Cisco Network Assurance Engine Release Notes, Release 3.0(1)

Table of Contents

First Published: 2018-11-26

Last Modified: 2019-04-30

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, Release 3.0(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
April 30 , 2019	In the Open Caveats section, added caveat CSCvp52256.
February 13, 2019	In the Usage Guidelines section, added a note about CSCvo18229.
February 12, 2019	3.0(1): Release 3.0(1) became deferred. 3.0(1a): Release 3.0(1a) became available. Added the resolved caveat for this release.
November 26, 2018	Created the release notes for the 3.0(1) 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.

Build Information

There are three models of the Cisco NAE : Small, Medium, and Large. See the *Cisco Network Assurance Engine Getting Started Guide* for information regarding the system requirements for the various appliance models.

Appliance Model: NAE-V500-S

Build ID: 20

Build Time:

February 7, 2019 4:06:53 AM PST

February 7, 2019 12:06:53 PM UTC

Appliance Model: NAE-V1000-M

Build ID: 20

Build Time:

February 7, 2019 4:06:53 AM PST

February 7, 2019 12:06:53 PM UTC

Appliance Model: NAE-V2000-L

Build ID: 20

Build Time:

February 7, 2019 4:06:53 AM PST

February 7, 2019 12:06:53 PM UTC

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
4.0	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

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	200 leaf switches
Number of VMs	3	3	3
TCAM Rules	200 K	400 K	400 K
End Points	50 K	100 K	100 K
Number of Prefix Matches	25 K	50 K	50 K
Number of Concurrent Assurance Analysis	1	1	1
Analysis Interval in ACI Network Mode	15 minutes or more	15 minutes or more	15 minutes or more
Analysis Interval in ACI Application Mode	25 minutes or more	15 minutes or more	15 minutes or more

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)	100

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.

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.

New and Changed Information

New Software Features

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

Feature	Description
Segmentation compliance	Segmentation compliance can be used to set up regulatory compliance rules. With this feature, the user can verify that a set of entities in a walled area cannot communicate with other entities.
Smart Event suppression	Smart event suppression can be used to suppress smart events in the Cisco NAE UI. With this feature, the user can view only the smart events that are relevant.
Policy delta enhancements	The following enhancements were added to the policy delta view: * Policy delta view now includes 3 panels, Changed Policy Object, Policy Viewer, and Audit Log. * The **Changed Policy Object** panel, displays the changed policy object tree across the two epochs. * The **Policy Viewer** panel displays the policy configuration across the earlier and later epochs. * The **Audit Log** panel displays all the audit logs that were created between the two epochs.
Physical Interface View in Tenant Forwarding Visualization	The **Physical Interface View** displays the physical interface health and provides the visual indication of the interface status for any leaf switch in the assurance group.
Prefix Communication View in Tenant Forwarding Visualization (Beta feature)	The **Prefix Communication View** visualization, 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.
Authentication with LDAP	This feature allows administrators to grant access to the Cisco NAE appliance to users configured on externally managed authentication servers such as the Lightweight Directory Access Protocol (LDAP) sever.
Search enhancements	New search filters such as event code, check code, check status, requirement, and requirement set were added in this release.
Highlight primary affected objects	The primary affected objects in a smart event are highlighted enabling you to differentiate if the affected object is primary or secondary.
Large appliance model	Cisco NAE appliance with a scale limit of 200 leaf switches is added in this release
Policy delta support for Cisco APIC release 2.2	Policy delta is supported for Cisco APIC release 2.2 and later versions.

Feature	Description
Cisco APIC 4.0(1)support	Cisco APIC Release 4.0(1) is supported by Cisco NAE Release 3.0(1).
New Smart Events	New Layer 2, VPC, and compliance smart events were introduced in this release. See the *Cisco Network Assurance Engine Smart Events Reference Guide* for more information.

Usage Guidelines

This section lists usage guidelines for the Cisco NAE.

- Cisco NAE Release 3.0(1a) address the vulnerability for CSCvo18229. To fix the vulnerability, you must update the administrator password from the GUI after upgrading from 3.0(1) to 3.0(1a).
- 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.

- The Cisco NAE does not perform any checks for IPv6 prefixes.
- 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.
- The Tenant Forwarding Prefix Communication radial view and Security Enforcement Health radial view will not display the results if there is a large amount of data. In the Prefix Communication view, you can view the results for large amount of data in the tabular view. Use the toggle icons in the top right of the screen to switch between the radial view and the tabular view.

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.

The following table lists the open caveats in the release 3.0(1).

Table 5. Open Caveats in the Release 3.0(1)

Bug ID	Description
CSCvn41481	In the **Health Delta** page, performing a search using the Interface filter does not display any search results.
CSCvn38061	Few compliance smart events may not be suppressed when Event Suppression feature is enabled on compliance events.
CSCvn38061	Few compliance smart events may not be suppressed when Event Suppression feature is enabled on compliance events.
CSCvp52256	INFO events are raised when partial set of checks are performed successfully on an affected object.

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.

The following table lists the resolved caveats in the release 3.0(1).

Table 6. Resolved Caveats in the Release 3.0(1)

Bug ID	Description
CSCvh73136	The Cisco NAE appliance setup can begin even if invalid SMTP port number is used for SMTP configuration.
CSCvk29632	Cisco NAE generates multiple tenant security events with same mnemonic and primary affected objects.
CSCvk40368	Leaf switch name is not available for **System Category** Smart Events.
CSCvk50947	In the **TCAM** page, the number of TCAM utilization smart event does not match the leaf switches in the rule count visualization chart.
CSCvk53143	In the **Tenant Endpoint** details and Smart Events page, IP Filter for IPv6 works only in the compressed format.

The following table lists the resolved caveats in the release 3.0(1a).

Table 7. Resolved Caveats in the Release 3.0(1a)

Bug ID	Description
CSCvo18229	Cisco Network Assurance Engine CLI Access with Default Password Vulnerability.

Cisco NAE Release 3.0(1a) address the vulnerability for CSCvo18229. To fix the vulnerability, you must update the administrator password from the GUI after upgrading from 3.0(1) to 3.0(1a).

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 8. Known Behaviors in the 3.0(1) Release

Bug ID	Description
CSCvi51374	For scale configurations, a few API queries (notably the prefix, TCAM, 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.

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 9. Cisco NAE Documentation

Document	Description
Cisco Network Assurance Engine Release Notes	This document.
Cisco Network Assurance Engine Getting Started Guide	Describes how to install the Cisco NAE and how to use the GUI.
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.

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.