Cisco Network Assurance Engine Getting Started Guide, Release 3.1(1)

Table of Contents

Cisco Network Assurance Engine . . . 3

Overview . . . 3

Architecture . . . 5

Management and Network Connectivity . . . 6

Assurance Control Modes . . . 10

Installation Requirements . . . 12

System Requirements . . . 12

Hypervisor Requirements . . . 12

Supported Browsers . . . 13

Compatibility Information . . . 14

ACI Features Assured by Cisco NAE . . . 15

Service Graphs Are Not Assured . . . 17

Verified Scalability Limits . . . 18

Increasing Disk Size . . . 20

Installing Cisco Network Assurance Engine . . . 21

Prerequisites . . . 21

Installation and Initial Configuration Workflow . . . 21

Installing the Cisco NAE OVA . . . 21

Setting Up the Cisco NAE Appliance . . . 23

Editing Time Configuration for a Host . . . 24

Uploading A Certificate Authority Signed Certificate . . . 25

Performing Online Analysis . . . 26

Performing Offline Analysis . . . 28

Cisco Network Assurance Engine Licensing . . . 30

Cisco NAE License . . . 30

Updating License . . . 30

Cisco Network Assurance Engine GUI . . . 32

Overview of the GUI . . . 32

Cisco NAE GUI Icons . . . 33

Settings Menu . . . 35

Timeline . . . 35

Summary Boards Area . . . 37

Hot Topics Area . . . 38

Search . . . 39

Visualization Area . . . 39

Tenant Endpoint Details Area . . . 43

Smart Events Area . . . 43

Exporting Data from the GUI . . . 44

Epoch Delta Analysis . . . 46
Epoch Delta Analysis . . . 46
Guidelines and Limitations . . . 47
Creating Epoch Delta Analysis . . . 47
Viewing Delta Analysis Results . . . 48
Viewing Health Delta Analysis . . . 48
Viewing Policy Delta Analysis . . . 49
Compliance Analysis . . . 51
Compliance Analysis Tab . . . 51
Manage Compliance Requirements . . . 52
Manage Compliance Requirements Tab . . . 52
Creating EPG Selector . . . 52
Creating Traffic Selector . . . 53
Creating Compliance Requirement . . . 54
Creating Compliance Requirement Set . . . 55
Smart Event Management . . . 57
Smart Event Suppression . . . 57
Smart Event Suppression Workflow . . . 57
Creating New Event Rule . . . 59
Creating New Event Ruleset . . . 59
Cisco Network Assurance Engine User Access and Authentication . . . 61
User Access and Authentication . . . 61
Creating a User Account . . . 61
Prerequisites for LDAP . . . 61
Creating a New Authentication Domain . . . 62
Managing Cisco Network Assurance Engine . . . 64
Managing User Accounts . . . 64
Managing Passphrase . . . 64
Managing Appliance Settings . . . 65
Managing Assurance Groups . . . 66
Setting Log Levels . . . 66
Deleting Bundle File . . . 67
Managing Epoch Delta Analysis . . . 67
Managing Authentication Domains . . . 67
Managing EPG Selectors . . . 68
Managing Traffic Selectors . . . 68
Managing Compliance Requirements . . . 69
Managing Compliance Requirement Sets . . . 69
Managing Event Rules . . . 70
Managing Event Rulesets . . . 70
Upgrading and Downgrading Cisco Network Assurance Engine . . . 72

- Supported Upgrade Paths for Cisco NAE 72
- Upgrading Cisco NAE OVA 72
- Creating VM Snapshots 73
- Downgrading Cisco NAE 75

Troubleshooting 76

- Downloading Logs 76
- Appliance Events 76
- Appliance Event Types 76
- Troubleshooting Scenarios 79

First Published: 2019-03-31

Last Modified: 2020-07-06

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)

© 2017-2020 Cisco Systems, Inc. All rights reserved.

Cisco Network Assurance Engine

Overview

The Cisco Network Assurance Engine (NAE) software provides operators with a new approach to manage SDN-based data centers confidently. The Cisco NAE software 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 software 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.

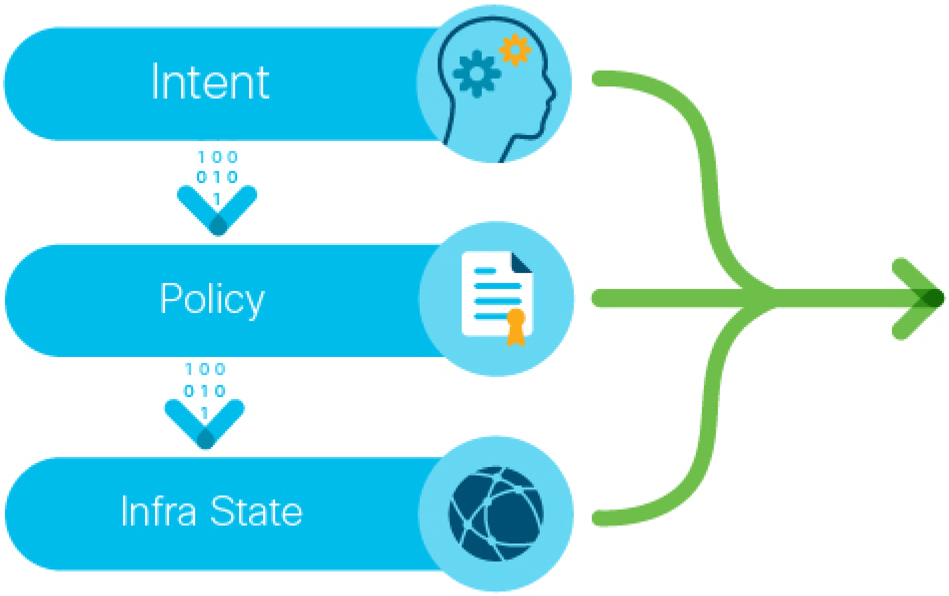

Figure 1. Taking the intent, policy, and the infra state from a device

Figure 2. Network-wide model of the underlay, overlay, and virtualization layers

Leveraging formal mathematical techniques and a deep understanding of the networking domain, the Cisco NAE software is able to answer three fundamental questions about the network:

1. How do I guarantee that I have not introduced errors into the fabric while specifying my policy and configuration?
   - In SDN networks, the impact of a misconfiguration is amplified with centralized automation
   - With increased frequency of changes, misconfigurations are much more common
2. How do I understand the actual current state of the network?
   - Dynamic events (protocol learning, VM mobility, and so on) can make the network deviate from the intended state
   - Central intent has to be propagated to multiple nodes in a large distributed system; consistency issues are unavoidable in such systems
   - With multiple abstraction layers in SDN networks, manually inspecting and reconstructing the network state and configuration has become prohibitively challenging
3. How do I rapidly diagnose the network for the root cause when issues arise?
   - How do I identify these lingering issues before they impact the application?
   - How do I reduce the cost of downtime?

By proactively running this broad set of checks on the network model and providing deep visibility across the fabric, the Cisco NAE software transforms the operating mode from reactive to proactive. The Cisco NAE software enables operators to predict network outages and vulnerabilities before they impact business, reduce risk while accelerating changes and migrations, and rapidly find the root cause of problems. With a complete diagnostic record and compliance rules, operators can ensure continuous compliance and easily satisfy audits.

Architecture

The Cisco NAE can be deployed as a cluster of three virtual machines. The main components include:

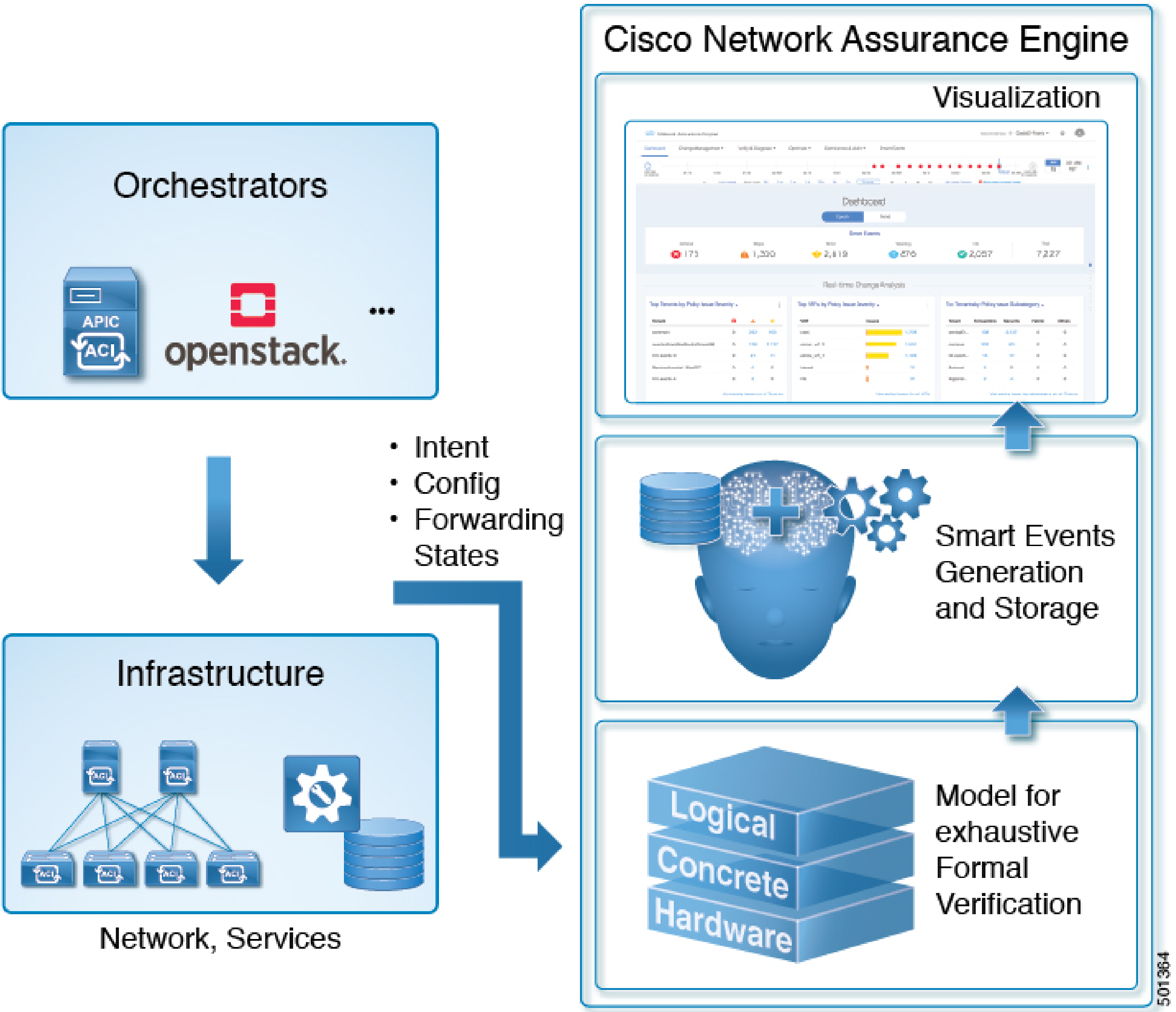

Figure 3. Cisco NAE Architecture

- Data collection—The data collection components are responsible for discovering the ACI fabric comprising of the APIC controllers, spine switches, and leafs switches. Data collection components also polls the discovered fabric to collect APIC logical model and switch concrete model data via REST API interface. The forwarding tables stored in the switch hardware memory such as TCAMs are collected using the SSH interface.
- Formal Modeling—The formal modeling component uses mathematical based techniques to determine if the intent specified in the Cisco ACI policy has been met.
- Smart Events— The results of the formal modeling are generated as **Smart Events** and they are displayed in the Events tab in the GUI.
- Visualization— A graphical representation of the analysis performed by the Cisco NAE and the information generated by the Cisco NAE is displayed in the **Visualization** area of the GUI. The visualization area is a powerful tool for quickly discovering problems with network nodes and

configuration, and viewing a detailed view of each issue.

Management and Network Connectivity

The Cisco NAE can be deployed as a cluster of three virtual machines.

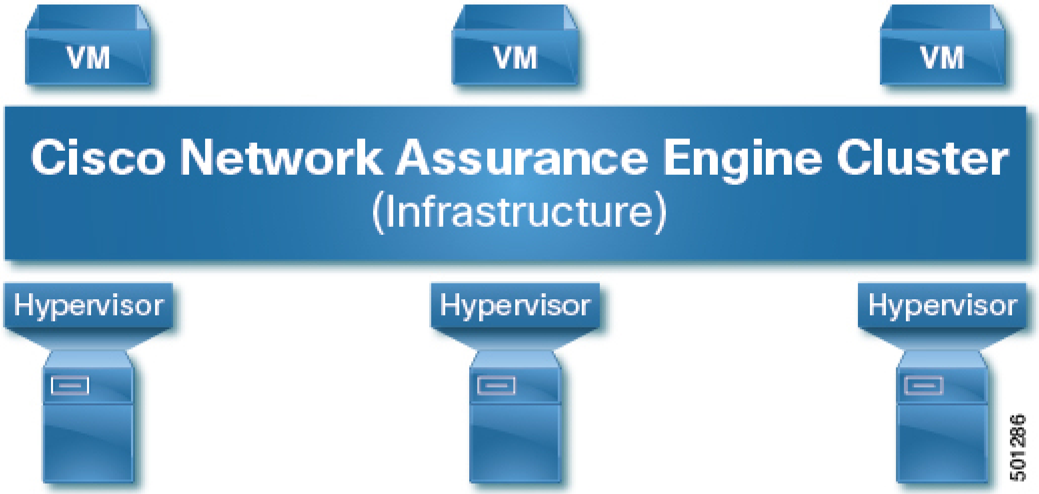

Figure 4. Cisco NAE Appliance

Cisco NAE can be deployed using the following design options to access the management network of the Cisco ACI fabric.

- Out-of-band management interface
- In-band management interface

Starting from Cisco NAE release 2.1(1), Network Address Translation (NAT) deployment is supported. NAT can deployed using using out-of-band management or in-band management interface.

By default, out-of-band management interface will be used to access the management network of the Cisco ACI fabric. If out-of-band management interface is not configured, then in-band management interface will be used. If both out-of-band management interface and in-band management interface are configured, then out-of-band management interface will be used.

Out-of-Band Management Access

In out-of-band management access (OOB), the Cisco NAE appliance can access the ACI fabric on the out-of-band network. We recommend that you use out-of-band management access to connect the Cisco NAE to the ACI fabric.

