Cisco Network Assurance Engine
Release Notes, Release 2.1(1)

Table of Contents

First Published: 2018-07-28

Last Modified: 2018-04-30

Cisco Network Assurance Engine, Release 2.1(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
July 28, 2018	Created the release notes for the 2.1(1) release.
August 13, 2018	Created the release notes for the 2.1(1a) patch release.
September 14, 2018	Created the release notes for the 2.1(1b) patch release. Added the resolved caveats for this release.
April 30 , 2019	In the Open Caveats section, added caveat CSCvp52256.

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 two models of the Cisco NAE : Small and Medium. 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:70

Build Time:

September 19, 2018 11:51:01 AM PDT

September 19, 2018 6:51:01 PM UTC

Appliance Model: NAE-V1000-M

Build ID:70

Build Time:

September 19, 2018 11:51:01 AM PDT

September 19, 2018 6:51:01 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
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
APIC Fabric Size	50 leaf switches	100 leaf switches
Number of VMs	3	3
TCAM Rules	200 K	400 K
End Points	50 K	100 K
Number of Prefix Matches	25 K	50 K
Number of Concurrent Assurance Analysis	1	1
Analysis Interval in ACI Network Mode	15 minutes or more	15 minutes or more
Analysis Interval in ACI Application Mode	25 minutes or more	15 minutes or more

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
Licensing	Cisco NAE is licensed as an annual subscription with 1-, 3-, and 5-year term options. Use the Cisco NAE to upload a valid license.
Epoch Delta Analysis	Epoch delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two epochs. Policy delta in Epoch Delta Analysis is currently supported for Cisco APIC version 2.3 and later versions.
Export data from GUI	Exporting the data from certain tables in the GUI to JSON and CSV format is supported.
Support for NAT configuration for ACI fabric	Network Address Translation (NAT) deployment is supported. NAT can deployed using using out-of-band management or in-band management interface.
Global Station Table (GST) Assurance	Cisco NAE checks for all the GST entries in the leaf switches and determines the incorrect GST entries.
Local search enhancements	The **Search** bar enables you to filter by objects and then by name or DN to perform a contained search.
ACI 3.2 support	Cisco APIC Release 3.2(1) is supported by Cisco NAE Release 2.1(1).
Context sensitive help	Context sensitive help is now available for the inspector pages in the Cisco NAE appliance.
Cisco NAE appliance documentation	Documentation for the Cisco NAE appliance can be viewed and downloaded from the **Settings** menu.

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.

- 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.

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 4. Open Caveats in the Release 2.1(1)

Bug ID	Description
CSCvh73136	The Cisco NAE appliance setup can begin even if invalid SMTP port number is used for SMTP configuration.
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.
CSCvk29632	Cisco NAE generates multiple tenant security events with same mnemonic and primary affected objects.
CSCvk36185	Renaming or replacing a filter entry does not show any change in the epoch health delta.
CSCvk40368	Leaf switch name is not available for **System Category** Smart Events.
CSCvk48347	If a prefix has both **int** and **ext** next hops, the `TENANT_INTERNAL_SUBNET_RIB_FIB_MISMATCH` may be spurious.
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.
CSCvk53143	In the **Tenant Endpoint** details and Smart Events page, IP Filter for IPv6 works only in the compressed format.
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.

Resolved Caveats in the 2.1(1) Release

The following table lists the resolved caveats in this release.

Table 5. Resolved Caveats in the Release 2.1(1)

Bug ID	Description
CSCvh78357	Details for a single smart event may be split across multiple UI widgets, instead of being consolidated in a single widget.
CSCvh98022	The offline assurance data file can be deleted while the offline analysis is in progress.
CSCvi11448	The bundle file cannot be deleted if the status is **Failed to Delete**, or **Failed to Upload**, or **Upload in Progress**.
CSCvi19770	At times you are unable to log in to the Cisco NAE appliance after session expiry, unless refreshed.
CSCvi42261	Cisco NAE allows you to deploy without specifying all the three IP addresses of the VMs in the cluster leading to a state where the deployment may not function appropriately.
CSCvi47947	In the **Tenant Forwarding** page, the L3 Forwarding table contains more than one entry for the same VRF and PREFIX combination if the exact same internal subnet is defined across multiple BDs and/or multiple L3Outs in the same VRF.
CSCvi47952	In the **Tenant Forwarding** page, the `route_type` is marked as internal, even if there is an exact match between the internal and external subnet.
CSCvi49785	In the **Tenant Forwading** page, the L3 forwarding table fails to load if the page contains a large number of leaf switches and contracts.

Resolved Caveats in the 2.1(1b) Release

The following table lists the resolved caveats in this release.

Table 6. Resolved Caveats in the Release 2.1(1b)

Bug ID	Description
CSCvm06469	Intermittent HTTP 503 errors from API requests and degraded NAE performance.

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 7. 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.