delta Analysis

Use this procedure to manage a epoch delta analysis.

Procedure

1. Choose **Epoch Analysis** > **Epoch Delta Analysis**.
2. Click **Analysis Management**.
3. In the **Delta Analysis** table, select a delta analysis and click the ✏ icon to edit the name.
4. Click the ⚙ icon and then choose **Delete** to delete the delta analysis. To delete a delta analysis that is running, you must stop the delta analysis before deleting.
5. Click the ⚙ icon and then choose **Stop** to stop a running delta analysis.
6. Click the ⚙ icon and then choose **View Results** to view the results of a delta analysis.

Managing Object Selectors

> Currently, this is supported for ACI Assurance Group only.

Use this procedure to manage Object selectors.

Before You Begin

- You have created at least one object selector.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Object Selectors**.
2. In the Object Selector table that is displayed, click the ⚙ icon in the **Action** column for the object selector you want to manage.
3. Choose the action to perform from the following options:
    a. Choose **Edit** to edit the object selector from the Object Selectors table.
    b. Choose **Delete** to delete the object selector, and in the **Delete Object Selector** dialog box that is displayed, confirm **Delete**.

> If the Object Selector that you want to delete is used in a requirement, remove the association and then delete the Object selector.

c. Choose **Copy** to copy the values of the existing object selector to create a new object selector, and perform the following actions:
    i. In the **Create New Object Selector** dialog box, in the **Object Selector Name** field, add a name.
    ii. In the remaining pre-populated fields, modify any values as appropriate.
    iii. Click **Save**.

Managing Traffic Selectors

> Currently, this is supported for ACI Assurance Group only.

Use this procedure to manage traffic selectors.

Before You Begin

- You have created at least one traffic selector.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Traffic Selectors**.
2. In the Traffic Selector table that is displayed, click the ⚙ icon in the **Action** column for the

Traffic selector you want to manage.

3. Choose the action to perform from the following options:
   a. Choose **Edit** to edit the traffic selector from the Traffic Selectors table.
   b. Choose **Delete** to delete the traffic selector, and in the **Delete Traffic Selector** dialog box that is displayed, confirm **Delete**.

> If the Traffic Selector that you want to delete is used in a requirement, remove the association and then delete the traffic selector.

Managing Compliance Requirements

> Currently, this is supported for ACI Assurance Group only.

Use this procedure to manage compliance requirements.

Before You Begin

- You have created at least one compliance requirement.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Compliance Requirements**.
2. Click the ⚙ icon in the **Action** column for the compliance requirement you want to manage.
3. Choose the action to perform from the following options:
   a. Choose **Edit** to edit the compliance requirement from the **Edit Compliance Requirement** area.
   b. Choose **Delete** to delete the compliance requirement, and in the **Delete Compliance Requirement** dialog box that is displayed, confirm **Delete**.

> If the Compliance Requirement that you want to delete is used in a requirement set, remove the association and then delete the Compliance Requirement.

Managing Compliance Requirement Sets

> Currently, this is supported for ACI Assurance Group only.

Use this procedure to manage compliance requirement sets.

Before You Begin

- You have created at least one compliance requirement set.

Procedure

1. Choose **Compliance** > **Manage Compliance** > **Compliance Requirement Sets**.
2. Click the ⚙ icon in the **Action** column for the compliance requirement you want to manage.
3. Choose the action to perform from the following options:
    a. Choose **Edit** to edit the compliance requirement set from the **Edit Requirement Set** area.
    b. Choose **Delete** to delete the compliance requirement set, and in the **Delete Requirement Set** dialog box that is displayed, confirm **Delete**.

> If the Requirement Set is associated with an assurance group, disassociate the Requirement Set and then delete the Requirement Set.

Managing Event Rules

Use this procedure to manage event rules.

Before You Begin

- You have created at least one event rule.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rules**.
2. Select an event rule and click the ⚙ icon in the **Action** column to perform the following actions:
    a. Choose **Edit** to edit the event rule.
    b. Choose **Copy** to copy the event rule.
    c. Choose **Delete** to delete the event rule.
3. Click an event rule to view the details of the event rule.

