Cisco Network Assurance Engine Release Notes, Release 5.0(1)

Table of Contents

First Published: 2020-07-24

Last Modified: 2021-03-05

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
September 24, 2020	Release 5.0(1a) for Cisco NAE app became available.
July 24, 2020	Release 5.0(1) became available.

New Software Features

New Software Features in Release 5.0(1)

Feature	Description
DCNM Assurance	Cisco NAE now supports the NX-OS data center fabric deployments along with 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.
Cisco NAE app	Cisco NAE app is available to be deployed on Cisco Application Services Engine.
TACACS+ support	Administrators can grant access to Cisco NAE appliance to users configured on externally managed authentication servers such as the Terminal Access Controller Access Control System Plus (TACACS+) server.
Historical Data Import and Export	Historical Data Import and Export feature enables a super administrator to import epoch data from a remote location or export epoch data to a remote location for ACI and NX-OS fabrics.
Smart Licensing enhancements	Orchestrator license is no longer required for Cisco NAE.
Pre-Change Analysis	The user can perform Pre-Change Analysis for supported Fabric Access Policies using JSON or XML upload files.
Increase Compliance scale	The user can configure Segmentation Compliance rules with a tenant object selector.
TCAM compression and optimization support	TCAM compression entries are listed in the Cisco NAE Policy CAM screen dashlets.
Compliance for Naming Conventions	Compliance for Naming Conventions is supported.
Configuration Compliance Containment Check	You can perform a configuration compliance containment check against a specified configuration.
Cisco APIC 5.0 support	Cisco APIC Release 5.0 is supported by Cisco NAE Release 5.0(1).

Feature	Description
New Smart Events	The following smart events were introduced in this release: • CHANGE_ANALYSIS: (3090, 90001-90010, 90020-90030) • COMPLIANCE: (11058, 11059, 11060, 11065) • SYSTEM: (50014, 50015, 50018, 50032-50038, 600011-600018) • TENANT_FORWARDING: (90040-90043)
Smart Events deprecated	The following smart event were deprecated in this release: • CHANGE_ANALYSIS: (7028)
New API commands	The following API commands for Pre-Change Analysis operations were added. • Create a Pre-Change Analysis Using a JSON/XML Configuration File • Get a Pre-Change Analysis Job • Get All Pre-Change Analysis Jobs • Delete a Pre-Change Analysis Job • Get Pre-Change Analysis Configuration JSON
New API command prefix requirement	REST API commands must have the prefix `/nae/api/v1`. In previous releases, the `/nae/` segment was optional.

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
CSCvu21980	Cisco NAE does not detect overlapping external subnet with BD subnet.	5.0(1)
CSCvu67993	In some cases, the smart event `VPC_DOMAIN_INCONSISTENT` displays configuration status as **Invalid**. Check the smart event `VPC_PARAMETERS_INCONSISTENT` for more information.	5.0(1)
CSCvu60329	Using the API `allow_unsupported_object_modification is true` for a PCA job, may result in false positive or negative smart events.	5.0(1)
CSCvu81037	Cisco NAE raises the incorrect warning level smart events on port channels (PC) and virtual port channels (vPC) that are used for L3Out under certain conditions.	5.0(1)
CSCvu32911	When there is a vPC type-2 mismatch in Interface-VLAN routing and Output Queuing parameters, Cisco NAE does not generate `VPC_DOMAIN_INCONSISTENT` smart event.	5.0(1)
CSCvu77756	When there is a mismatch in vPC Output-Queuing type-2 parameter, Cisco NAE does not generate `VPC_PARAMETERS_INCONSISTENT` smart event.	5.0(1)
CSCvv11505	When you perform a search by pasting the value in the search field, the value is pasted twice.	5.0(1)
CSCvv08622	If you apply the severity filter on the search field and access the Event page from the prefix table, the event table does not display any results.	5.0(1)
CSCvv098715	Performing a search for subnet or route in Global Search or Event Suppression page does not display the results in the events table. The results are displayed in the prefix table.	5.0(1)
CSCvv08248	Download option for PCA jobs with tenant configuration size exceeding 8KB is disabled.	5.0(1)