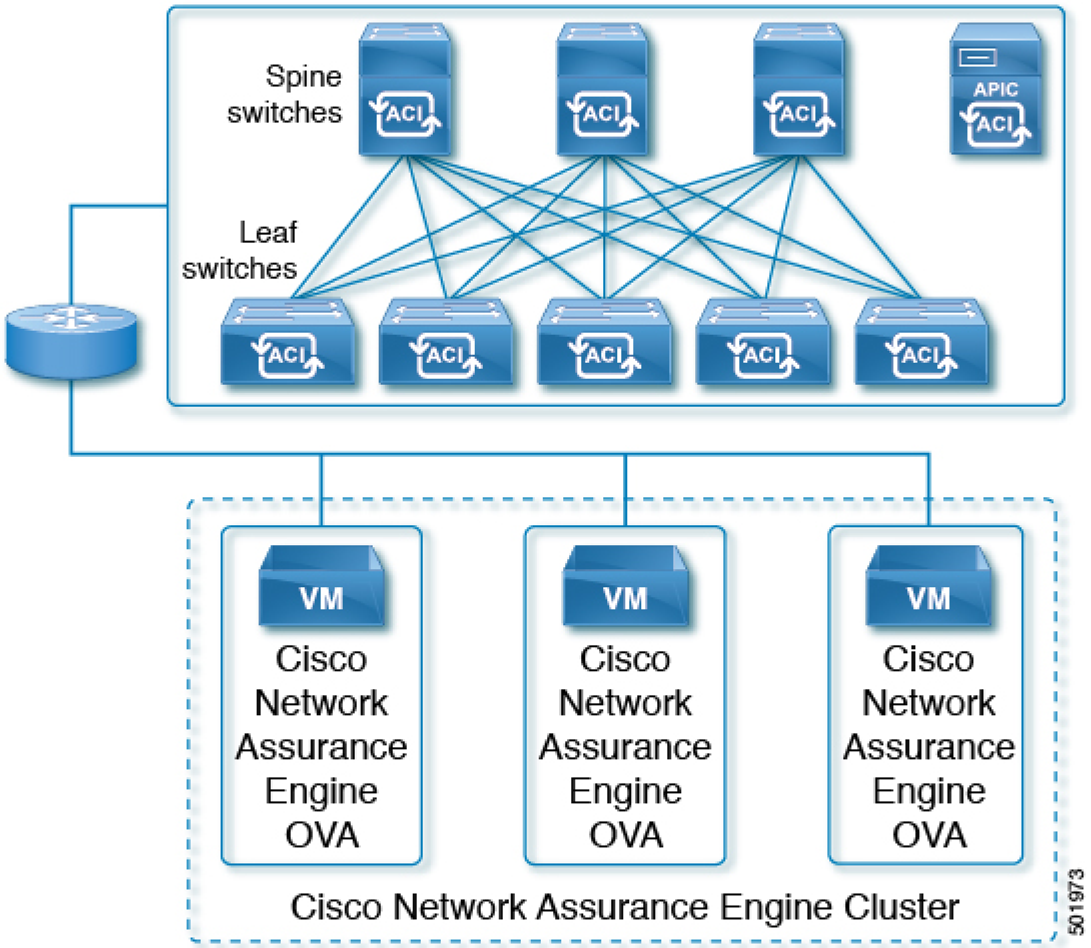
Spine switches
APIC
ACI
Leaf switches
VM
Cisco Network Assurance Engine OVA
Cisco Network Assurance Engine Cluster
501973

Figure 5. Out-of-Band Management Access

In-Band Management Access

In in-band management access, the Cisco NAE appliance will use the leaf switches for in-band access to the ACI fabric.

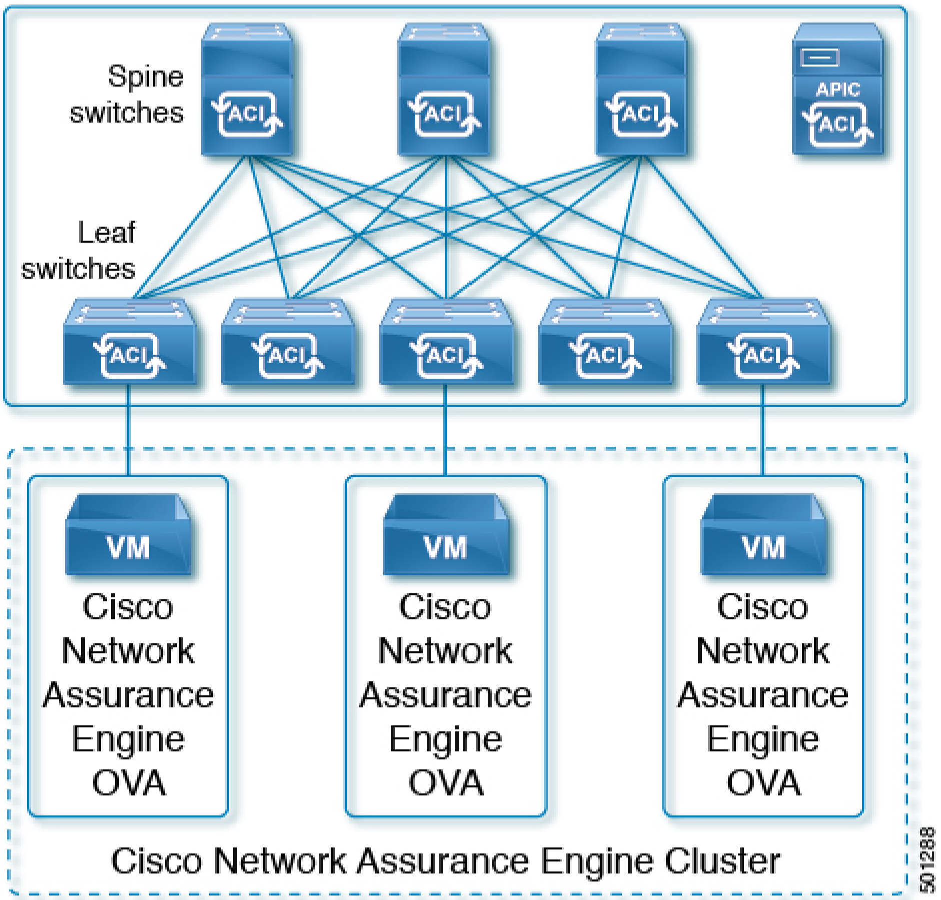
Spine switches
ACI
ACI
ACI
APIC
ACI
Leaf switches
ACI
ACI
ACI
ACI
ACI
VM
Cisco Network Assurance Engine OVA
VM
Cisco Network Assurance Engine OVA
VM
Cisco Network Assurance Engine OVA
Cisco Network Assurance Engine Cluster
501288

Figure 6. In-Band Management Access

Network Address Translation (NAT) Deployment

Starting from Cisco NAE release 2.1(1), Cisco NAE can access ACI fabric deployed across the NAT boundry. In this topology, Cisco NAE communicates with Cisco APIC through NAT.

The following deployment options for NAT are supported:

- NAT with out-of-band management interface

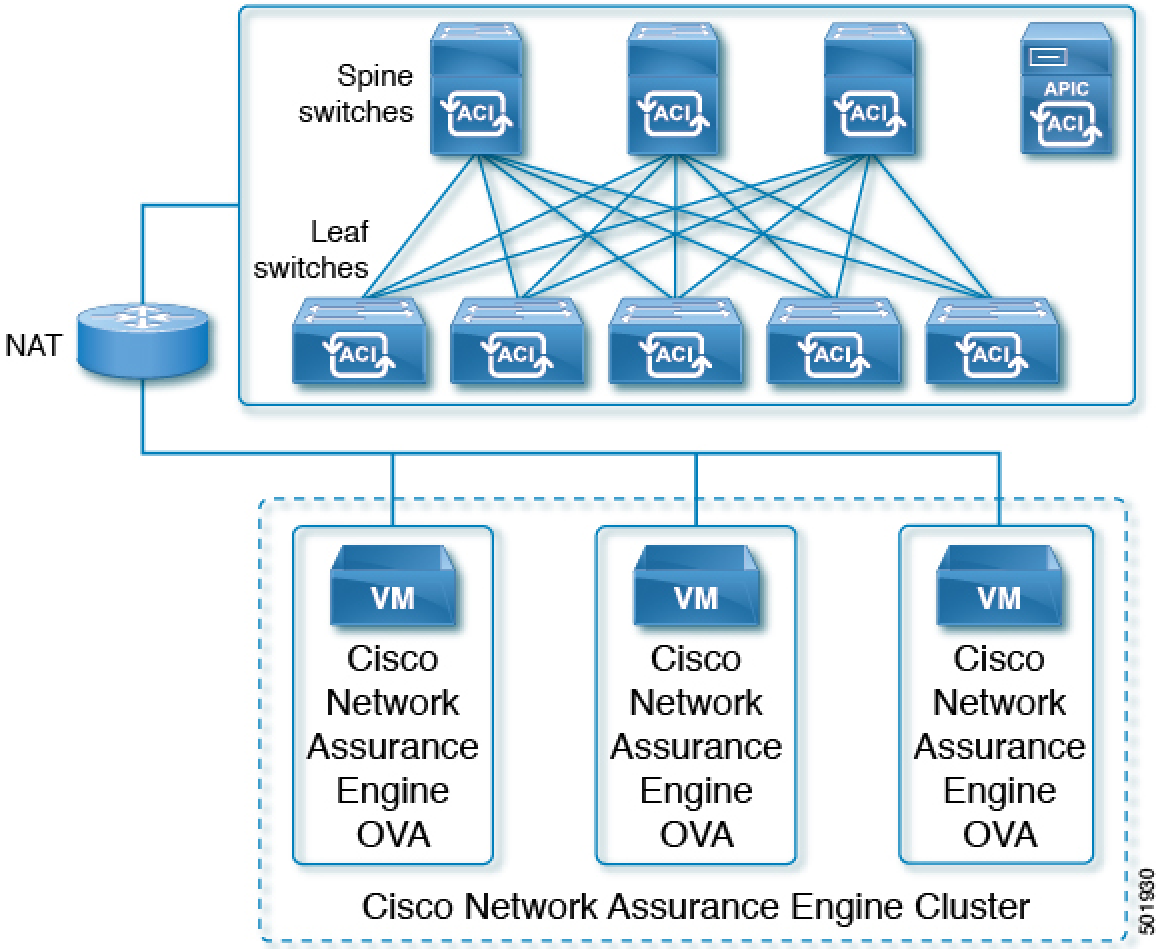
Spine switches
ACI
ACI
ACI
APIC
ACI
Leaf switches
ACI
ACI
ACI
ACI
ACI
NAT
VM
Cisco Network Assurance Engine OVA
VM
Cisco Network Assurance Engine OVA
VM
Cisco Network Assurance Engine OVA
Cisco Network Assurance Engine Cluster
501930

Figure 7. NAT with Out-of-Band Management Access

- NAT with in-band management interface

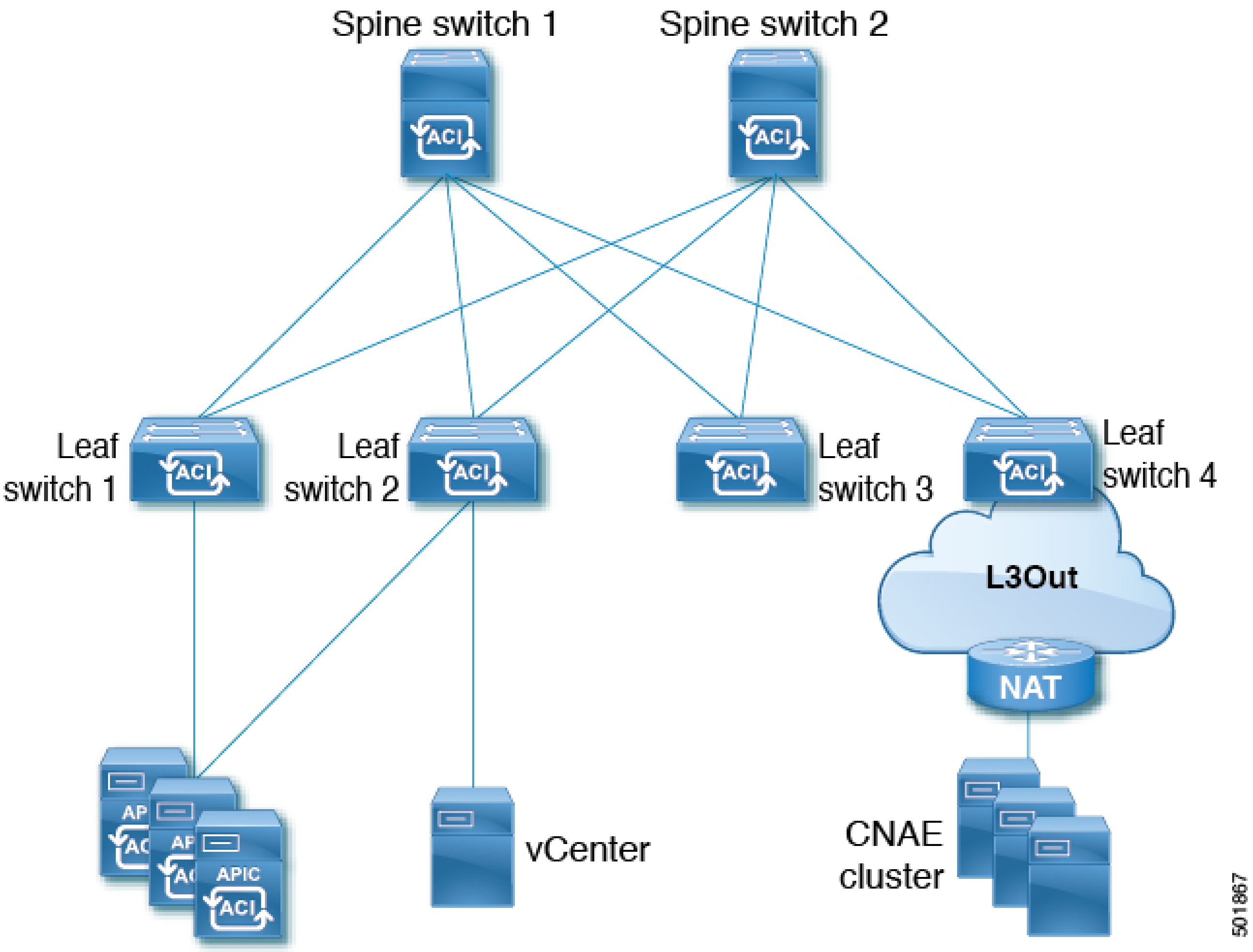

Figure 8. NAT with In-Band Management Access

Important Notes

- For Cisco NAE deployment behind NAT, there should not be any overlaps between out-of-band subnets and in-band subnets in the network.
- Ensure that in-band and out-of-band IP addresses are routable for Cisco NAE to access the ACI fabric.

Assurance Control Modes

Cisco NAE assurance control capability enables you to analyze the Assurance Group in two modes, online analysis and offline analysis. An Assurance Group contains all the network nodes that should be analyzed together. Assurance control involves collecting data from the Assurance Group, running the analysis to create a model with the collected data, and generating the results. The results are then displayed on the **Dashboard**.

Online analysis provides assurance on the Assurance Group in real time. In online analysis data collection, model generation, and results generation are carried out simultaneously. In the online mode the collected data is analyzed immediately after collection followed by result generation. This is repeated after at a fixed time interval as specified by the operator.

Offline analysis provides a one-time assurance of the Assurance Group. Offline analysis offers the flexibility of decoupling the data collection stage from the analysis stage. In offline analysis data is collected using a Python script and the collected data is then uploaded to Cisco NAE to provide one-time assurance. The collected data can also be analyzed at any later point in time. It enables the operator to collect the data during change management windows and then perform the analysis. It also fulfills compliance requirements of an organization.