Managing Event Rulesets

Use this procedure to manage event rulesets.

Before You Begin

- You have created at least one event ruleset.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rulesets**.
2. Select an event ruleset and click the ⚙ icon in the **Action** column to perform the following actions:
    a. Choose **Associate** to associate the event ruleset to the current Assurance Group.
    b. To associate the event ruleset to a different assurance group,
        i. Select the Assurance Group from the **Assurance Group** drop-down list.
        ii. Select the event ruleset and click the ⚙ icon in the **Action** column.
        iii. Choose **Associate**.
    c. Choose **Activate** to activate the event ruleset. To activate an event ruleset, it must be associated with an Assurance Group. Activating an event ruleset not associated with an Assurance Group, automatically associates the event ruleset with the current Assurance Group and activates the event ruleset.
    d. Choose **Disassociate** to disassociate the event ruleset from the current Assurance Group. Disassociating an active event ruleset will deactivate the event ruleset.
    e. Choose **Deactivate** to deactivate the event ruleset.

f. Choose **Edit** to edit the event ruleset.

g. Choose **Copy** to copy the event ruleset.

h. Choose **Delete** to delete the event ruleset. Deleting a ruleset does not delete the rules included in the ruleset.

Update Setup for a Pre-Change Analysis

> Currently, this is supported for ACI Assurance Group only. After you save and run a pre-change analysis, you cannot edit it. You can use the results or you can delete it.

Before You Begin

- At least one assurance group must be created.
- At least one base epoch must be created.
- You have created at least one pre-change analysis.

Procedure

1. Choose **Change Management** > **Manage Pre-Change Analysis**.
2. In the **Manage Pre-Change Analysis** table that is displayed, click the ⚙ icon in the **Action** column for the Pre-Change Analysis setup you want to change.
3. Choose the action to perform from the following options:
   a. Choose **View** to view a Pre-Change Analysis manual configuration.
   b. Choose **View Epoch Delta** to view the health delta analysis between the base epoch and the Pre-Change Analysis job. Click the browser back button two times to return to the Pre-Change Analysis screen.
   c. Choose **Edit** to modify a Pre-Change Analysis. You can only edit a Pre-Change Analysis job that is saved earlier and it displays an analysis status of **Saved**. After you initiate a Pre-Change Analysis, you cannot edit it.
   d. Choose **Download** to download the configuration file that can be uploaded to Cisco APIC.
   e. Choose **Clone** to clone a new Pre-Change Analysis from an existing manual configuration Pre-Change Analysis. For additional details about cloning a pre-change analysis, see Clone Pre-Change Analysis.
   f. Choose **Delete** to delete the Pre-Change Analysis, and in the **Delete Traffic Selector** dialog box that is displayed, confirm **Delete**.

Troubleshooting

Downloading Logs

Use this procedure the download the logs for the Cisco NAE appliance.

Procedure

1. Choose **Settings** > **Download Tech Support Logs**. The logs are collected from each VM in the cluster and they are aggregated into a tar file. Downloading logs can take up to several minutes.
2. (Optional) If it is taking more than 5 minutes for the tech support logs to be downloaded, you can access the logs using the following procedure. You can also use this procedure, if you receive an error message while downloading the tech support logs.
   a. Contact Cisco TAC to obtain the one time password (OTP) for root access.
   b. Log in to one of the VMs of the appliance as root.
   c. Run the following command:

      ```
      /usr/lib/candid/share/support/tech_support --logs --dir /hadoop/network-audits
      --output tech_support
      ```

   d. Download the following tar file from the VM and provide it to TAC for debugging.

      ```
      /hadoop/network-audits/tech_support.<timestamp>.tar
      ```

Appliance Events

Cisco NAE raises **Appliance Events** to monitor the health of the appliance. These events are generated as part of the cron job that is installed on all the hosts and the cron job is configured to run every 5 mins. The **Appliance Events** are useful for troubleshooting the appliance.

Procedure

1. Choose **Settings** > **Appliance Status**.
2. Click **Event Name** to view the details of the event.

Appliance Event Types

The **Appliance Events** are categorized into the following types.