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
CSCvq75199	When viewing an interface ethernet in Explorer, Smart Events that contain the interface name parameter are also visible.	5.0(1)
CSCvs72114	Configuration compliance for EPG raises a verified smart event even if the corresponding EPG does not have an attribute.	5.0(1)
CSCvu02174	Cisco NAE REST API Swagger Interface does not contain information for all the published REST APIs for Cisco NAE.	5.0(1)
CSCvv84144	Mismatch between Cisco NAE app version displayed in the **Appliance Administration** GUI on the Cisco NAE app and on the Cisco Application Services Engine Apps GUI.	5.0(1a)

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.	5.0(1) and later
CSCvk36185	Renaming or replacing a filter entry does not show change in epoch health delta.	5.0(1) and later
CSCvo42680	LOG_PERMIT_POLICY_ENFORCED smart event is generated for the actrlRule that has threshold, redir action.	5.0(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.	5.0(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.
- 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

Software Compatibility Information

The following tables list 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 Fabric Compatibility Information

Cisco APIC Release	Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches
5.0	15.0
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

Table 2. Cisco NX-OS Fabric Compatibility Information with DCNM Assurance Group

Cisco DCNM Release	Cisco Nexus 9000 Series NX-OS	Switch Support	Topology and Deployment
11.3.1 11.4.1	9.3(3)	The 9300-EX, -FX, -FX2, and -GX platform switches and the 9500 platform switches with -EX and -FX line cards are supported.	BGP eVPN VXLAN topology and deployments are supported

Supported Load Balancers

The following table lists the supported load balancers for the Cisco NAE. (Currently, this is supported for ACI Assurance Group only.)

Table 3. 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 for ACI Fabric

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

Table 4. 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 5. 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 the 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, only 50 tenants are supported, and the option to enable the aggregate info events will be present only for Segmentation requirements using a tenant object selector. If the option is enabled, there will no longer be any info events for EPG pairs, and only EPG pair-based violation events will be generated.
Fabric wide rules	150 K

Table 6. Verified Scalability Limits for Explorer

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

Verified Scalability Limits for NX-OS Fabric

The following tables lists the maximum verified scalability limits.

Table 7. Verified Scalability Limits for Cisco NAE with Cisco NX-OS Fabric

Feature	Cisco NX-OS Fabric Scale Limits
System Routing Template	Default
VXLAN VTEPs	38
VXLAN Layer 2 VNIs	2,000
VXLAN Layer 3 VNIs/VRFs	900
VXLAN Multicast Groups	100
VXLAN Overlay MAC Addresses	64,000
VXLAN Overlay IPv4 Host Routes	60,000
VXLAN Overlay IPv6 Host Routes	16,000
VXLAN Overlay IGMP Snooping Groups	800
VXLAN IPv4 LPM Routes	2,264
VXLAN IPv6 LPM Routes	2,256
VLANs on VTEP Node	2,900 (Total VLANs)
STP Logical Ports	2,900
VPC Port Channels	32
Underlay IS-IS Neighbors	11
Underlay PIM Neighbors	9 (Spine switches), 3 (Leaf switches)

Table 8. Verified Scalability Limits for OVA Deployment

Feature	Scale Limit for Appliance Model: Small	Scale Limit for Appliance Model: Medium
Cisco NX-OS Fabric Size	40 leaf switches	100 leaf switches
Number of VMs	3	3
Number of Prefix Matches (LPM routes)	4,500	4,500
IPV4/IPv6 Host	See the scales in **Verified Scalability Limits for Cisco NAE with Cisco NX-OS**.	See the scales in **Verified Scalability Limits for Cisco NAE with Cisco NX-OS**.
Layer 2 MAC Addresses	**See table ABOVE**	**See table ABOVE**
Total Number of Smart Events, Endpoints, and Prefixes	16,000	16,000
Number of Concurrent Assurance Analysis	1 concurrent and 4 scheduler serial	1 concurrent and 4 scheduler serial

Feature	Scale Limit for Appliance Model: Small	Scale Limit for Appliance Model: Medium
Analysis Interval	15 minutes or more	15 minutes or more

Table 9. Verified Scalability Limits for Explorer

Feature	Scale Limit
Total number of associations that can be explored	500,000

Licensing Information

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

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