Installation Requirements

System Requirements

There are three models currently shipping with Cisco NAE: Small, Medium, and Large. The following tables identify the system requirements for installing the Cisco NAE.

Table 1. System Requirements

Requirement	Appliance Model: Small	Appliance Model: Medium	Appliance Model: Large
Model	NAE-V500-S	NAE-V1000-M	NAE-V2000-L
Virtual Machines	3 VMs	3 VMs	3 VMs
CPU (vCores per VM)	8	12	24
Memory (GB per VM)	40	64	96
Disk	1 TB in total per VM	2 TB in total per VM	4 TB in total per VM
Storage	SSD	SSD	SSD
APIC Fabric Size	50 leaf switches for a 3 VM cluster	100 leaf switches for a 3 VM cluster	400 leaf switches for a 3 VM cluster

Important Notes

- Starting from release 3.0(1), HDD storage is not supported.
- In a production environment, the supported and required configuration for Virtual Disks is to use Thick Provision. In the Lab environment if you have configured the Cisco NAE appliance using Thin Provision, you must not use the same appliance in the production environment.
- The recommended Intel processor for vCPUs mentioned in the table System Requirements is Intel® Xeon® CPU E5-2697A v4 @ 2.60GHz, or later.
- For a particular Cisco NAE model, the disk space required depends on the retention period of the epoch data. To increase the disk size, See Increasing Disk Size.
- The IOPS performance numbers for storage system SSDs tested are as follows:
  - Sequential Read (up to) 550 MB/s
  - Sequential Write (up to) 500 MB/s
  - Random Read (100% Span) 84000 IOPS
  - Random Write (100% Span) 27000 IOPS
  - Read/Write Latency: < 70 µs

Hypervisor Requirements

Requirement	Description
VMware vSphere	ESXi 5.5, 6.0, 6.5, 6.7

Important Notes

- VMware Virtual Machine File System (VMFS5) datastore is required for VMware vSphere.
- Download the Cisco NAE software image based on the Cisco NAE appliance model type and the VMware vSphere version. For ESXi version 5.5, use the Cisco NAE software image for VMware vSphere version 6.0.

For example, to install Cisco NAE, Release 2.0(1b) software, for appliance model small and for VMware version ESXi version 5.5, download the image `cisco_nae_v500_s2_k9-2.0.1b_6.0-install.zip`.

Supported Browsers

- Chrome

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

ACI Features Assured by Cisco NAE

The following section lists the ACI features assured by the Cisco NAE.

Supported Fabric Deployment Options

- Stretched Fabric
- Multipod

ACI Mode

- Network Mode
- Application Mode

APIC Policy

- Networking Policy
- Security Policy
- Access Policy

Tenancy

- Multi Tenant
- Application Profile
- Endpoint Group (EPG)
- Bridge Domain
- Virtual Routing and Forwarding (VRF)
- Contract and Filters
- IPv4 support
- IPv6 support

EPG

- Application EPG
- External L3Out EPG
- Contract Preferred Group

Access Domain Profile

- Physical
- L3Out

Smart Event Use Cases

- Real Time Change Analysis

- Tenant End Points
- Tenant Forwarding
- Tenant Security
- TCAM Optimization

APIC Connectivity to Cisco NAE

- Out-of-Band Management (OOB)
- In-Band Management
- Network Address Translation (NAT)

ACI Features Not Supported by Cisco NAE

The following ACI features are not supported by the Cisco NAE

- Cisco ACI Multi-Site
- Microsegmentation
- GOLF
- Remote Leaf
- vPOD
- Specifying deny action while associating a filter with a subject in a standard contract
- Intra-EPG contracts
- Service Graphs (To get further details, see Service Graphs Are Not Assured.)
- Contract Inheritance

Service Graphs Are Not Assured

Service graphs are not assured by Cisco NAE. With the introduction of the current Cisco NAE release, spurious smart events will not be raised if an ACI fabric setup fulfills ALL of the following requirements:

- A service graph template must have route redirect enabled.
- Only a single service node is supported, and the service node must be in the GoTo mode Function Type under the Function Node properties.
- If the **threshold-redir** command is used, the threshold down action must be set to **permit**.
- The direct connect option for service graphs is not supported, therefore the value must be set to **False**.
- The set of provider/consumer BDs must not overlap with the set of shadow EPG BDs. Additionally, every shadow EPG must have its own BD.
- The provider EPG and the consumer EPG must be one of the following types: an L3Out InstP, an application EPG, or a vzAny.
- In a transit-routing case with a PBR contract, the provider L3Out and consumer L3Out must be different L3Outs.
- There must be a single service graph per contract, and the service graph must be bi-directional.
- The must be no filters set on function node connectors under the service graph template.
- Only one service graph per contract is supported.
- Subnets on logical interface contexts are not supported.

ℹ Inter-VRF service graph support is a beta feature in this release. `UNSUPPORTED_SERVICE_CHAINING_FEATURE_DETECTED` will not be raised for inter-VRF service graph feature.

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
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	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

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.

Increasing Disk Size

Use this procedure to increase the disk size of the Cisco NAE VM in VMware vShphere.

Procedure

1. Log in to Cisco NAE.
2. Choose **Settings** > **Assurance Group Configuration**.
3. Select the Assurance Group and click the stop icon to stop the analysis.
4. Log in to VMware vSphere (or vCenter) Client.
5. Select the Cisco NAE VM.
6. From the **Actions** menu, choose **Power** > **Shut Down Guest OS** to shut down the VM gracefully.
7. Choose **Edit Settings** > **Virtual Hardware** > **Hard Disk 2**.
8. Enter the desired disk size.
9. Click **OK**.
10. Repeat steps 5-9 for all the 3 VMs.
11. From the **Actions** menu, choose **Power** > **Power On** to power on the VM.
12. Power on all the 3 VMs.
13. To verify, log in to Cisco NAE. Choose **Settings** > **Appliance Administration**.
14. The disk usage is displayed in the **Assurance Data Controls** tile.

> ⚠ Decreasing the disk size is not supported and may result in complete loss of data and/or the Cisco NAE appliance. As a result, you may have to reinstall the appliance. We recommend that you increase the disk size gradually.

Installing Cisco Network Assurance Engine

Prerequisites

- You have installed the Python version 2.7.11 or later to perform offline analysis.
- You have the IP addresses, subnet mask, and gateway information for the Cisco NAE appliance.
- You have the IP addresses of the primary and secondary DNS server.
- You have the IP addresses of the primary and secondary NTP server.
- You have the credentials for the SMTP server.
- Ensure that ports 443 and 22 are open for HTTPS and SSH communication between the Cisco NAE and the APIC.
- Cisco NAE VMs should have unrestricted communication between them, preferably in the same VLAN.

Installation and Initial Configuration Workflow

Installation and initial configuration of the Cisco NAE includes the following steps:

1. Installing the Cisco NAE OVA. See Installing Cisco NAE OVA.
2. Setting up the Cisco NAE appliance. See Setting Up Cisco NAE Appliance.
3. Performing analysis on the Assurance Group in online mode or offline mode.
    a. To perform online analysis, see Performing Online Analysis.
    b. To perform offline analysis, see Performing Offline Analysis.
4. Configure local users or configure authentication domains .
    a. To configure local users for accessing the Cisco NAE appliance, see Creating a User Account.
    b. To configure authentication domains, see Creating a New Authentication Domain.

Installing the Cisco NAE OVA

Use this procedure to install the Cisco NAE OVA.

Before You Begin

- You need administrator privileges to connect to VMware vSphere or vCenter.
- You have the Cisco NAE OVA image. The OVA image set contains a set of OVAs for the different appliance flavors. You will receive the OVA for the appliance flavor based on the license you purchased.
- You have the IP address, subnet mask, and gateway information for the Cisco NAE appliance.

Procedure

1. Log in to VMware vSphere (or vCenter) Client.
2. In the **Navigation** pane, choose the **Data Center** for deployment.
3. Choose **File** > **Deploy OVF Template**. The **Deploy OVF Template** window appears.
4. In the **Source** pane, browse to the location, choose the file, and click **Open** to choose your OVF source location.
5. In the **OVF Template Details** pane, verify the details and click **Next**.
6. In the **End User License Agreement** pane, read the license agreement and click **Accept**.
7. In the **Name and Location** pane, do the following:
   a. (Optional) In the **Name** field, enter the VM name.
   b. Choose the **Inventory** Location where the Cisco NAE is being deployed and click **Next**.
8. In the **Host/Cluster** pane, choose the required cluster and click **Next**.
9. In the **Storage** pane, choose the location in which to store virtual machine files.
10. In the **Disk Format** pane, enter the data store and the required space for the appliance.
11. In the **Disk Format** pane, click the **Thick Provision** button, and click **Next**.

    ℹ In a production environment, the supported and required configuration for Virtual Disks is to use Thick Provision. In the Lab environment if you have configured the Cisco NAE appliance using Thin Provision, you must not use the same appliance in the production environment.

12. In the **Properties** pane, provide the following information and click **Next**:
    - IP Address
    - Subnet Mask
    - Gateway
13. In the **Ready to Complete** pane, verify the options selected and click **Finish**.
14. Reserve all of the memory allocated to each virtual machine to avoid performance issues.
15. Edit VM settings to setup disk 1 on a different physical datastore than disk 2.
16. Power on the VM.
17. Cisco NAE virtual appliance is deployed as a cluster of three virtual machines. Repeat the steps to deploy the remaining virtual machines in the cluster.

    ℹ You must perform the installation on one VM at a time. Do not perform the installation on all 3 VMs simultaneously.

18. After the three virtual machines boots up, copy and paste the Cisco NAE IP address that appears into a supported web browser to access the Cisco NAE Login page.

Setting Up the Cisco NAE Appliance

The Cisco NAE virtual appliance is deployed as a cluster of three virtual machines. Use this procedure to set up your administrator profile, configure DNS, NTP, and SMTP server, and add virtual machines for fabric configuration.

Before You Begin

- You have the IP addresses of the virtual machines.
- You have the IP address of the primary and secondary DNS server.
- You have the IP address of the primary and secondary NTP server.
- You have the host name of the SMTP server.

Procedure

1. Use the Cisco NAE IP address obtained from the procedure Setting Up Cisco NAE Appliance to access the Cisco NAE Login page.
2. Log in to the Cisco NAE. The **Appliance Setup** form appears.
3. Complete the following fields for **Administrator Profile**.
   a. Enter the email address.
   b. Enter the password and enter the password again to confirm.
4. Complete the following fields for **Cluster Configuration**.

> You must add at least three virtual machines to the cluster. The IP address of the Virtual Machine 1 is pre-populated. Ensure that each of these VMs are reachable before clicking Submit, and power must remain on during installation.

a. Click + to add Virtual Machine 2 to the cluster and enter the IP address of the virtual machine.
b. Click + to add Virtual Machine 3 to the cluster and enter the IP address of the virtual machine.

5. Complete the following fields for **DNS Server**.

DNS servers are configured for hostname resolution. Cisco NAE validates the reachability of the DNS servers. You must specify at least one DNS server.

a. Enter the IP address of the primary DNS server.
b. (Optional) Enter the IP address of the secondary DNS server.

6. Complete the following fields for **NTP Server**.

NTP servers are configured to synchronize time. Cisco NAE validates the reachability of the NTP servers. For configuring remote NTP server, you must specify at least one NTP server.

> ℹ Cisco NAE uses local NTP service to ensure all the VMs in its cluster have synchronized time. The time source for local NTP service can be an external NTP server or the local VM time of the primary VM in the cluster. We recommend that you use the external NTP server option in a production environment as time source rather than local VM time of primary VM. It is highly recommended that you set time correctly during the installation of the appliance via external NTP server or at the host of the VM used for installation. Setting time back or in future in the appliance VMs or in the host post installation is not supported and can result in unpredictable behavior including but not limited to loss of data in some scenarios. If you need to set time back post installation then the supported method is to re-install the appliance and set time correctly.

a. Check **Use External NTP Server** check box to configure external NTP server.
   i. Enter the domain name of the primary NTP server.
   ii. (Optional) Enter the domain name of the secondary NTP server.

b. Uncheck **Use External NTP Server** check box to configure the local NTP. See Editing Time Configuration for a Host.

7. Complete the following fields for SMTP server.

Cisco NAE appliance leverages email as the mechanism for password recovery. SMTP Server configuration is required for password recovery.

> ℹ We strongly recommended that you configure the SMTP server information, since it is required by the admin for password recovery.

a. Enter the host name of the SMTP server.

b. Enter the port number. Examples include common default ports, SMTP port number 25, or secure SMTP (SSL) port number 465.

c. (Optional) Check the **SSL** check box to configure SSL for SMTP.
   i. Enter the username and password to access the SMTP server.

8. Click **Submit**. The **Summary Configuration** page is displayed. It may take approximately 10 minutes for the **Summary Configuration** to be displayed.

9. Verify the configuration and click **Launch Cisco Network Assurance Engine**.

Editing Time Configuration for a Host

Use this procedure to edit time configuration for a host in VMware vShphere.

Procedure

1. Log in to VMware vSphere (or vCenter) Client.

2. Choose **Inventory** > **Hosts and Clusters**.

3. Select the host to set the date and time.
4. Choose **Configuration** > **Time Configuration**
5. Choose the **Time** and **Date** from the drop-down list.
6. Click **OK**.
7. Reboot the virtual machines.

> Once you edit the time configuration for the host, you cannot set up the NTP server using the Cisco NAE appliance.

Uploading A Certificate Authority Signed Certificate

Cisco NAE appliance includes default self-signed certificates for the LDAP and web server.

After installing the Cisco NAE appliance, you can replace the default LDAP and web server certificates with any Certificate Authority (CA) signed certificate.

Before you begin

- You have generated the CA signed certificate that you want to upload to the appliance.
- You have the permission to access and upload the certificate.
- For the CA signed LDAP certificate, the certificate path and certificate alias are available.
- For the CA signed web server certificate, the certificate path and certificate key path are available.

Procedure

Perform the following steps to upload a CA signed LDAP certificate.

1. Generate a CA signed LDAP certificate.
2. Log in to a VM in the Cisco NAE appliance as an admin user.
3. Copy the certificate files to the VM and set the permission for all the folders or files in the path to 755.
    a. Example 1: If you copy the certificates directly to the admin folder `/home/admin/filename` or into a sub folder `/home/admin/folder1/folder2/filename`, run the command `chmod –R 755 admin` to change the permissions.
    b. Example 2: If you copy the certificates into a folder that is created under the home or the tmp folder `/home/folder1/filename` or `/tmp/folder1/filename`, run the command `chmod –R 755 folder1` to change the permissions.
4. Run the command `python /lib/candid/python/InstallLdapCertificate.py`.
5. Enter the admin password.
6. Enter the certificate path. Certificate path is the location of the CA signed LDAP certificate.
7. Enter the certificate alias. Certificate alias name is unique name assigned to the CA signed

certificate in the keystore.

8. Run the command `python /lib/candid/python/GetLdapCertificate.py` to verify if the certificate has been installed successfully.
9. Log in to the other VMs to verify if the certificate is uploaded to all the VMs in the NAE cluster.
10. (Optional) Run the command `python /lib/candid/python/DeleteLdapCertificate.py` to delete the CA signed LDAP certificate. You cannot delete the default self-signed LDAP certificate.

