Cisco Network Assurance Engine Release Notes, Release 4.0(1)

Table of Contents

First Published: 2019-08-26

Last Modified: 2019-12-12

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)

© 2017-2019 Cisco Systems, Inc. All rights reserved.

Cisco Network Assurance Engine, Release 4.0(1), Release Notes

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

Additional product documentation is listed in the **Related Documentation** section.

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

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
August 26, 2019	Created the release notes for the 4.0(1) release.
September 27, 2019	Created the release notes for the 4.0(1a) release.
December 12, 2019	Created the release notes for the 4.0(1b) release.

Introduction

The Cisco NAE provides operators with a new approach to manage SDN-based data centers confidently. The Cisco NAE is built on a comprehensive formal model of the network, combined with deep domain knowledge of networking. The Cisco NAE software provides operations teams with continuous and proactive network verification and intent assurance.

Business drivers such as cloud, mobile, and digitization trends are demanding more from modern data centers, rapidly increasing their scale, rate of change, and complexity. With the Cisco Application Centric Infrastructure (ACI) and other SDN technologies, network infrastructures have evolved to provide programmable interfaces, automation, agility, and virtualization. However, operational tools still center around traditional approaches, such as probe tools, packet sniffers, and the command line interface (CLI) to reason about the network. These are inherently reactive-after-the-fact, manual, and rely on the tribal knowledge of a handful of experts to reasonably reconstruct a network state.

The Cisco NAE takes the intent from the controller as a logical policy, as well as configurations and the data plane (infra) state from each switch device, to build a network-wide model of the underlay, overlay, and virtualization layers.

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 2. Cisco ACI Compatibility Information

Cisco APIC Release	Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches
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

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	10
EPG pair limit check per Requirement (includes both directions)	1000
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

Important Notes

- For production analysis, the supported Assurance Group setting for **Analysis Interval** is 15

minutes or more. An interval below 15 minutes should be only used for lab or test purposes.

- Depending on the complexity of the configured policies, in some cases, it has been observed that the run time exceeds 15 minutes, especially for the Cisco NAE small appliance. This issue can be addressed in the following ways:
  - Set a polling interval of greater than 15 minutes to provide more time for the computation to finish.
  - Deploy a Cisco NAE medium appliance. The run time may come down below 15 minutes as there is more processing power and memory in the medium appliance to finish the analysis sooner.
- Rarely it has been observed that the appliance may not be able to analyze the security policy complexity of the rules on a given switch. As a result, the Cisco NAE will skip the security policy analysis for that particular switch and carry out the rest of the analysis normally. It is important to note the following:
  - The security radial view will show the contracts on the switch for which the analysis could not be run as **Green** to facilitate security contract visualization.
  - The following **System Assurance** event will be generated to indicate that the security analysis of a given switch could not be performed.
    - EVENT: UNABLE_TO_PERFORM_SECURITY_ANALYSIS _FOR_SWITCH
    - CATEGORY : SYSTEM
    - SUBCATEGORY: ASSURANCE_CONTROL
    - Primary object: Leaf switch on which the security policy analysis could not be performed.
    - Description: The Cisco NAE appliance could not perform tenant security analysis for this particular leaf switch. This happens as the rule complexity grows beyond the bounds of the first generation solver.
- Support for a scale limit of 400 leaf switches for the Large appliance in the ACI network mode is a beta feature in this release.

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 Getting Started Guide* for information on uploading a license to Cisco NAE.

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

New and Changed Information

New Software Features

The following table lists the new software features in this release:

Feature	Description
Explorer	The Explorer feature in NAE analyses a policy snapshot from the Cisco APIC to enable data center operators and architects to: • Explore the ACI object models and associations • Verify connectivity and segmentation between network assets The Explorer feature is based on natural language query interface. The types of queries supported by the feature include What, Can, How, and View.
Schedule Assurance Group Analysis	In this release, 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.
License enhancements	Starting with Cisco NAE 4.0(1), after the expiry of the trial license (30 days after installation), the analysis will stop. Users are urged to request a license as soon as Cisco NAE is installed.
Compliance Enhancements	• Object selectors for Configuration Compliance can be created. • BETA FEATURE: Using the preview link to view the objects that are included or excluded in the object selector is a Beta feature in Cisco NAE Release 4.0(1). To provide Beta feedback on this feature, send your comments to your Cisco account team.
Deny Action support	Standard contracts with deny action are supported.
Policy CAM optimization	For contracts, Policy CAM Optimization is assured by Cisco NAE.

