Cisco Network Assurance Engine Release Notes, Release 4.1(x)

Table of Contents

First Published: 2020-02-10

Last Modified: 2020-05-18

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

Introduction

This document describes the features, caveats, and limitations for the Cisco Network Assurance Engine (NAE).

Release notes are sometimes updated with new information about restrictions and caveats.

See Related Content for information regarding additional product documentation.

Date	Description
April 30, 2020	Release 4.1(2) became available.
March 2, 2020	Added CSCvt11952 to the Open Issues section.
February 10, 2020	Release 4.1(1) became available.

New Software Features

New Software Features in Release 4.1(1)

Feature	Description
Smart Licensing	Cisco Smart Licensing is enabled in Cisco NAE. Cisco Smart Licensing is a unified license management system that manages all the software licenses across Cisco products. As a new Cisco NAE user, after you log into Cisco NAE, Smart Licensing is automatically placed in the Evaluation Period for 90 usage days. After you register with CSSM (Cisco Smart Software Manager), the Evaluation Period countdown clock stops and Smart Licensing is in the Registered state. Users that upgrade to Cisco NAE, release 4.1(1) from an earlier release will be in the unregistered and evaluation mode. In order to register, they must contact their Cisco Sales Representative. Their representative will convert their existing licenses to the Smart Licenses and deposit them into CSSM. If they do not have a CSSM account already, a new CSSM account will be created for them. See the *Cisco Network Assurance Engine Installation and Upgrade Guide, Release 4.1(x)* for more information.
Pre-Change Analysis	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.
Assurance for Load Balancer	An Assurance Entity can be included in an Assurance Group. An Assurance Entity is an ancillary item in the ACI fabric that provides support to the overall fabric.In this release, an F5 load balancer can be included as an Assurance Entity and can be included in an Assurance Group.
Explorer Enhancements	In the Explorer page, up to four active epochs for exploring across all Assurance Groups is supported.
Import or Export Configuration	Import or export of an Cisco NAE appliance configuration is supported in this release. You can import or export all or individual parts of a configuration such as Assurance Groups, Event Rules, Compliance, and user configuration.
Global Search enhancements	The Global Search field accepts a partial identifier to filter the menu of available objects for the search. You can export results of a global search to a comma separated variables (csv) or JSON file.

Feature	Description
Appliance Migration	Migration of Cisco NAE appliance is supported for migration from small to medium appliance model and migration from medium to large appliance model
ACI GOLF Assurance	ACI GOLF is now assured by Cisco NAE.
Cisco HyperFlex Systems support	Cisco HyperFlex HX240c M5 SFF Hybrid is supported for Cisco NAE. See the *Cisco Network Assurance Engine Installation and Upgrade Guide, Release 4.1(1)* for more information.
Cisco APIC 4.2 support	Cisco APIC Release 4.2 is supported by Cisco NAE Release 4.1(1).
Config Compliance for EPG	A preview link is available to view the objects that are included or excluded in the object selector in Cisco NAE.
L1 event enhancement	The following smart events were enhanced with additional interface information: • LEAF_CONFIGURED_INTERFACE_OPER_UP (6020) • LEAF_CONFIGURED_INTERFACE_OPER_DOWN_ADMIN_UP (6021) • LEAF_CONFIGURED_INTERFACE_OPER_DOWN_ADMIN_DOWN (6022) • LEAF_UNCONFIGURED_INTERFACE_OPER_UP (6023) • LEAF_UNCONFIGURED_INTERFACE_OPER_DOWN_ADMIN_UP (6024) • LEAF_USED_INTERFACE_OPER_DOWN_ADMIN_UP (6029) • LEAF_USED_INTERFACE_OPER_DOWN_ADMIN_DOWN (6030)
Add view filters on Smart Events page	The buttons for filtering the display of smart events are added to the Smart Event Dashboard.
New Smart Events	The following smart events were introduced in this release: • CHANGE_ANALYSIS smart events (Event code: 7028, 7029) • Load Balancer assurance smart events (Event code: 31013, 31014, 31015, 31016, 31017, 31018, 31019, 31020) • SYSTEM smart events (Event code: 31002, 31003, 31006, 31007, 60011) • TENANT_FORWARDING smart events (Event code: 6312)

New Software Features in Release 4.1(2)

Feature	Description
Compliance scale enhancements	Support for up to 200 requirements per Requirement Set.
Compliance APIs	Additional compliance APIs are added.

Open Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the releases in which the bug exists. A bug might also exist in other releases.

Release notes are sometimes updated with new information about restrictions and caveats.