Perform the following steps to upload a CA signed web server certificate. Uploading a CA signed web server certificate will replace the default self-signed web server certificate.

1. Generate a CA signed web server certificate.
2. Log in to a VM in the Cisco NAE appliance as an admin user.
3. Run the command `python /lib/candid/python/InstallWebCertificate.py`.
4. Enter the admin password.
5. Enter the certificate path. Certificate path is the location of the CA signed web server certificate.
6. Enter the certificate key path. Certificate key path is the location of the key for the certificate file.
7. To view the certificate, log in to the appliance using the Chrome browser. Click **More Tools** > **Developer Tools** > **Security** > **View Certificate** to view the certificate.

Performing Online Analysis

An Assurance Group provides Intent Assurance for a group of entities at the same time. Assurance Group configuration allows you to configure the entities that need to be analyzed together. Performing online analysis allows the Cisco NAE to collect data from the Assurance Group, build a model with the collected data, and generate results. The results are displayed on the **Dashboard** as Epochs.

Use this procedure to perform online analysis.

Before You Begin

- You must have the credentials to access the APIC hosts.
- APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure export policy.

Procedure

1. Choose **Settings** > **Assurance Group Configuration**.
2. Click **Create New Assurance Group**.
3. Complete the following fields for **Create New Assurance Group**.
   a. In the **Name** field, enter the name.
   b. In the **Description** field, enter the description.

c. Check the **Switch to online mode** check box, to automatically analyze the Assurance Group in real time. Ensure that **Switch to online mode** check box is selected.

d. In the **Username** field, enter the user name to access the APIC hosts.

e. In the **Password** field, enter the password to access the APIC hosts.

f. From the **Analysis Interval** drop-down list, choose the interval to run the analysis. Analysis interval includes the time to collect data from APIC and the switches, analyze the data to build a model, generate results, and display them on the Dashboard. For production environments, the recommended analysis interval is a minimum of 15 minutes. An interval below 15 minutes should be used only in lab environments or for testing.

g. From the **Analysis Timeout** drop-down list, choose the time the system needs to wait before terminating the analysis. This value should be greater than the **Analysis Interval**

h. Check the **Start Immediately** check box, to start the analysis of the selected Assurance Group immediately.

4. Complete the following fields for **APIC Hosts**.

   a. In the **APIC Hostname 1** field, enter the APIC host name in the format apic1.example.com.

   b. Click + to add another APIC host name. We recommend that you add all the APIC hosts to the Assurance Group.

5. Complete the following fields for **Collection Settings**. Collection settings are required for NAT and epoch delta analysis. See Creating Epoch Delta Analysis. See Management and Network Connectivity.

   a. Check the **Use APIC Configuration Export Policy** check box, to export configuration policy for policy delta.

   b. Click **Show**.

   c. Select the **Export Format**.

   d. In the **Export Policy Name** field, enter policy name.

   e. Check the **Use NAT Configuration File** check box, to upload a file that has the Network Address Translation (NAT) table.

   f. Click **Show**.

   g. Click **Download NAT Configuration File Template**.

   h. Enter the public and private IP address mapping in the NAT configuration CSV file to indicate the NAT translation that needs to be used to access the APIC hosts.

   i. Click **Browse** to upload the CSV formatted NAT configuration file containing the public and private IP address mapping to be used to access the Assurance Groups.

   j. In the **File Name** field, enter the file name and click **Upload**.

6. Click **Save**.

7. The status of the analysis is displayed in the Data Collection form. Cisco NAE performs analysis on only one fabric at a time. To perform analysis on another fabric, you must stop the analysis on the current fabric and then start the analysis on another fabric. You can perform the following actions:

   - Click the play icon to start the analysis.
   - Click the stop icon to stop the analysis.
   - See Managing Assurance Group.

8. To view the results of the analysis, click **Dashboard**. See Timeline. Ensure that you have the correct Assurance Group selected to view the results. Click **Assurance Group** and select the Assurance Group from the drop-down list.
9. To export data, select a epoch dot on the timeline and click **Export Data**.

Performing Offline Analysis

Use the procedure to perform offline analysis. See the *Cisco Network Assurance Engine Fundamentals Guide* for information about the Offline Data Collection Script.

Procedure

1. Choose **Settings** > **Download Offline Collection Script** to download the python script.
2. Run the downloaded script to collect the data for assurance. See README for more information.

> The python offline data collection script is only supported on Mac OS or CentosOS. Running the script from a Windows server will result in an error and Cisco NAE will indicate that the APIC version is unsupported.

3. Choose **Settings** > **Offline File Management** to upload the collected data.
4. Click **Create New Upload**.
5. In the **Create New Upload** form, complete the following fields.
   a. Click **Browse** to upload the collected data to provide one-time assurance.
   b. In the **Name** field, enter the name of the file.
   c. In the **Description** field, enter the description.
6. Click **Submit**. After the file has been uploaded successfully, it is displayed in the Upload table.
7. Choose **Settings** > **Offline Analysis**.
8. In the **New Offline Analysis** form, complete the following fields.
   a. In the **Analysis Name** field, enter the name of the offline analysis.
   b. From the **File** drop-down list, choose the file with the collected data.
   c. From the **Assurance Group** drop-down list, choose the Assurance Group.
   d. (Optional) Click + to add another Assurance Group. Use this form if you want to define a new Assurance Group.
   e. From the **Analysis Timeout** drop-down list, choose the time the system needs to wait before terminating the analysis. You can also enter the time the system needs to wait before terminating the analysis.
9. Click **Run** to run the offline analysis. After the offline analysis is completed, the status is

displayed in the **New Offline Analysis** form. Cisco NAE performs analysis on only one fabric at a time. To perform analysis on another fabric, you must stop the analysis on the current fabric and then start the analysis on another fabric.

10. To view the results of the analysis, click **Dashboard**. See Timeline.

Cisco Network Assurance Engine Licensing

Cisco NAE License

Starting with Cisco NAE release 2.1(1a), licensing is enabled in Cisco NAE. Cisco NAE software will offer full functionality for a period of 30 days after installation. After this period expires, data collection and analysis will continue in Cisco NAE release 2.1(1a), but in subsequent releases the analysis will stop. Users are urged to request a license as soon as Cisco NAE version 2.1(1a) is installed.

The types of licenses available for Cisco NAE include:

- Trial license: Allows the use of Cisco NAE software for a period of 30 days. Allows the use of Cisco NAE to conduct a Proof of Value trial.
- Production license: Allows the use of Cisco NAE software for the term specified in the purchase contract.
- Not-For-Resale (NFR) license: Valid for a period of 365 days from the date of installation. This license is available for partners ONLY to train and get familiar with the software. This is an unlimited feature license available at no cost to the partner.

Workflow For Obtaining Cisco NAE License

1. After Cisco NAE is installed, a Trial license is automatically enabled. The Trial license is valid for a period of 30 days.
2. Contact your account representative to request for a valid license before the Trial license expires.
3. Choose **Settings** > **About Network Assurance Engine**, to obtain the Appliance ID and Appliance Model information.
4. Provide the following details when you request for a valid license.
   a. Appliance ID
   b. Customer Name
   c. License Type
   d. Appliance Model
5. Upload the valid license to Cisco NAE. See <<updating_license, Updating License

Updating License

Use this procedure to update the Cisco NAE license.

Procedure

1. Choose **Settings** > **License**.
2. Click **Update License**.

3. In the **Upload License File**, click **Browse** to upload a valid license file.
4. Click **Upload**.
5. The License details are displayed on the **License Page**

Cisco Network Assurance Engine GUI

Overview of the GUI

The Cisco NAE GUI is a browser-based graphical user interface that communicates internally with the Cisco NAE software engine by exchanging REST API messages. At the top of the GUI are several tabs, and each tab expands to reveal subtabs. Choosing a subtab opens the respective inspector page. An inspector page provides information about the smart events for the respective portion of your network. Each inspector page generally has several areas and panes, and multiple dashlets in the areas.

On most pages, you can jump to the different areas by clicking the corresponding circular button in the middle of the right edge of the page. The blue circle is the currently-displayed area.

A dashlet is a small panel that provides a summary of a specific type of information that relates to the content of a page. The exact layout varies by inspector page.

The GUI contains the following pages:

- Dashboard tab—Provides a high-level overview of the health of the fabric.
- Epoch Analysis tab-Provides information about the state of the fabric between two epochs.
- Change Management tab
  - Workflows
    - Real-time Change Analysis—Provides information about the assurance on real-time changes.
- Verify and Diagnose tab
  - Tenant
    - Tenant Endpoints—Provides information about the health of tenant endpoints.
    - Tenant Forwarding—Provides information about the health of tenant forwarding.
    - Tenant Security—Provides information about the health of tenant security.
- Optimize tab
  - Resource Optimization
    - TCAM—Provides information about the TCAM utilization in the Assurance Group.
- Smart Events tab—Provides information about all of the smart events.
- Assurance Group drop-down list—Enables you to choose which assurance group to analyze. Green color icon indicates an active Assurance Group.
- Settings menu—Enables you to perform various miscellaneous tasks, such as configure an assurance group, configure the log level settings, perform an offline analysis, manage users, view the REST API documentation, and see information about your installation of the Cisco NAE.
- User menu—Enables you to change your password, edit user account, or log out of the Cisco

NAE.

Cisco NAE GUI Icons

The following table provides a description of the Cisco NAE GUI icons.

Table 5. Cisco NAE GUI Icons

Icon	Description
+	A button that adds a virtual machine.
—	A button that removes a virtual machine.
Ⓒ	An icon that indicates a consumer endpoint group.
⋮	A button that displays more options for a dashlet. In most cases, the options enable you to toggle a dashlet’s view between the grid view and chart view.
✕	A button that closes an overlay or removes data.
▾	An icon that indicates a drop-down list.
✎	A button that opens the form to edit data.
🗎	A button that opens the form to view details.
?	A button that provides helpful tips.
✓	An icon that indicates information events.
!	An icon that indicates minor events.
⚠	An icon that indicates major events.
✖	An icon that indicates critical events.
!	An icon that indicates warning events.
✕	A button that closes a mode.
🔔	A button that opens a notification-related panel or data.
▶	A button that plays or starts data fetching.
■	A button that stops data fetching.
Ⓟ	An icon that indicates a provider endpoint group.
↻	A button that refreshes a page or dashlet.
⌄	A button that expands a sankey diagram.
⌃	A button that collapses a sankey diagram.
⚙	A button that opens the settings menu.
🔍	A button that opens the search form.
⚠	An icon that indicates a server issue.
›	A button that expands the TCAM bar.
⌄	A button that expands the Events Trend dashlet.

Icon	Description
︿	A button that collapses the Events Trend dashlet.
i	A button in the **Settings** menu that opens a form that displays information about the installed Cisco NAE software build.
⚙	A button in the **Settings** menu that opens the assurance control configuration form.
☑	A button in the **Settings** menu that opens the appliance status form.
⚙	A button in the **Settings** menu that opens the appliance settings form.
API	A button in the **Settings** menu that displays the API documentation.
⇧	A button in the **Settings** menu that opens the offline file management form.
📈	A button in the **Settings** menu that opens the offline analysis form.
👥	A button in the **Settings** menu that opens the user management form.
LOG	A button in the **Settings** menu allows you to downloads tech support logs.
</>	A button in the **Settings** menu that allows you to download offline collection script.
●	An icon in the radial view of the visualization area that indicates an endpoint group.
⦶	An icon in the radial view of the visualization area that indicates an L2ExtInstp endpoint group.
⊘	An icon in the radial view of the visualization area that indicates an L3Out endpoint group.
•	An icon in the radial view of the visualization area that indicates a private network to VRF instance.
⊙	An icon in the radial view of the visualization area that indicates a shared network between a VRF instance.
✪	An icon in the radial view of the visualization area that indicates a vzAny endpoint group.
◎	A button in the visualization area that toggles the radial view.
ⓘ	An icon that you hover the mouse cursor over to see legend information.
↩	An icon in the Timeline area that goes back to the previous epoch selection.
⏭	An icon in the Timeline area that displays the oldest epoch.
⏮	An icon in the Timeline area that displays the latest epoch.
⏩	An icon in the Timeline area that displays the next epoch.
⏪	An icon in the Timeline area that displays the previous epoch.
☰	An icon that customizes the columns in a table.

Icon	Description
↓≡	An icon that sorts the columns in a table in ascending order.
↓≡	An icon that sorts the columns in a table in descending order.
⬍	An icon that indicates that the table can be sorted.
≡	An icon that indicates allows you to change the order of a column in a table.
✓	An icon that indicates a selected object.

Settings Menu

The **Settings** menu enables you to perform various tasks, such as configure an assurance group, configure the log level settings, perform an offline analysis, manage users, view the REST API documentation, and see information about your installation of the Cisco NAE. The menu contains the following items:

- **Assurance Group Configuration**—Enables you to add, delete, or modify an assurance group.
- **Download Offline Collection Script**—Downloads the offline collection script.
- **Offline File Management**—Enables you to upload previously-downloaded fabric data so that you can use the Cisco NAE in offline data analysis mode. You can also delete offline data.
- **Offline Analysis**—Enables you to perform offline data analysis. Cisco NAE provides one-time assurance of the offline data.
- **Appliance Administration**—Displays details of the Cisco NAE appliance cluster such as information about each individual virtual machine in the cluster, software version installed, the configured log level settings for the appliance, the disk usage, and authentication domain details.
- **Appliance Status**—Displays the smart events that relate to the appliance.
- **User Management**—Enables you to create user accounts and change the password of the accounts.
- **Download Tech Support Logs**—Downloads the tech support logs as a .tar file to your local system.
- **License**—Enables you to update an Cisco NAE license.
- **Appliance Documentation**—Enables you to view and download Cisco NAE documentation.
- **About Cisco Network Assurance Engine**—Displays information about your installation of the Cisco NAE.

Timeline

The timeline is located near the top of the inspector pages. The timeline shows the date and time of data collection (not analysis). Data is represented by dots on the timeline, which are referred to as epochs.

An epoch is a period of time in your network’s history during which the Cisco NAE collected and analyzed data. The size of the epoch gives a rough indication of the quantity of smart events at that time, with a larger epoch indicating more smart events.

An epoch can be one of the following colors:

- Gray—This indicates normal operation.
- Flashing Blue—This indicates that the Cisco NAE is currently running an analysis on the data.
- Red—This indicates critical errors are detected for an EPOCH during online analysis.
- Blue—This indicates an analysis based on offline data collection.

By default, the timeline shows a time range of 2 hours and 45 minutes with markings at 15 minute intervals to give you an estimate of when the data collection occurred. You can hover the mouse cursor over an epoch to see the exact time that the data collection occurred.

To export data, click **Export Data**. This allows you save the data collected for a selected EPOCH during online analysis for offline analysis at a later time.

You can change the time range by clicking one of the preset time durations under the timeline, or you can click **Custom** to specify a time range of your choice. Optionally, you can hover over an epoch to highlight it (do not click the epoch), then click and drag the mouse cursor over the timeline to choose that area as the custom time range. You can scroll backward or forward in time by intervals of the chosen time range (with a default of 2 hours and 45 minutes) by clicking the left or right arrow buttons that are located at either end of the timeline.