Feature	Description
GUI updates	The GUI updates in this release includes • Consolidation of Search, Visuals, and Dashlets across the NAE GUI. • Consolidation of **Tenant Forwarding**, **Tenant Endpoint**, **Tenant Security** pages to the **Explorer** page. • The **Prefix Communication View** in the Tenant Forwarding page is now available in the **Explorer** page. • **Real-time Change Analysis** page has been renamed to **Policy Analysis**. • **TCAM** page has been renamed to **Policy CAM**.
Global Search	The Global Search feature allows you to search for objects (across multiple epochs). The results of the Global Search appear in the **Smart Event** table, **Tenant Endpoint** table, and the **Prefix** table.
Smart Event Lifecycle	Smart Event Lifecycle tracks every Smart Event across time, and displays the occurrences in a graphical epoch timeline.
Provide the Primary Affect Object (PAO) columns in the Smart Event view of individual events	The PAO feature expands a smart event table row to display additional information about the smart event such as epochs, VRFs, EPGs, BDs, and tenants.
Offline Analysis enhancements	The ability to delete offline analysis is supported in this release.
Remote leaf assurance	Cisco NAE now assures remote leaf.
Cisco APIC 4.1 support	Cisco APIC Release 4.1 is supported by Cisco NAE Release 4.0(1).
Upgrade	Upgrade from Cisco NAE release 3.1(1) to Cisco NAE release 4.0(1) is supported.
New Smart Events	The following smart events were introduced in this release: • Change Analysis smart events (Event code: 3034, 7021, 7022, 7023, 7024, 7025, 7026, 7027, 10070, 10071) • Compliance smart events (Event code: 11048, 11049, 11050, 11051, 11052, 110531, 1054, 11055, 11056) • System smart events (Event code: 60013) • Tenant Endpoint smart events (Event code: 30033, 30034) • Tenant Forwarding smart events (Event code: 6010, 6014) • Tenant Security smart events (Event code: 10057)

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.
- 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 }}
```

Caveats

Open Caveats

This section lists the open caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

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

Table 6. Open Caveats in the Release 4.0(1)

Bug ID	Description
CSCvq75199	When viewing an interface ethernet in Explorer, Smart Events that contain the interface name parameter are also visible.
CSCvq75701	CAN query cannot talk on a filter port query (ICMP/TCP).
CSCvq82544	Epoch timeline does not show updated information after an offline analysis is deleted.
CSCvq99544	Performing a search on Policy CAM related events, results in an error.
CSCvr02870	Passing checks are not displayed in the detailed view for the smart event `APP_EPG_STATIC_PORT_PATH_MAY_NOT_DEPLOY`.

Table 7. Open Caveats in the Release 4.0(1a) and 4.0(1b)

Bug ID	Description
CSCvq75199	When viewing an interface ethernet in Explorer, Smart Events that contain the interface name parameter are also visible.
CSCvq75701	CAN query cannot talk on a filter port query (ICMP/TCP).
CSCvq82544	Epoch timeline does not show updated information after an offline analysis is deleted.
CSCvq99544	Performing a search on Policy CAM related events, results in an error.
CSCvr81155	Cisco NAE leaves snapshot files on APIC after exporting the APIC configuration.

Resolved Caveats

This section lists the resolved caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Resolved Caveats in the Release 4.0(1)

Table 8. Resolved Caveats in the Release 4.0(1)

Bug ID	Description
CSCvn41481	In the **Health Delta** page, performing a search using the Interface filter does not display any search results.

Resolved Caveats in the Release 4.0(1a)

Table 9. Resolved Caveats in the Release 4.0(1a)

Bug ID	Description
CSCvr02870	Passing checks are not displayed in the detailed view for the smart event `APP_EPG_STATIC_PORT_PATH_MAY_NOT_DEPLOY`.

Resolved Caveats in the Release 4.0(1b)

Table 10. Resolved Caveats in the Release 4.0(1b)

Bug ID	Description
CSCvs10499	Upgrading from Cisco NAE release 2.0.1 to release 4.0.1 or 4.0.1a fails.

Known Behaviors

This section lists caveats that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Table 11. Known Behaviors in the 4.0(1) and 4.0(1a) Release

Bug ID	Description
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.
CSCvk36185	Renaming or replacing a filter entry does not show change in epoch health delta.
CSCvo42680	LOG_PERMIT_POLICY_ENFORCED smart event is generated for the actrlRule that has threshold, redir action.
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 rime range.

Related Documentation

The following table describes the Cisco NAE documentation:

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

Table 12. Cisco NAE Documentation

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, please send your comments to cisconae-docfeedback@cisco.com. We appreciate your feedback.