Bug ID	Description	Exists in
CSCvq75199	When viewing an interface ethernet in Explorer, Smart Events that contain the interface name parameter are also visible.	4.1(1), 4.1(2)
CSCvs72114	Configuration compliance for EPG raises a verified smart event even if the corresponding EPG does not have an attribute.	4.1(1), 4.1(2)
CSCvu02174	Cisco NAE REST API Swagger Interface does not contain information for all the published REST APIs for Cisco NAE.	4.1(1), 4.1(2)

Resolved Issues

Click the bug ID to access the Bug Search Tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Bug ID	Description	Fixed In
CSCvq75701	CAN query cannot talk on a filter port query (ICMP/TCP).	4.1(1)
CSCvq82544	Epoch timeline does not show updated information after an offline analysis is deleted.	4.1(1)
CSCvq99544	Performing a search on Policy CAM related events, results in an error.	4.1(1)
CSCvr02870	Passing checks are not displayed in the detailed view for the smart event `APP_EPG_STATIC_PORT_PATH_MAY_NOT_DEPLOY`.	4.1(1)
CSCvs38034	The Epoch timeline is marked as timed out for certain epochs.	4.1(1)
CSCvs45697	Configuration errors in ADC events may not be detected when the same VRF name and IP subnet are present in different tenants.	4.1(2)
CSCvt11952	Incorrect segmentation violation may be reported by compliance.	4.1(2)

Known Issues

Click the Bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the releases in which the known behavior exists. A bug might also exist in releases.

Bug ID	Description	Exists In
CSCvi51374	For scale configurations, a few API queries (notably the prefix, Policy CAM, or endpoint table) can result in an HTTP error code 500 due to a high load on the DB/backend.	4.1(1) and later
CSCvk36185	Renaming or replacing a filter entry does not show change in epoch health delta.	4.1(1) and later
CSCvo42680	LOG_PERMIT_POLICY_ENFORCED smart event is generated for the actrlRule that has threshold, redir action.	4.1(1) and later
CSCvq70757	For an object with the same key for either **Event Table**, **Endpoint Table** or **Prefix Table**, the search display may show multiple rows depending on the time range.	4.1(1) and later

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:
  - If you upload a JSON file in the Change Definition field, the file size must be no greater than 15 MB.
  - If you upload a file or specify the changes manually, the Tenant file within which the configuration is modified must be no greater than 15 MB.
  - If you upload a file with unsupported objects, Cisco NAE will remove the unsupported object and run the job.
- A Pre-change Analysis job may fail or return incorrect results if the Cisco ACI configuration has features that are unsupported by Cisco 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.

Software Compatibility Information

The following table lists the compatibility information for the Cisco NAE.

Release versions of the Cisco APIC and the Cisco NX-OS software that are not listed in the table below are not supported.

Table 1. Cisco ACI Compatibility Information

Cisco APIC Release	Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches
4.2	14.2
4.1	14.1
4.0	14.0
3.2	13.2
3.1	13.1
3.0	13.0
2.3	12.3
2.2	12.2
2.1	12.1
2.0	12.0
1.3	11.3
1.2	11.2

Supported Load Balancers

The following table lists the supported load balancers for the Cisco NAE.

Table 2. Supported Load Balancers

Load Balancer Name	Release
F5 BIG-IP LTM	12.1.3
F5 BIG-IP LTM	14.1.0

Hardware Compatibility Information

The Cisco APIC hardware compatibility information for Cisco NAE can be accessed at the following website:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/release-notes/Cisco-APIC-Release-Notes-412.html#CompatibilityInformation

Verified Scalability Limits

The following table lists the maximum verified scalability limits for the Cisco NAE .

Table 3. Verified Scalability Limits

Feature	Scale Limit for Appliance Model: Small	Scale Limit for Appliance Model: Medium	Scale Limit for Appliance Model: Large
APIC Fabric Size	50 leaf switches	100 leaf switches	400 leaf switches
Number of VMs	3	3	3
Policy CAM Rules	200 K	400 K	400 K
Endpoints	50 K	100 K	100 K
Number of Prefix Matches	25 K	50 K	50 K
Total number of smart events, endpoints, and prefixes	300 K	500 K	600 K
Number of Concurrent Assurance Analysis	1	1	1
Analysis Interval in ACI Network Mode	15 minutes or more	15 minutes or more	30 minutes or more
Analysis Interval in ACI Application Mode	25 minutes or more	15 minutes or more	Not Supported

Table 4. Verified Scalability Limits for Compliance

Compliance Checks	Scale Limit
Total number of Requirement Sets that can be active at a given time	3
Number of Requirements per Requirement Set	200 Requirements of type Compliance Requirement and Naming Convention 10 Requirements of type Segmentation, Traffic Selector, and SLA