The date and time displayed to the right of the timeline represents the date and time of the currently chosen epoch. Use the arrows under the timeline to go to the first epoch, go to the previous epoch, go to the next epoch, or go to the last epoch. The **Live Updates** button sets the timeline to display the current date and time. The **Epochs with my events** button sets the timeline to display the epochs that contain one or more events that have been assigned to a particular user.

> When you assign an event from one user to another, the events are not reflected in the **Epochs with my events** timeline immediately. To view the epochs with reassigned events you must either refresh the page or select a different Assurance Group.

We recommended that you view less than 500 epochs at one time. If you have a lot of epochs in selected time-range, you can drag on the timeline to zoom into a smaller time window.

Dashboard Trend View

On the **Dashboard** inspector page, you can toggle between the standard epoch view and the trend view on the timeline by clicking the **Epoch** or **Trend** button, respectively. The epoch view is the default, which shows only the smart events of the selected epoch. The trend view shows the smart events trend in the dashlets across the chosen time range. The date and time displays a range of two dates and times, beginning with the start of the time range and ending with the end of the time range.

The first row of the dashboard changes to display the smart events trend for all smart event types for all categories. The trends are displayed as lines of the color appropriate to the smart event type; the lines give a graphical representation of the increase or decrease in the quantity of smart events. The remaining dashlets collapse to display fewer dashlets that generically display the smart events trend for critical, major, and minor smart events for the following categories:

- Real-time Change Analysis (RTCA)
- Tenant Endpoints
- Tenant Forwarding
- Tenant Security
- TCAM Utilization

As with the first row, the dashlets display the trends as lines of the color appropriate to the smart event type. Near the bottom of each dashlet, you can click on the name of a smart event type to toggle displaying the trend of that smart event type in the dashlet.

You can click the **Expand** link at the bottom of a dashlet to see a pop-up form that displays all of the smart event types, instead of only the critical, major, and minor smart events. Near the bottom of the form, you can click on the name of a smart event type to toggle displaying the trend of that smart event type in the form.

Summary Boards Area

The summary boards area provides a broad view of the issues that the Cisco NAE discovered in the fabric. For most pages, the summary boards area consists of the first two rows of dashlets. The exact composition of the summary area varies by page. For example, the **Dashboard** page does not have the summary boards area, while the **TCAM** page has only one row.

For most pages, the dashlet in the first row provides the number of each type of smart event. The following list provides the types of events:

- **Critical**—Critical smart events indicate issues that you must address as soon as possible.
- **Major**—Major smart events indicate serious issues that do not stop your Assurance Group from functioning, but you should address them as soon as possible.
- **Minor**—Minor smart events indicate issues that are not serious, but you should address them eventually.
- **Warning—**Warning smart events indicate things that are not issues now, but they have the potential to become issues later.
- **Info**—Info smart events generally indicate objects that are healthy. A low number of info smart events can indicate that there are issues in the fabric, while a high number of info smart events can indicate that most objects are healthy.
- **Total**—The total number of smart events of all types on the page.

The second row usually contains two dashlets. The dashlets provide the numbers of issues in the fabric by object, type, or category, depending on the page. The second row provides a different way (compared to the first row) of categorizing the issues.

Hot Topics Area

The hot topics area usually consists of two or three rows of dashlets. Each row has from one to three dashlets. The exact number of rows and dashlets varies by page.

The hot topics area helps you to determine which issues to resolve first by listing the objects of a particular type (leaf switches, tenants, endpoint groups, or application profiles) that have the most issues.

For the **Tenant Security** inspector page, you can change the dashlets from the grid view to the chart view. The grid view displays the number of issues (Smart Events) for the five objects that have the most critical violations, major violations, and minor violations, in that order of importance. The chart view displays a bar graph of the same data, providing a visual representation of the data.

For most of the other inspector pages, the dashlets display the five objects that have the most issues of the type indicated by the dashlet's title, such as health, violations by severity type, a subcategory of issues, or route count. The title of each dashlet is a drop-down list that you can use to change the type of object for which the dashlet displays data.

You can click a violations count in a dashlet to go to the Smart Events area and have the area display more information about Smart Events of the appropriate severity type for the appropriate type of object. Also, in the visualization area, the filter becomes set to filter for the Smart Events of the object that you clicked and the **View Control** options get set based on what you clicked. You can use this functionality only if the violation count is greater than 0.

For example, if you click the count of major violations for an application profile, the Smart Events area displays the Smart Events with severity type "Major" for that application profile. In the visualization area, the "APPLICATION PROFILE" parameter is added to the filter field, the **View Options** section has **Tenants** chosen, the **App Profiles** button is toggled on, the **Severities** section has only the major violations toggled on, and the **Event Count** section has all of the count ranges toggled on. You must manually enter the specific application profile name in the field for the "APPLICATION PROFILE" parameter.

Expanded Dashlet View

At the bottom of each dashlet is a link that opens a page with an expanded dashlet view. The expanded view displays the same data for all objects (not just the top five) of the type that is appropriate for the dashlet. For inspector pages other than the **Tenant Security** page, you can choose the type of object using the title drop-down list. If the dashlet has a **More** button that enables you to switch between the chart view and grid view, then the expanded view also has a **More** button that serves the same function.

Some of the columns have a search field in which you can type a string, which narrows the table to only those objects whose values contain the string for that column's parameter.

You can sort the table by one of the columns in descending or ascending order by clicking the **Sort** button next to the column's header. Clicking the button multiple times cycles through the sort options, and clicking on a different column's sort button resets the previous column's sort order and sorts the table by the new column. Optionally, you can hold **Shift** and click more than one of the **Sort** buttons to sort by multiple columns.

You can click a violations count to close the expanded dashlet view, go to the Smart Events area, and have the area display more information about Smart Events of the appropriate severity type for the appropriate type of object. Also, in the visualization area, the filter becomes set to filter for the Smart Events of the object that you clicked and the **View Control** options get set based on what you clicked. You can use this functionality only if the violation count is greater than 0.

Search

The **Search** bar filters by objects that you choose by clicking in the **Add Filters** field, and choosing from the options to perform a contained search. You can click **Add Filters** to filter by resources and then by resource name or DN. You can also use the severity icon to filter by severity.

When you click an unhealthy count in a severity-related dashlet on the GUI screen, it takes you to the **Search** bar which provides you filtered content based on your selection.

The Smart Events table (following the Search bar) displays a filtered view based on items chosen in the Search bar.

The following examples help you understand how the Search bar works —

- In the **Search** bar, if you choose to filter with Application Profile, the search function forces you to choose a specific application profile. You can then further choose to add a different object, such as Contract and the search function forces you to choose a specific contract. As these are two different objects, the AND operator is used to provide the search results.
- If you filter using two of the same objects, such as two application profiles, then the OR operator will be used to filter the search results.

Additional Severity choices are also available to filter the search. Based on the filters you use, the tables following the **Search** bar provide you with filtered information.

When you click **Reset**, it resets the default **Search** bar settings.

For smart events, you can also search on event code, check code, check status (failing or passing status or both), and event rule.

Visualization Area

The visualization area provides a graphical representation of the analysis that the Cisco NAE performed and the information that the Cisco NAE generated. The visualization area is a powerful tool for quickly discovering who and what is having a problem, and how many problems the object has. The visualization area presents a graphical version of the numerical data in the dashlets. Only the **Tenant Security** and **Tenant Endpoints** inspector page have the visualization area.

Visualization Area of the Tenant Security Inspector Page

The **Tenant Security** inspector page displays a radial view. The different parts of the radial view represent different types of information. The outer ring represents the tenants, the inner ring represents application profiles, and arced lines in the middle show the health of the contracts. The points where the arced lines and inner ring connect represent endpoint groups. The colors of the arced lines corresponding to the same colors used by smart events.

For example, a red line indicates that the contract has one or more critical smart events, orange indicates major smart events, and yellow indicates minor smart events. The tooltips for the arced lines provide more information about the health, including the severity type of the smart events and how many smart events there are of each smart event. You can click on an arced line to change the visualization area to show the endpoint groups of the contract.

The lower right corner of the graph pane contains the following controls:

- **Back to Overview** button—Changes the visualization area to show the tenant security overview (the original view).
- **Circle with a line inside**—The line is the arc that you clicked, and has the same color as the arc.
- **Expand All** button—Expands the display of all of the endpoint groups to see the full information about them.
- **Collapse All** button—Collapses the display of all of the endpoint groups to hide the information about them.

At the top of the visualization area is a filter field, which you can use to narrow down the amount of data in the graph. If you click in the field, the Cisco NAE presents several suggestions for filter parameters. You can click on one or more of the parameters to have them be added to the filter field. You can click the same parameter multiple times to add it more than once. Optionally, you can start typing in the filter field and the Cisco NAE displays the closest matches to whatever you typed. For example, if you type "app," the Cisco NAE displays "Application Profile" as the closest match. You can click on one of the closest matches or you can type the full filter name and press **Enter** to add the filter to the filter field.

After adding a filter parameter, you must enter a string in that parameter’s text field to specify an object of the parameter’s type. For example, if you added LEAF as a parameter, you must then enter a specific leaf switch’s name in the LEAF parameter’s text field. As you type, the Cisco NAE displays the closest matches to whatever you typed. You can click on one of the closest matches or you can type the full object name and press **Enter** to add the object name to the parameter’s text field.

You can also filter the graph by smart event severity by deselecting any of the severity types to the right of the filter field. Click **Reset** to reset the filter to display all severities.

The **View Control** pane contains the following controls:

- **View Options** section
  - **Tenants** button—Changes the graph to display the tenants instead of the VRF instances. Clicking this button deselects the VRFs button.
  - **VRFs** button—Changes the graph to display the VRF instances instead of the tenants. Clicking this button deselects the Tenants button.
  - **App Profiles** button—A toggle that includes or excludes application profiles from the graph. You can click this button only if the graph is displaying the tenants.

    - **Bridge Domains** button—Changes the graph to display only the VRF instances. You can click this button only if the graph is displaying the VRF instances.

- **Event Count** section—Each button is a toggle that includes or excludes all contracts from the graph that have the specified quantity of smart events.
- **Violations by Policy Type** section—Updates the filter to filter by smart events of the selected policy types.

Visualization Area of the Tenant Endpoints Inspector Page

The **Tenant Endpoints** inspector page displays a bar graph. The information displayed in the graph depends on what you specify for the filter and the value that you choose in the **Show** drop-down list.

You can use the filter field to narrow down the amount of data in the graph. If you click in the field, the Cisco NAE presents several suggestions for filter parameters. You can click on one or more of the parameters to have them be added to the filter field. You can click the same parameter multiple times to add it more than once. Optionally, you can start typing in the filter field and the Cisco NAE displays the closest matches to whatever you typed. For example, if you type "app," the Cisco NAE displays "Application Profile" as the closest match. You can click on one of the closest matches or you can type the full filter name and press **Enter** to add the filter to the filter field.

After adding a filter parameter, you must enter a string in that parameter's text field to specify an object of the parameter's type. For example, if you added "Leaf" as a parameter, you must then enter a specific leaf switch's name in the Leaf parameter's text field. As you type, the Cisco NAE displays the closest matches to whatever you typed. You can click on one of the closest matches or you can type the full object name and press **Enter** to add the object name to the parameter's text field.

You can also filter the graph by smart event severity by deselecting any of the severity types to the right of the filter field. Click **Reset** to reset the filter to display all severities.

The possible values for the **Show** drop-down list are as follows:

- **Leaf**—The graph displays information about the fabric's leaf switches.
- **Tenant**—The graph displays information about the fabric's tenants.
- **App Profile**—The graph displays information about the fabric's application profiles.
- **EPG**—The graph displays information about the fabric's endpoint groups.
- **VRF**—The graph displays information about the fabric's VRF instances.
- **BD**—The graph displays information about the fabric's bridge domains.

The second drop-down list enables you to choose the sort order of the bars. The possible values are as follows:

- **Total EPs**—Sorts by the total quantity of endpoints on the left, with the quantity of the different smart events on the right.
- **Unhealthy**—Sorts by the most unhealthy endpoints on the left, with the quantity of the

different smart events on the right.

- **Total EP Events**—Sorts by the total quantity of endpoint smart events on the left, with the quantity of the different smart events on the right.
- **Critical**—Sorts by the endpoints with the most critical smart events on the left, with the quantity of the different smart events on the right.
- **Major**—Sorts by the endpoints with the most major smart events on the left, with the quantity of the different smart events on the right.
- **Minor**—Sorts by the endpoints with the most minor smart events on the left, with the quantity of the different smart events on the right.
- **Warning**—Sorts by the endpoints with the most warning smart events on the left, with the quantity of the different smart events on the right.
- **Info**—Sorts by the endpoints with the most information smart events on the left, with the quantity of the different smart events on the right.

Click the sort button to the left of the drop-down list to toggle between sorting in descending order and ascending order by the chosen category.

You can click a bar graph to change the smart events area to display more information about the smart events for that object. Click the left side of the graph to see all of the smart events, or click the color on the right side that corresponds to the specific smart event type that you want to see. The smart events provide information about the health of the object, such as which health checks were done and which health checks are passing.

The **View Control** pane contains the following controls:

- **EP Health Status** section
  - **Unhealthy** button—A toggle that includes or excludes unhealthy endpoints from the graph.
  - **Total button**—A toggle that includes or excludes the total quantity of endpoints from the graph.
- **View By** section
  - **Severity** button—Changes the View Control pane to display the Severity section. Clicking this button deselects the **Subcategory** button.
  - **Subcategory** button—Changes the View Control pane to display the Subcategory section. Clicking this button deselects the **Severity** button.
- **Severity** section—Each button is a toggle that includes or excludes all endpoints from the graph that have at least one of the respective smart event type. This section displays only if you clicked the **Severity** button.
- **Subcategory** section—This section displays only if you clicked the Subcategory button. The buttons in this section perform the following functions:
  - **EP Learning** button—A toggle that includes or excludes endpoints that have learning issues.
  - **EP IP Address** button—A toggle that includes or excludes endpoints that have IP address allocation issues.

    - **EP Static** button—A toggle that includes or excludes endpoints that have static issues.

Tenant Endpoint Details Area

The **Tenant Endpoints** inspector page has a tenant endpoint details area, which has a table that provides the following information about the endpoints:

- Severity
- MAC
- IP
- BD
- VRF
- Tenant
- Application Profile
- Leaf switch

You can click an entry to get more information about that endpoint.

Smart Events Area

By default, the smart events area lists all of the smart events that are relevant to the inspector page. For example, the smart events area of the **Tenant Security** inspector page shows tenant security smart events. The title of the table indicates the total quantity of smart events that are on the table. For example, a title of "Tenant Endpoints Events (12)" indicates 12 smart events.

The columns of the smart events table vary depending on the inspector page, although all smart events tables have the following columns:

- **Severity**—The severity type of the smart event, represented by the icon for that severity type. This column has a search field that enables you to filter for smart events of the severity type that you specify. Even icons represent the severity types, you must enter the severity type as a string in the field. The possible severity types are as follows:
    - Critical
    - Major
    - Minor
    - Warning
    - Info
- **Event Subcategory**—The subcategory for the smart event.
- **Event Name**—The code for the smart event. You can click a code to expand the row to display the following information about the smart event:
    - Description—A short description of the smart event.
    - Impact—Describes the impact that the smart event has on the fabric.