Provisioned Capacity Events

These events monitor the appliance capacity provisioned with respect to the defined specifications of the appliance. These events are generated at every reboot. The different specifications are defined for the different flavors of the appliance. The following events are included in this category.

1. APPLIANCE_PROVISIONED_CAPACITY_BELOW_SPEC
2. APPLIANCE_PROVISIONED_CAPACITY_ABOVE_SPEC
3. APPLIANCE_PROVISIONED_CAPACITY_AT_SPEC

Local Filesystem Usage Events

These events monitor the storage usage on each of the hosts.

The following events are included in this category.

1. APPLIANCE_FILESYSTEM_NORMAL
2. APPLIANCE_FILESYSTEM_EXCEEDED_LOW_WATERMARK
3. APPLIANCE_FILESYSTEM_EXCEEDED_HIGH_WATERMARK

Web Server Events

These events monitor the health of the web servers. The following events are included in this category.

1. APPLIANCE_WEB_SERVICES_OPERATION_NORMAL
2. APPLIANCE_WEB_SERVICES_PARTIAL_FAILURE
3. APPLIANCE_WEB_SERVICES_COMPLETE_FAILURE

Application Server Events

These events monitor the health of the application servers. The following events are included in this category.

1. APPLIANCE_APPLICATION_OPERATION_NORMAL
2. APPLIANCE_APPLICATION_PARTIAL_FAILURE
3. APPLIANCE_APPLICATON_COMPLETE_FAILURE

Database Events

These events monitor the health of the database. The following events are included in this category.

1. APPLIANCE_DATABASE_OPERATION_NORMAL
2. APPLIANCE_DATABASE_PARTIAL_FAILURE
3. APPLIANCE_DATABASE_REACHED_LOW_THRESHOLD
4. APPLIANCE_DATABASE_AT_PURGE_LIMIT

Analysis Latency Events

These events monitor the time taken to analyze the data. Each analysis is associated with an analysis interval and analysis must be completed within the specified interval time.

The following events are included in this category.

1. ANALYSIS_COMPLETED
2. ANALYSIS_COMPLETED_BUT_TOOK_TOO_LONG
3. ANALYSIS_TIMED_OUT

Analysis Application Events

These events monitor the health of the analysis application.

The following events are included in this category.

1. APPLIANCE_ANALYSIS_ENGINE_OPERATION_NORMAL
2. APPLIANCE_ANALYSIS_ENGINE_FAILURE

HDFS Filesystem Events

These events monitor the health of the namenodes and datanodes.

The following events are included in this category.

1. APPLIANCE_FILESYSTEM_OPERATION_NORMAL
2. APPLIANCE_FILESYSTEM_PARTIAL_FAILURE
3. APPLIANCE_FILESYSTEM_COMPLETE_FAILURE

YARN Events

These events monitor the health of the resource Managers and node managers.

The following events are included in this category.

1. APPLIANCE_INFRA_RESOURCE_OPERATION_NORMAL
2. APPLIANCE_INFRA_RESOURCE_PARTIAL_FAILURE
3. APPLIANCE_INFRA_RESOURCE_COMPLETE_FAILURE

Host Reachability Events

These events monitor if all the hosts are reachable from all other hosts in cluster. A ping test is used to test reachability of the hosts.

The following events are included in this category.

1. ALL_CLUSTER_MEMBERS_ARE_REACHABLE

2. CLUSTER_MEMBER_REACHABILITY_ERROR

Troubleshooting Scenarios

This section contains information about possible solutions for common troubleshooting scenarios for the Cisco NAE appliance.

Problem

Unavailability of the datastore in the host results in the failure of the file system IO located in the guest VM of the Cisco NAE appliance. As a result, the guest VM’s kernel filesystem driver marks the mounted file system as read-only making the Cisco NAE appliance unavailable. The functionality of the Cisco NAE appliance such as generating new epochs, collecting tech support logs, and accessing the UI is affected.

Solution

To resolve this issue, contact Cisco TAC.