EPG pair limit check per Requirement (includes both directions)	1000 The scale limit is applicable if the compliance requirement flag`enable_aggregate_event_for_tenant` is set to false using Cisco NAE REST APIs. 500 The scale limit is applicable for number of violated EPG pairs if the compliance requirement flag`enable_aggregate_event_for_tenant` is set to true using Cisco NAE REST APIs. NOTE: In the latter case, the scale switches to Tenants, and 50 Tenants are supported. In addition, no **info** events are generated for EPGs that conform to the compliance rule. You will only see violations.
Fabric wide rules	150 K

Table 5. Verified Scalability Limits for Explorer

Feature	Scale Limit
Total number of associations we can explore	500 K
Fabric wide rules	150 K

Licensing Information

Cisco NAE is licensed as an annual subscription with 1-, 3-, and 5-year term options.

See the *Cisco Network Assurance Engine Ordering Guide* for more information.

See the *Cisco Network Assurance Engine Installation and Upgrade Guide* for information regarding Smart Licensing.

End-of-Life and End-of-Sale Notices

The End-of-Life (EoL) and End-of-Sale (EoS) notices for Cisco NAE can be accessed from the following website:

https://www.cisco.com/c/en/us/products/data-center-analytics/network-assurance-engine/bulletin-listing.html

Usage Guidelines

This section lists usage guidelines for the Cisco NAE.

- The Cisco NAE appliance leverages email as the mechanism for password recovery. We strongly recommended that you configure the SMTP server information, as that is required by the admin for password recovery. You can configure SMTP server information during Day 0 setup or after you setup the Cisco NAE appliance. To configure SMTP server after Day 0, perform the following steps:
  1. Choose **Settings** > **Appliance Administration**.
  2. Click the details icon on the **Appliance Settings** card.
  3. Enter the SMTP server information.
- Admin can use the following two methods to change the user's password.
  - In the **Change Password** form, enter the user's current password and then enter the new password.
  - Use the **Forgot Password** link. The SMTP server must be configured in order to reset the password using the forgot password link.
- Ensure that the last octet of the IP address is unique for each VM in the cluster. In the Cisco NAE appliance, hostname is created using last octet of VM's IP address. If the VMs in the Cisco NAE cluster are assigned the same last octet, they will get the same hostname which will lead to issues while forming the cluster.
- We recommend that you upload only one file at a time per VM in the cluster. Uploading multiple files at the same time can lead to the appliance being unresponsive. this recommendation applies to offline datasets and the upload bundle.
- Appliance settings must be configured on only one VM in the Cisco NAE cluster. Do not configure the appliance settings on more than one VM simultaneously.
- 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.
- The data collected by the Cisco NAE appliance from an unsupported version of APIC or switch, may result in generation of false positives. Assurance events will also be generated. See Compatibility Information .
- 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.
- 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 need to be rendered, the slower the page will load.
- We recommend that you do not create more than 100 Assurance Groups or perform more than 100 offline analysis.
- When the installation of the Cisco NAE is in progress, if you refresh the page during the **Restarting System Services** operation, the error message `Experiencing temporary connectivity`

`loss. Waiting for the server to respond.` is displayed. During this operation, system services are being restarted to complete the installation of the Cisco NAE. You may experience temporary connection loss while this operation is in progress.

- During the upgrade process, ensure that all the VMs are up and running. Partial upgrades of the VMs is not supported.
- While you are currently allowed to create more than one Epoch Delta Analyses at any given time, we recommend that you 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.
- Occasionally, on slower links, accessing Cisco NAE using IP address may result in UI not displaying all the icons. Use the Fully Qualified Domain Name to display the icons.
- 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 }}
```

Related Content

The Cisco NAE documentation can be accessed from the following website:

https://www.cisco.com/c/en/us/support/data-center-analytics/intent-assurance/tsd-products-support-series-home.html

Document	Description
Cisco Network Assurance Engine Release Notes	This document.
Cisco Network Assurance Engine Installation and Upgrade Guide	Describes how to install and upgrade the Cisco NAE.
Cisco Network Assurance Engine Getting Started Guide	Describes how to configure and manage the Cisco NAE.
Cisco Network Assurance Engine Fundamentals Guide	Describes some of the use cases for the Cisco NAE.
Cisco Network Assurance Engine Smart Events Reference Guide	Describes the smart events found in the Cisco NAE.
Cisco Network Assurance Engine REST API User Guide	Describes the REST APIs found in the Cisco NAE.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to cisconae-docfeedback@cisco.com. We appreciate your feedback.

Legal Information