- Affected Objects—A table that provides information about the objects that triggered the smart event. The table varies depending on the inspector page.
- Checks—Two tables that provide information about the checks that were done to find the issue. One table contains the failing conditions and the other contains the passing conditions. If no checks passed, then that table is excluded.

This column has a search field that enables you to filter for specific smart event codes.

- **Event Description**—The quantity of smart events of that same type.
- **Event Description**—A short description of the smart event.

You can hover the mouse cursor over some of the table cells to see a tooltip that provides expanded information about the object in the cell. An example of the expanded information is the full path of a provider tenant.

At the bottom right of the smart smart events area, you can choose how many rows to display on a page.

See the *Cisco Network Assurance Engine Smart Events Reference Guide* for more information.

> If the event suppression feature is activated, the smart event count and the smart events listed take into account the event rules.

See About Smart Event Suppression for more information.

Exporting Data from the GUI

Starting from Cisco NAE release 2.1(1), you can export the data from certain tables in the GUI to JSON and CSV format.

Exporting the data from the following tables in the GUI is supported.

- All Smart Events tables in the Cisco NAE GUI.
- End Point Details table in the **Tenant End Points** inspector page.
- L3 Forwarding table in the **Tenant Forwarding** inspector page.

To export data to the JSON format, navigate to the table in the inspector page and then choose **Table Settings** > **Export to JSON**.

To export data to the CSV format, navigate to the table in the inspector page and then choose **Table Settings** > **Export to CSV**.

Important Notes

- The data from all the columns in the table are exported irrespective of the columns selected in the **Column Customization** setting for the table.
- Ordering the table columns using the **Column Customization** setting does not affect the order of the columns when the data is exported.

- In each export instance you can export the data contained in 10,000 rows. To export the data from a table containing more than 10,000 rows, you must select the rows containing the dataset to be exported.

Epoch Delta Analysis

Epoch Delta Analysis

Cisco NAE performs analysis of an Cisco ACI fabric at regular intervals called epoch and the epoch data is collected in 15 minute intervals.

At each epoch, Cisco NAE captures a snapshot of the controller policies and the fabric run time state, performs analysis, and generates smart events. The smart events generated describe the health of the network at that epoch.

Epoch delta analysis enables you to analyze the difference in the policy, run time state, and the health of the network between two epochs. Epoch delta analysis consists of the following components:

- **Analysis Management**: Enables you to create a new delta analysis and manage existing analysis. See Creating Epoch Delta Analysis.
- **Delta Analysis**: Enables you to view results of successful delta analysis such as health delta and policy delta. See Viewing Delta Analysis Results.

Health Delta

Health Delta analyses the difference in the health of the fabric across the two epochs. The results are displayed in the following areas:

- **Smart Event Count**: Displays the difference in smart event count per severity across the two epochs.
- **Health Delta by Resources**: Displays the count of resources by type (for example, Tenants, EPGs, contracts) that have seen a change in their health. The changes can either be issues resolved or new issues detected.
- **All Smart Events**: The **Aggregated** view displays the delta status for each smart event name across the two epochs. The **Individual** view displays the delta status for each smart event across the two epochs and also the failing conditions for the event.

Policy Delta

Policy Delta analyzes the differences in the policy between the two epochs and provides a corelated view of what has changed in the ACI Fabric.

The policy delta view enables you to:

- View the changed policy objects between the two epochs.
- View the added, modified, and deleted policy configurations between the two epochs.
- Export the policy configuration for the earlier epoch policy and later epoch policy.
- Search for text in added, modified, deleted, and unchanged areas in the policy delta.

- View the context around the modified areas in the policy delta.
- View the difference in the APIC audit logs across the two epochs.

To view the policy delta between the two epochs, you must configure the collection settings for an Assurance Group. See Performing Online Analysis.

Guidelines and Limitations

The following general guidelines are applicable to Epoch Delta Analysis:

- While you are currently allowed to create more than one Epoch Delta Analyses at any given time, we recommend that you do 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 following guidelines and limitations are applicable for policy delta:

- The **APIC Configuration Export Policy** must be configured. See Performing Online Analysis.
- The **APIC Configuration Export Policy** must be of the same format (XML/JSON) for both the epochs.
- The policy delta will not be performed if there are any APIC configuration export policy collection errors.

Creating Epoch Delta Analysis

Use this procedure to create an epoch delta analysis.

Before You Begin

- You have configured the collection settings for an Assurance Group. See Performing Online Analysis.
- APIC admin writePriv privileges allow information collection on the APIC host and leaf switches. You must have APIC admin writePriv privileges to configure the **APIC Configuration Export Policy**.

Procedure

1. Choose **Epoch Analysis** > **Epoch Delta Analysis** > **Analysis Management**.
2. Click **Create New Delta Analysis**.
3. Complete the following fields for **Create New Delta Analysis**.
   a. In the **Name** field, enter the name. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description.

c. From the **Earlier Epoch** drop-down list, choose the first epoch for the delta analysis. You can also use the timeline to select an earlier epoch. See Timeline for more information.

d. From the **Later Epoch** drop-down list, choose the second epoch for the delta analysis. You can also use the timeline to select a later epoch.

> The two epochs selected for the delta analysis must belong to the same Assurance Group.

4. Click **Run**.
5. The status of the delta analysis is displayed in the **Delta Analysis** table. Cisco NAE performs one delta analysis at a time. To perform another delta analysis, you must stop the current delta analysis and then start the another delta analysis. See Managing Epoch Delta Analysis.
6. To view the results of the delta analysis, select a delta analysis from the **Delta Analysis** table. From the Actions menu, choose **View Results**. See Viewing Delta Analysis Results.

Viewing Delta Analysis Results

Use this procedure to view the results of the delta analysis.

- To view the results of health delta analysis, See Viewing Health Delta Analysis.
- To view the results of Policy delta analysis, See Viewing Policy Delta Analysis.

Viewing Health Delta Analysis

Use this procedure to view the results of the health delta analysis.

Procedure

1. Choose **Epoch Analysis** > **Epoch Delta Analysis** > **Delta Analysis**.
2. Click **Health Delta** to view the results of the health of the fabric.

   a. **The Smart Event Count** displays the difference in the smart event count per severity across the two epochs. The first count represents the smart events found only in the earlier epoch. The second count represents the smart events common in both the epochs. The third count represents the smart events found only in the later epoch.

      i. Click the smart event count to view the smart event details.

   b. The **Health Delta By Resources** displays the health delta across various APIC resource types. It also displays the count of the resources with issues, without issues, and the total resources.

      i. Click the resource count to view the resources associated with the resource count.

      ii. Hover on the resource name to view the resource DN.

      iii. Click the resource name to view the smart event details for that resource.

   c. In the **Search** bar use the multiple filters to search for smart events.

        i. Click **Add Filters** to filter by resources and then by resource name or DN.

        ii. Click the ●○ icon to filter by the epochs used for the delta analysis.

    d. The **All Smart Events** table displays the aggregated and individual view of the smart event delta.

        i. Click **Aggregated** to view the delta status for each smart event name across the two epochs. The **Count** column displays the consolidated number of events across the two epochs.

        ii. Click **Individual** to view displays the delta status for each smart event across both the epochs and also the failing conditions for the event. Click **Event Name** to view the smart event details.

Viewing Policy Delta Analysis

Use this procedure to view the results of the policy delta analysis.

Procedure

1. Choose **Epoch Analysis** > **Epoch Delta Analysis** > **Delta Analysis**.
2. Click **Policy Delta** to view the results of the policy changes across the two epochs. Policy Delta includes 3 panels, Changed Policy Object, Policy Viewer, and Audit Log.
3. The **Changed Policy Object** panel, displays the changed policy object tree across the two epochs.
    a. Drill down on a particular object to view the object types that have changed. The number indicates the number of changes to the object.

    b. Select the changed object type to view the smart events that have changed.

    c. Click DN link to access the affected object type in APIC.

    d. Click **Show Changes** to view the changes in the Policy Viewer and Audit Log panels. The corresponding changes in the Policy Viewer and Audit Log panels are highlighted.

    e. Use the **Search** bar to perform a DN search.
4. The **Policy Viewer** panel displays the policy configuration across the earlier and later epochs. The policy configuration for the earlier epoch is called the earlier epoch policy. The policy configuration for the later epoch is called the later epoch policy.
    a. Use the color coding to visualize the added, deleted, modified, and unchanged content across the two policies. Click the ⓘ icon for information about the color coding.

    b. The ●○ icon lists the line numbers for the content in the earlier epoch policy. The ○● icon lists the line numbers for the content in the later epoch policy.

    c. Click **Show More Above** or **Show More Below** to display more content.

    d. Click the ⤓ icon to export the earlier epoch policy or to export the later epoch policy.

    e. Enter a value in the **Search** bar to perform a text search.

        i. Select **ALL** to search across all the content in the earlier epoch policy and later epoch policy.

        ii. Select **Changed** to search across the changed content in the earlier epoch policy and later epoch policy.

5. Cisco NAE collects audit logs from APIC and computes the difference in the audit logs between the two epochs. The **Audit Log** panel then displays all the audit logs that were created between the two epochs. A correlated view of what has change in the datacenter is displayed in the **Audit Log** panel. When you select a particular object in the **Changed Policy Object** panel, the relevant difference is highlighted in the **Policy Viewer** panel and the relevant audit log is highlighted in the **Audit Log** panel. APIC audit logs are records of user-initiated events such as logins and logouts or configuration changes that are required to be auditable. For every epoch, the audit log history is limited to last 24 hrs.

    a. In the audit log panel, green color indicates the audit log attributes such as VLAN that have been added. Red color indicates the audit log attributes that have been deleted. Yellow color indicates the audit log attributes that have been modified.

    b. Use the **Search** bar to perform a DN, User ID, or text search.

    c. Hover on an audit log entry to view when the changes were made and who made the changes. The timestamp on the audit log entry corresponds to the the timestamp on the APIC audit log.

    d. Click Audit Log entry to access the affected object type in APIC.

Compliance Analysis

Compliance Analysis Tab

Every epoch verifies compliance analysis results. In each epoch, one event for every requirement that is analyzed is raised. For example, if an assurance group runs a compliance analysis on an epoch every 15 minutes, and there are two requirements associated with the epoch, two smart events will be raised.

When an epoch runs for a specific assurance group, all the active requirement sets that are associated with that assurance group are verified and validated.

> ℹ To be included as an active requirement set, you must associate your compliance requirement to the assurance group and activate the compliance requirement.

Manage Compliance Requirements

Manage Compliance Requirements Tab

The **Manage Compliance Requirements** tab enables the user to verify Segmentation Compliance and Service Level Agreement (SLA) compliance, and traffic restriction compliance. Compliance can be used to set up regulatory compliance rules. With segmentation compliance, the user can establish walled areas around a set of entities that must not communicate with other entities. SLA compliance can also set up rules for entities that must talk with other entities. Traffic restriction compliance requirements allow the user to specify restrictions on protocols and ports for communication between EPGs.

In the NAE UI, the user specifies their compliance requirements. The NAE appliance, verifies in the subsequent epochs, whether the compliance requirements are satisfied by the policy that is configured on Cisco APIC. If satisfied, an event is raised stating that the compliance requirement is satisfied. One event per requirement per epoch is raised. For example, if an assurance group runs a compliance analysis on an epoch every 15 minutes, and there are two requirements associated with the epoch, two smart events will be raised.

The following examples provide you with information about the compliance segmentation **include** and **exclude** rules:

- Contains EPGs in Tenants with names that start with “a” or ending with “z”. EPGs in Tenants such as “abz” that satisfy both criteria are included only once.
- Contains EPGs in Tenants with names that start with “a” and are also in VRFs where the Tenant is “xyz” and the VRF name contains “c”. For example: When an EPG under Tenant “abc” that is in a VRF with DN uni/tn-xyz/ctx-abcde is selected, verify that both the Tenant and the VRF criteria match. An EPG under Tenant “abc” that is in a VRF with DN uni/tn-xyz1/ctx-abcde is not selected because the VRF Tenant does not match.
- Contains all EPGs under Tenants that begin with “a” except those that contain “d”. For example: An EPG under Tenant “abc” is selected. An EPG under Tenant “abcd” is not selected.
- Contains all EPGs under Tenants that begin with “a” except those EPGs that are also in the VRF with DN uni/tn-rrr/ctx-sss.

Creating EPG Selector

Use this procedure to create an EPG Selector.

Before You Begin

- At least one assurance group must be created.

Procedure

1. Choose **Compliance** > **Manage Compliance Requirements** > **EPG Selectors**.
2. Click **Create New EPG Selector**.

3. Complete the following fields for **Create New EPG Selector**.
   a. In the **Name** field, enter the name. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description. (Optional step)
   c. In the **Include EPGs** field, from the drop-down options, choose the relevant EPGs based on the options available in the match criteria.

> ℹ You may use multiple match criteria and the included EPGs will be a union and intersection of the criteria that you choose.

   d. In the **Excluded EPGs** field, from the drop-down options, choose the relevant EPGs based on the options available.
   e. Click **Save**.

> ℹ Your EPG Selectors are created.

4. The list of EPG selectors is displayed under the **EPG Selectors** tab.

For additional details about editing or deleting EPG selectors, see Managing EPG Selectors.

Creating Traffic Selector

Use this procedure to create a traffic selector.

> ℹ You must configure the Traffic Selectors before configuring the Compliance Requirement and the Compliance Requirement Sets (in that order of sequence).

Before You Begin

- At least one assurance group must be created.

Procedure

1. Choose **Compliance** > **Manage Compliance Requirements** > **Traffic Selectors**.
2. Click **Create New Traffic Selector**.
3. Complete the following fields for **Create New Traffic Selector**.
   a. In the **Traffic Selector Name** field, enter the name. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description. (Optional step)
   c. In the **Talk On** area, from the **EtherType** field drop-down options, choose the appropriate EtherType.

> ℹ Certain **EtherType** choices will require you to make additional choices from drop-down lists that appear based upon your selections.

4. To add additional EtherType options, click **Add On**, and choose additional EtherType options.
5. Click **Save**.

Your traffic selectors are created. The list of traffic selectors is displayed under the **Traffic Selectors** tab.

For additional details about editing or deleting traffic selectors, see Managing Traffic Selectors.

Creating Compliance Requirement

Use this procedure to create a compliance requirement.

Before You Begin

- At least one assurance group must be created.
- Your EPG selectors are created.
- Your traffic selectors are created.

Procedure

1. Choose **Compliance** > **Manage Compliance Requirements** > **Compliance Requirements**.
2. Click **Create New Compliance Requirement**.
3. Complete the following fields for **Create New Compliance Requirement**.
    a. In the **Compliance Requirement Name** field, enter the name. The name must be unique across all the analyses.
    b. In the **Description** field, enter the description. (Optional step)
4. In the **Compliance Type** area, perform the appropriate steps to specify the requirements depending on whether you choose **Segmentation** or **SLA**.
    a. If you choose **Segmentation** perform the following steps:
        i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.
        ii. Choose the appropriate communication operator (for example **Must Not talk to**).
        iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.
    b. If you choose **SLA** perform the following steps:
        i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.
        ii. Choose the appropriate communication operator (for example **Must Talk to**).
        iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.
        iv. Click **Select Traffic Selector name** and choose a traffic selector name.
    c. If you choose **Traffic Restriction** perform the following steps:
        i. Click **Enter EPG Selector A name** and choose an EPG selector name from the list.
        ii. Choose the appropriate communication operator (for example **Must Not Talk to**).

> When you choose the value **Must Not Talk To**, Cisco NAE verifies that the EPGs do not communicate with the specified protocol in the traffic selector field. When you choose the value **May Talk To**, Cisco NAE verifies that the EPGs communicate on protocols other than the protocol specified in the traffic selector field.

iii. Click **Enter EPG Selector B name**, and choose an EPG selector name from the list.

iv. Click **Select Traffic Selector name** and choose a traffic selector name.

5. Click **Save**.

You have created a compliance requirement. For additional details about editing or deleting compliance requirements, see Managing Compliance Requirements.

Creating Compliance Requirement Set

Use this procedure to create a compliance requirement set.

Before You Begin

- At least one epoch analysis has been completed.
- Your EPG selectors and requirements are created.

Procedure

1. Choose **Compliance** > **Manage Compliance Requirements** > **Compliance Requirement Sets**.
2. Click **Create New Compliance Requirement Set**.
3. Complete the following fields for **Create New Compliance Requirement Set**.
   a. In the **Compliance Requirement Set Name** field, enter the name. The name must be unique across all the analyses.
   b. In the **Description** field, enter the description. (Optional step).
   c. In the **Associate to current Assurance Group** field, check the checkbox.

> You can only associate with the current assurance group.

d. In the **Activate this Compliance Requirement Set** field, check the checkbox if you want to activate the requirement set.

> When an epoch runs for a specific assurance group, all the active requirement sets that are associated with that assurance group are verified and validated.

e. In the **Associated Requirements** area, click the **Associate** link to choose the requirements that you want to associate from the **Associate Requirements** table.

> Similarly, you can disassociate requirements by clicking the **Disassociate** link.

f. Click **Save**.

You have created a compliance requirement set. For additional details about editing or deleting compliance requirement sets, see Managing Compliance Requirement Sets.

Smart Event Management

Smart Event Suppression

A smart event in Cisco NAE provides information about the state of your network at the time represented by the epoch. Smart events are categorized as either Critical, Major, Minor, Warning, or Informational. Smart event suppression feature enables you to suppress smart events in the Cisco NAE UI and view only the smart events that are relevant.

Smart Event Suppression Workflow

Smart event suppression workflow includes the following steps:

1. Create event rules: An event rule enables you to match a smart event against a rule using the match criteria.
    - An event rule contains the match criteria required to match a smart event against the rule and the action that should be applied on the matched smart event.
    - You can use attributes such as severity, category, subcategory, event code, affected object, and check code to define the match criteria for the event rule.
    - A match criteria can contain one attribute or multiple attributes.
        - If a match criteria contains multiple attributes, then the events containing all the attributes will be matched.
        - If an match criteria contains multiple check codes, then the events containing any one check code will be matched.
        - If an match criteria contains multiple affected objects, then the events containing all of the affected objects will be matched.
    - If an event rule contains multiple match criteria, then the events containing the union of the match criteria will be matched.
    - Each event rule can have only one action. The options include **Suppressed**, **Never Suppressed**, and **No Action**.
    - An event rule containing the option **Never Suppressed**, supersedes an event rule containing the option **Suppressed**.
    - An event rule containing the option **No Action**, cannot be added to an event ruleset.

See Creating New Event Rule for more information.

2. Add event rules to event rulesets: An event ruleset enables you to group event rules and associate them with an Assurance Group. The event rules are applied when you activate the event ruleset.
    - An event ruleset contains event rules.
    - An event rule can be part of multiple event rulesets.
    - An event ruleset can be associated with an assurance group or with multiple assurance

groups.

    - An event ruleset can be activated or deactivated.
    - When the event ruleset it activated, the event rules are applied.

See Creating New Event Ruleset for more information.

Manage Event Rules

On the **Smart Events** inspector page, the user can create and manage event rules and event rulesets under the **Manage Event Rules** tab.

Current Epoch Event Rules Snapshot

On the **Smart Events** inspector page, the user can view the event rules for the current epoch selected in the timeline under the **Current Epoch Event Rules Snapshot** tab.

Click **Smart Events Count** to view the smart events that match the event rule.

Creating New Event Rule

Use this procedure to create a new event rule.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rule**.
2. Click **Create New Event Rule**.
3. Complete the following fields for **Create New Event Rule**.
   a. In the **Event Rule Name** field, enter the name.
   b. In the **Description** field, enter the description.
   c. From the **Suppression** drop-down list, choose, the action for the event rule. The default is **No Action**. An event rule containing the action **Never Suppressed**, supersedes an event rule containing the action **Suppressed**. An event rule containing the option **No Action**, cannot be added to an event ruleset.
4. Click **Add New Match Criteria** to define the match criteria for the event rule.
   a. Select the attributes for the match criteria. You can use severity, category, subcategory, event code, affected object, and check code to define the attribute for the match criteria.

> If multiple affected objects are included in the match criteria, then the events containing all the affected objects will be matched. If multiple check codes are included in the match criteria, then the events containing any one check code will be matched.

d. Click the ⚙ icon and click **Done**.

e. Check the checkbox for the match criteria.

> If an event rule contains multiple match criteria, then the events containing the union of the match criteria will be matched.

d. Click **Save**.

5. The new event rule is displayed in the **New Event Rule** table below.

Creating New Event Ruleset

Use this procedure to create a new event ruleset.

Before You Begin

- You have created an event rule.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rulesets**.
2. Click **Create New Event Ruleset**.
3. Complete the following fields for **Create New Event Ruleset**.
    a. In the **Event Ruleset Name** field, enter the name.

    b. In the **Description** field, enter the description.

    c. Check the **Associate to Current Assurance Group** checkbox to associate the event ruleset to the current Assurance Group. To activate the event ruleset, it must be associated with an Assurance Group.

    i. To associate the event ruleset at a later time, see Managing Event Rulesets.

    ii. To associate the event ruleset with another Assurance Group, see Managing Event Rulesets.

    d. Check the **Activate this Compliance Requirement Set** checkbox to activate the event ruleset. To activate the event ruleset at a later time, see Managing Event Rulesets.
4. In the **Associate Event Rules** area, click the **Associate Never Suppressed Event Rules** to choose the event rules that you want to associate from the **Never Suppress Event Rule** table. Click **Associate**.
5. In the **Associate Event Rules** area, click the **Associate Suppressed Event Rules** to choose the event rules that you want to associate from the **Suppressed Event Rule** table. Click **Associate**.

> If you include a combination of Never Suppressed Event Rules and Suppressed Event Rules in your event ruleset, the Never Suppressed Event Rules will take precedence over the Suppressed Event Rules.

6. (Optional) To disassociate an event rule, select the event rule and click **Disassociate**.
7. Click **Save**.

Cisco Network Assurance Engine User Access and Authentication

User Access and Authentication

In Cisco NAE, an administrator can choose to configure users on the Cisco NAE appliance itself and not to use external AAA servers. These users are called local users. To configure local users, see Creating a User Account.

Cisco NAE also allows administrators to grant access to users configured on externally managed authentication servers such as Lightweight Directory Access Protocol (LDAP). To authenticate users with an LDAP server See Creating a New Authentication Domain.

A login domain defines the authentication domain for a user. Login domains can be set to the Local, or LDAP. When accessing the UI, the Cisco NAE offers a drop-down list of domains to enable the user to select the correct authentication domain. The default is Local.

Session Management

In Cisco NAE, you can view or delete active user sessions using the REST API. These operations cannot be performed using the GUI.

See the *Cisco Network Assurance Engine REST API User Guide* for more information.

Creating a User Account

Use this procedure to create a new user account. Only an administrator can create a user.

Procedure

1. Choose **Settings** > **User Management**.
2. Click **Create New User Account**.
3. Complete the following fields for **Create New User Account**.
   a. In the **Email** field, enter the email address of the user.
   b. In the **Username** field, enter the username of the user account.
   c. In the **Password** field, enter the password to access the user account.
   d. Click **Save**.

Prerequisites for LDAP

LDAP has the following prerequisites:

- You have configured the LDAP server.
- You have the created the Cisco NAE users on the LDAP server.

- You have created a group for Cisco NAE users.
- You have added the Cisco NAE users to the group.
- You have the base DN, bind DN, and group DN on the LDAP server.

Creating a New Authentication Domain

Use this procedure to create a new authentication domain. Only an administrator can create an authentication domain.

Before You Begin

- You have the host name or IP address, port number, bind DN, base DN, and group DN of the LDAP server.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Authentication Domains** tile.
3. Click **Create New Authentication Domain**
4. Complete the following fields for **Create New Authentication Domain**.
   a. In the **Name** field, enter the name of the authentication domain.
   b. (Optional) In the **Description** field, enter the description of the authentication domain.
   c. From the **Authentication Type** drop-down list, choose the authentication type such as LDAP.
5. Complete the following fields for **LDAP Server Configuration**.
   a. In the **Hostname** field, enter the hostname or the IP address of the LDAP server.
   b. (Optional) Click + to add another hostname. You can configure a maximum of 3 LDAP servers.
   c. Check **LDAPS** check box to connect to the LDAP server using a secure connection.
   d. In the **Port Number** field, enter the port number of the LDAP server. The valid port range is 0-5535.
   e. (Optional) In the **Bind DN** field, enter the bind DN in the format `cn=NAE User,ou=Systems,ou=IT,ou=Departments,dc=nae_customer,dc=com`.
   f. (Optional) In the **Bind Password** field, enter the bind DN password.
   g. In the **Base DN** field, enter the base DN in the format `dc=nae_customer,dc=com`.
   h. In the **Timeout** field, enter the timeout in seconds. The valid timeout range is 0-15 seconds for each host.
   i. In the **Group DN** field, enter the group DN for the Cisco NAE users in the format `cn=NAE group,ou=groups,dc=nae_customer,dc=com`. Only the users belonging to the LDAP group will be granted access to the appliance.
   j. In the **Filter** field, enter the filter in the format `(&(objectclass=person)(cn=$userId))`. Filter

is used as a criteria to search for the user in the LDAP server.

k. The **Attribute** field, is pre-populated.

l. Click **Test Connection** to test the connection for the LDAP server.

    i. From the **LDAP Server** drop-down list, choose the LDAP server.

    ii. Enter the username and password to test the credentials on the LDAP server.

    iii. Click **Test**.

6. Click **Save**.

Managing Cisco Network Assurance Engine

Managing User Accounts

Use this procedure to manage user accounts.

Procedure

1. Choose **Settings** > **User Management**.
2. Select the user account.
3. From the **Action** column, choose the **Settings** icon.
4. To change the password of the user, click **Change Password**. Complete the following fields for **Change Password**.
   a. In the **Current Password** field, enter the current password.
   b. In the **Password** field, enter the new password.
      i. The password must be 8-32 characters long.
      ii. The password must have characters from the following characters types: lowercase, uppercase, digit, symbol.
      iii. The allowed symbols include: _ ! @ # $ % ^ & * ( )
   c. In the **Confirm Password** field, enter the new password again.
   d. Click **Save**.
5. To edit a user account, click **Edit User Account**. Complete the following fields for **Edit User Account**.
   a. In the **Email** field, update the email address.
   b. Click **Save**.
6. To delete a user account, click **Delete**. You cannot delete an Admin user.
   a. In the **Delete User** form, click **Delete**.

Managing Passphrase

In Cisco NAE, an administrator can define the password policy for users accessing the appliance. Use this procedure to configure the password requirements for Cisco NAE.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Passphrase Configuration** tile.
3. Complete the following fields for **Passphrase Configuration**.
   a. From the **Minimum passphrase length** drop-down list, choose the minimum length for the password. The default value is 15 characters.

b. From the **Password lifetime** drop-down list, choose the time (in days) before the user account is disabled if the password is not changed. The default value is 3650 days.

c. From the **Expiry warning period** drop-down list, choose the warning (in days) before the user account is given a grace period if the password is not changed. Expiry warning period is the number of days prior to the **Password lifetime**, when a user is warned that the password is about to expire. The default is 14 days. In addition to the **Password lifetime**, the user is also given a **Grace period** to change the password.

d. From the **Grace period** drop-down list, choose the grace period (in days) before the user account is disabled. Grace period is the number of days in addition to the **Password lifetime** to change the password before the user account is disabled. The default is 3 days.

> ℹ Once the grace period expires, the admin user will be forced to the change the password upon the next log in. Non-admin users will be locked out and the admin user will have to reset their password.

e. From the **Passphrase generation** drop-down list, choose the option to generate an instant password.

Managing Appliance Settings

Use this procedure to manage the Cisco NAE appliance settings.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Appliance Settings** tile.
3. To modify the DNS server, complete the following fields for **DNS Server**.
   a. Enter the IP address of the primary DNS server.
   b. (Optional) Enter the IP address of the secondary DNS server.
4. To modify the NTP server, complete the following fields for **NTP Server**.
   a. Check **Use External NTP Server** check box to configure external NTP server.

> ℹ We recommend that you use an external NTP server to configure NTP servers. We recommend you to set the NTP time in sync with the local time.

i. Enter the domain name of the primary NTP server.

ii. (Optional) Enter the domain name of the secondary NTP server.

   a. Uncheck **Use External NTP Server** check box to configure local NTP server.

5. To modify the SMTP server, complete the following fields for SMTP server.
   a. Enter the host name of the SMTP server.
   b. Enter the port number. Examples include common default ports, SMTP port number 25, or secure SMTP (SSL) port number 465.

   c. (Optional) Check the **SSL** check box to configure SSL for SMTP.
      i. Enter the username and password to access the SMTP server.

6. Click **Submit**.

Managing Assurance Groups

Use this procedure to manage an Assurance Group.

Procedure

1. Choose **Settings** > **Assurance Group Configuration**.
2. Click **Create New Assurance Group** to add an Assurance Group. See Performing Online Analysis.
3. Click the ✎ icon to edit an existing Assurance Group configuration. Stop the analysis before editing an Assurance Group configuration.

   > ℹ To edit a NAT configuration file, download the NAT configuration file template, update the file, and then upload it to the Cisco NAE appliance. See Performing Online Analysis.

4. Click the ⋮ icon delete an Assurance Group.
   - The delete operation only deletes the Assurance Group settings in the Cisco NAE.
   - When you delete the Assurance Group, all the offline analyses corresponding to the Assurance Group will be deleted.
5. Click the 🗎 icon to view the Assurance Group details.

Setting Log Levels

Use this procedure to set the log levels.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Log Level Settings** tile.
3. For each category, choose the log level from the drop-down list. By default, the log levels are set to **Error** setting.
4. Click **Save**.
5. (Optional) Click **Restore to Factory Default**, to reset the log level to the default value.
6. To download the logs, choose **Settings** > **Download Tech Support Logs**.

Deleting Bundle File

Use this procedure to delete the Cisco NAE bundle file.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Software Management** tile.
3. In the Upload table, select the bundle file.
4. From the **Actions** menu, choose **Delete**.
5. Click **Delete**.

Managing Epoch Delta Analysis

Use this procedure to manage a epoch delta analysis.

Procedure

1. Choose **Epoch Analysis** > **Epoch Delta Analysis**.
2. Click **Analysis Management**.
3. In the **Delta Analysis** table, select a delta analysis and click the ✏ icon to edit the name.
4. Click the ⚙ icon and then choose **Delete** to delete the delta analysis. To delete a delta analysis that is running, you must stop the delta analysis before deleting.
5. Click the ⚙ icon and then choose **Stop** to stop a running delta analysis.
6. Click the ⚙ icon and then choose **View Results** to view the results of a delta analysis.

Managing Authentication Domains

Use this procedure to manage authentication domains. Only an administrator can manage authentication domains.

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Authentication Domains** tile.
3. Select the authentication domain.
4. From the **Action** column, choose the **Settings** icon.
5. To edit an authentication domain, click **Edit**. You cannot edit the name of the authentication domain.
6. To delete an authentication domain, click **Delete**. You cannot delete the Local authentication domain.

When you delete an authentication domain, all the users in the authentication domain will be logged out from the appliance.

Managing EPG Selectors

Use this procedure to manage EPG selectors.

Before You Begin

- You have created at least one EPG selector.

Procedure

1. Choose **Compliance & Audit** > **Manage Compliance Requirements** > **EPG Selectors**.
2. In the EPG Selector table that is displayed, click the ⚙ icon in the **Action** column for the EPG selector you want to manage.
3. Choose the action to perform from the following options:
    a. Choose **Edit** to edit the EPG selector from the EPG Selectors table.
    b. Choose **Delete** to delete the EPG selector, and in the **Delete EPG Selector** dialog box that is displayed, confirm **Delete**.

If the EPG Selector that you want to delete is used in a requirement, remove the association and then delete the EPG selector.

Managing Traffic Selectors

Use this procedure to manage traffic selectors.

Before You Begin

- You have created at least one traffic selector.

Procedure

1. Choose **Compliance & Audit** > **Manage Compliance Requirements** > **Traffic Selectors**.
2. In the Traffic Selector table that is displayed, click the ⚙ icon in the **Action** column for the Traffic selector you want to manage.
3. Choose the action to perform from the following options:
    a. Choose **Edit** to edit the traffic selector from the Traffic Selectors table.
    b. Choose **Delete** to delete the traffic selector, and in the **Delete Traffic Selector** dialog box that is displayed, confirm **Delete**.

If the Traffic Selector that you want to delete is used in a requirement, remove the association and then delete the traffic selector.

Managing Compliance Requirements

Use this procedure to manage compliance requirements.

Before You Begin

- You have created at least one compliance requirement.

Procedure

1. Choose **Compliance & Audit** > **Manage Compliance Requirements** > **Compliance Requirements**.
2. Click the ⚙ icon in the **Action** column for the compliance requirement you want to manage.
3. Choose the action to perform from the following options:
   a. Choose **Edit** to edit the compliance requirement from the **Edit Compliance Requirement** area.
   b. Choose **Delete** to delete the compliance requirement, and in the **Delete Compliance Requirement** dialog box that is displayed, confirm **Delete**.

If the Compliance Requirement that you want to delete is used in a requirement set, remove the association and then delete the Compliance Requirement.

Managing Compliance Requirement Sets

Use this procedure to manage compliance requirement sets.

Before You Begin

- You have created at least one compliance requirement set.

Procedure

1. Choose **Compliance & Audit** > **Manage Compliance Requirements** > **Compliance Requirement Sets**.
2. Click the ⚙ icon in the **Action** column for the compliance requirement you want to manage.
3. Choose the action to perform from the following options:
   a. Choose **Edit** to edit the compliance requirement set from the **Edit Requirement Set** area.
   b. Choose **Delete** to delete the compliance requirement set, and in the **Delete Requirement Set** dialog box that is displayed, confirm **Delete**.

Managing Event Rules

Use this procedure to manage event rules.

Before You Begin

- You have created at least one event rule.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rules**.
2. Select an event rule and click the ⚙ icon in the **Action** column to perform the following actions:
   a. Choose **Edit** to edit the event rule.
   b. Choose **Copy** to copy the event rule.
   c. Choose **Delete** to delete the event rule.
3. Click an event rule to view the details of the event rule.

Managing Event Rulesets

Use this procedure to manage event rulesets.

Before You Begin

- You have created at least one event ruleset.

Procedure

1. Choose **Smart Events** > **Manage Events Rules** > **Event Rulesets**.
2. Select an event ruleset and click the ⚙ icon in the **Action** column to perform the following actions:
   a. Choose **Associate** to associate the event ruleset to the current Assurance Group.
   b. To associate the event ruleset to a different assurance group,
      i. Select the Assurance Group from the **Assurance Group** drop-down list.
      ii. Select the event ruleset and click the ⚙ icon in the **Action** column.
      iii. Choose **Associate**.
   c. Choose **Activate** to activate the event ruleset. To activate an event ruleset, it must be associated with an Assurance Group. Activating an event ruleset not associated with an Assurance Group, automatically associates the event ruleset with the current Assurance Group and activates the event ruleset.
   d. Choose **Disassociate** to disassociate the event ruleset from the current Assurance Group. Disassociating an active event ruleset will deactivate the event ruleset.
   e. Choose **Deactivate** to deactivate the event ruleset.

f. Choose **Edit** to edit the event ruleset.

g. Choose **Copy** to copy the event ruleset.

h. Choose **Delete** to delete the event ruleset. Deleting a ruleset does not delete the rules included in the ruleset.

Upgrading and Downgrading Cisco Network Assurance Engine

Supported Upgrade Paths for Cisco NAE

The following table lists the supported upgrade paths for the Cisco NAE.

Table 6. Supported Upgrade Paths for Cisco NAE

From	To
3.0(1a)	3.1(1)
2.1(1b)	3.0(1a)
2.0(1b)	2.1(1b)

Important Notes

> ℹ Before starting the upgrade process you must create snapshots of the VM. See Creating VM Snapshots

- During the upgrade process, ensure that the connectivity to the Cisco NAE is not disrupted and the power to any of the Cisco NAE VMs is not disconnected. Failure to comply can lead to the appliance being in an unusable state.
- Unusually high datastore read/write latency could lead to upgrade failures.
- During the upgrade process, ensure that all the VMs are up and running. Partial upgrades of the VMs is not supported.
- Upgrading from release 2.0(1b) to release 3.0(1a) is a two step process.
  1. Upload the bundle for release 2.1(1b) and upgrade to release 2.1(1b).
  2. Upload the bundle for 3.0(1a) and upgrade to release 3.0(1).

> ℹ Do not upload the 2.1(1b) and 3.0(1a) bundles simultaneously.

Upgrading Cisco NAE OVA

Use this procedure to upgrade the Cisco NAE OVA.

Before You Begin

- You have downloaded the Cisco NAE bundle file.
- All the VMs must be active at the time of the upgrade process.
- You have created snapshots of the VM. See Creating VM Snapshots

Procedure

1. Choose **Settings** > **Appliance Administration**.
2. Click the details icon on the **Software Management** tile.
3. Click **Upload Bundle File** to upload the bundle file targeted for upgrade.
4. In the **Upload Bundle File** form, complete the following fields.
   a. Click **Browse** to upload the bundle file.
   b. Select the **Upload Bundle File**.
   c. Click Add. After the file has been uploaded successfully, it is displayed in the Upload table.
5. In the Upload table, select the bundle file.
6. From the **Actions** menu, choose **Install**. The **Software Management** form displays the status of the software upgrade for each individual virtual machine in the Cisco NAE appliance cluster. After the upgrade has been completed successfully, the Cisco NAE login page appears. Choose **Install** only from one VM to upgrade the entire Cisco NAE cluster.
7. Enter your credentials to access the Cisco NAE UI.

> ℹ You must perform the online analysis on any Assurance Group only after the upgrade has been completed successfully.

Troubleshooting Upgrade Failure

Contact Cisco TAC immediately for any issues related to the upgrade process. If you encounter any issues related to the upgrade process, leave the system in the original failed state and contact Cisco TAC.

See Downloading Logs for information on downloading tech support logs.

Creating VM Snapshots

Use this procedure to create VM snapshots.

Procedure

1. Stop all online analysis.
   a. Choose **Settings** > **Assurance Configuration**.
   b. Select the Assurance Group and click the **Stop** icon.
2. Log in to VMware vCenter or vSphere Client and shut down all the VMs of the Cisco NAE appliance.

> ℹ Use the normal shutdown procedure using **Shutdown Guest OS** to shut down the VMs. Do not use the **Power Off** option.

3. In the vCenter or vSphere Client, create a new snapshot of each VM of the Cisco NAE appliance.

4. Power on all the VMs of the Cisco NAE appliance. You must power on all the VMs only once all the snapshots have been successfully completed.

Downgrading Cisco NAE

Important Notes

- You cannot downgrade from within the Cisco NAE appliance from the following releases:
    - Release 3.1(1) to 3.0(1a)
    - Release 3.1(1) to 2.1(1b)
    - Release 3.0(1a) to 2.1(1b)
    - Release 2.1(1b) to release 2.0(1b)
- After you upgrade to the release 3.1(1), 3.0(1a) or 2.1(1b), you cannot downgrade back to the release 3.0(1a), 2.1(1b) or 2.0(1b) build from which the upgrade was performed.
    - If downgrade capability is desired, you **must** take a VM snapshot before performing the upgrade. See Creating VM Snapshots.
    - Any configuration, as well as epochs and smart events generated after upgrading will be lost after a downgrade.
    - Before choosing to restore the cluster from the VM snapshot, contact Cisco TAC to see if any problem can be resolved without needing to take this action.
- The VM snapshot will continue to grow in size and consume disk space if it is kept for a long period of time. Ensure that you eventually delete the VM snapshot.

Troubleshooting

Downloading Logs

Use this procedure the download the logs for the Cisco NAE appliance.

Procedure

1. Choose **Settings** > **Download Tech Support Logs**. The logs are collected from each VM in the cluster and they are aggregated into a tar file. Downloading logs can take up to several minutes.
2. (Optional) If it is taking more than 5 minutes for the tech support logs to be downloaded, you can access the logs using the following procedure. You can also use this procedure, if you receive an error message while downloading the tech support logs.
   a. Contact Cisco TAC to obtain the one time password (OTP) for root access.
   b. Log in to one of the VMs of the appliance as root.
   c. Run the following command:

   ```
   /usr/lib/candid/share/support/tech_support --logs --dir /hadoop/network-audits
   --output tech_support
   ```

   d. Download the following tar file from the VM and provide it to TAC for debugging.

   ```
   /hadoop/network-audits/tech_support.<timestamp>.tar
   ```

Appliance Events

Cisco NAE raises **Appliance Events** to monitor the health of the appliance. These events are generated as part of the cron job that is installed on all the hosts and the cron job is configured to run every 5 mins. The **Appliance Events** are useful for troubleshooting the appliance.

Procedure

1. Choose **Settings** > **Appliance Status**.
2. Click **Event Name** to view the details of the event.

Appliance Event Types

The **Appliance Events** are categorized into the following types.

Provisioned Capacity Events

These events monitor the appliance capacity provisioned with respect to the defined specifications of the appliance. These events are generated at every reboot. The different specifications are defined for the different flavors of the appliance. The following events are included in this category.

1. APPLIANCE_PROVISIONED_CAPACITY_BELOW_SPEC
2. APPLIANCE_PROVISIONED_CAPACITY_ABOVE_SPEC
3. APPLIANCE_PROVISIONED_CAPACITY_AT_SPEC

Local Filesystem Usage Events

These events monitor the storage usage on each of the hosts.

The following events are included in this category.

1. APPLIANCE_FILESYSTEM_NORMAL
2. APPLIANCE_FILESYSTEM_EXCEEDED_LOW_WATERMARK
3. APPLIANCE_FILESYSTEM_EXCEEDED_HIGH_WATERMARK

Web Server Events

These events monitor the health of the web servers. The following events are included in this category.

1. APPLIANCE_WEB_SERVICES_OPERATION_NORMAL
2. APPLIANCE_WEB_SERVICES_PARTIAL_FAILURE
3. APPLIANCE_WEB_SERVICES_COMPLETE_FAILURE

Application Server Events

These events monitor the health of the application servers. The following events are included in this category.

1. APPLIANCE_APPLICATION_OPERATION_NORMAL
2. APPLIANCE_APPLICATION_PARTIAL_FAILURE
3. APPLIANCE_APPLICATON_COMPLETE_FAILURE

Database Events

These events monitor the health of the database. The following events are included in this category.

1. APPLIANCE_DATABASE_OPERATION_NORMAL
2. APPLIANCE_DATABASE_PARTIAL_FAILURE
3. APPLIANCE_DATABASE_REACHED_LOW_THRESHOLD
4. APPLIANCE_DATABASE_AT_PURGE_LIMIT

Analysis Latency Events

These events monitor the time taken to analyze the data. Each analysis is associated with an analysis interval and analysis must be completed within the specified interval time.

The following events are included in this category.

1. ANALYSIS_COMPLETED
2. ANALYSIS_COMPLETED_BUT_TOOK_TOO_LONG

Analysis Application Events

These events monitor the health of the analysis application.

The following events are included in this category.

1. APPLIANCE_ANALYSIS_ENGINE_OPERATION_NORMAL
2. APPLIANCE_ANALYSIS_ENGINE_FAILURE

HDFS Filesystem Events

These events monitor the health of the namenodes and datanodes.

The following events are included in this category.

1. APPLIANCE_FILESYSTEM_OPERATION_NORMAL
2. APPLIANCE_FILESYSTEM_PARTIAL_FAILURE
3. APPLIANCE_FILESYSTEM_COMPLETE_FAILURE

YARN Events

These events monitor the health of the resource Managers and node managers.

The following events are included in this category.

1. APPLIANCE_INFRA_RESOURCE_OPERATION_NORMAL
2. APPLIANCE_INFRA_RESOURCE_PARTIAL_FAILURE
3. APPLIANCE_INFRA_RESOURCE_COMPLETE_FAILURE

Host Reachability Events

These events monitor if all the hosts are reachable from all other hosts in cluster. A ping test is used to test reachability of the hosts.

The following events are included in this category.

1. ALL_CLUSTER_MEMBERS_ARE_REACHABLE
2. CLUSTER_MEMBER_REACHABILITY_ERROR

Troubleshooting Scenarios

This section contains information about possible solutions for common troubleshooting scenarios for the Cisco NAE appliance.

Problem

Unavailability of the datastore in the host results in the failure of the file system IO located in the guest VM of the Cisco NAE appliance. As a result, the guest VM’s kernel filesystem driver marks the mounted file system as read-only making the Cisco NAE appliance unavailable. The functionality of the Cisco NAE appliance such as generating new epochs, collecting tech support logs, and accessing the UI is affected.

Solution

To resolve this issue, contact Cisco TAC.