Cisco Network Assurance Engine Installation and Upgrade Guide, Release 4.0(1)

Table of Contents

First Published: 2019-08-19

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

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.

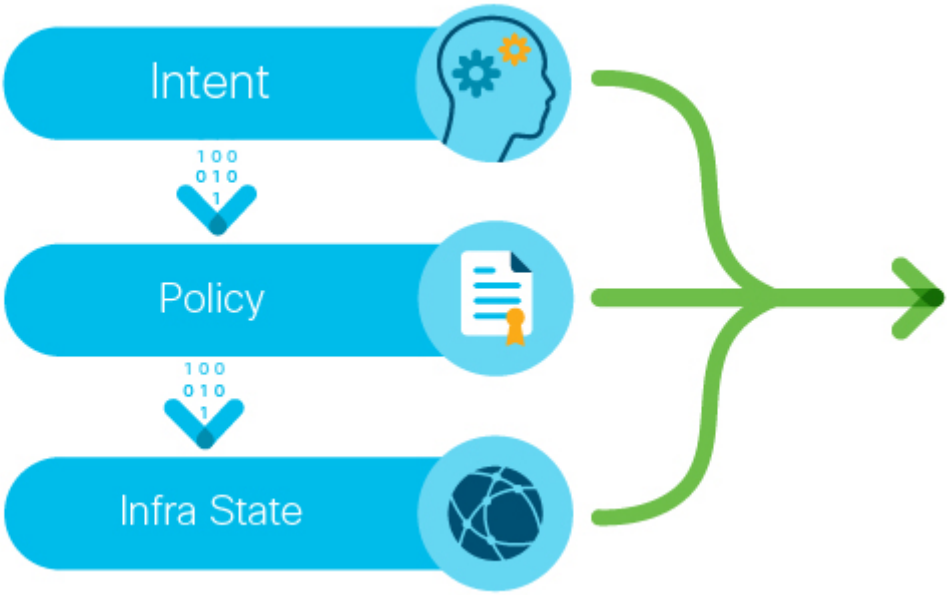

Figure 1. Taking the intent, policy, and the infra state from a device

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:

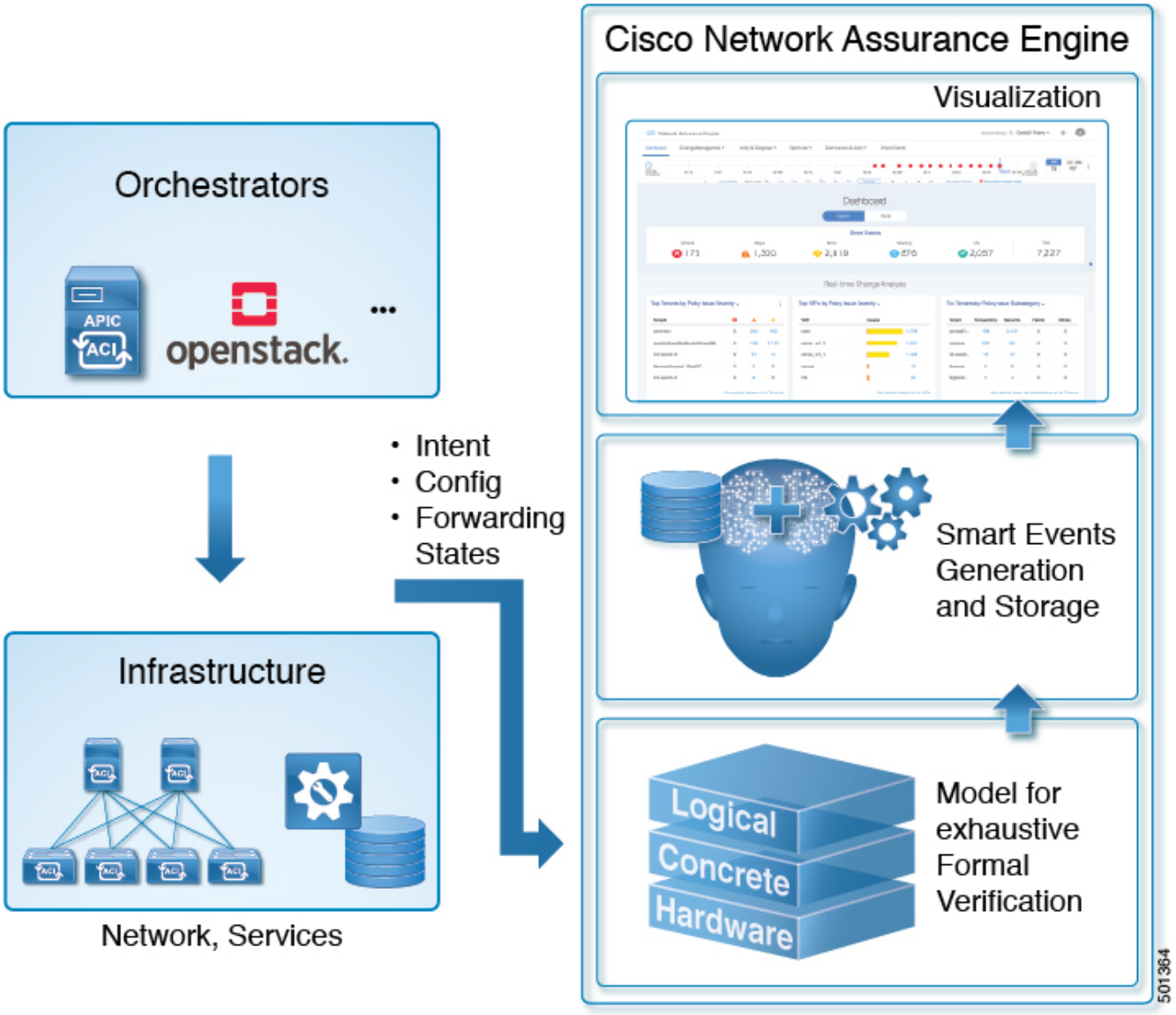

Figure 3. Cisco NAE Architecture

- 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.

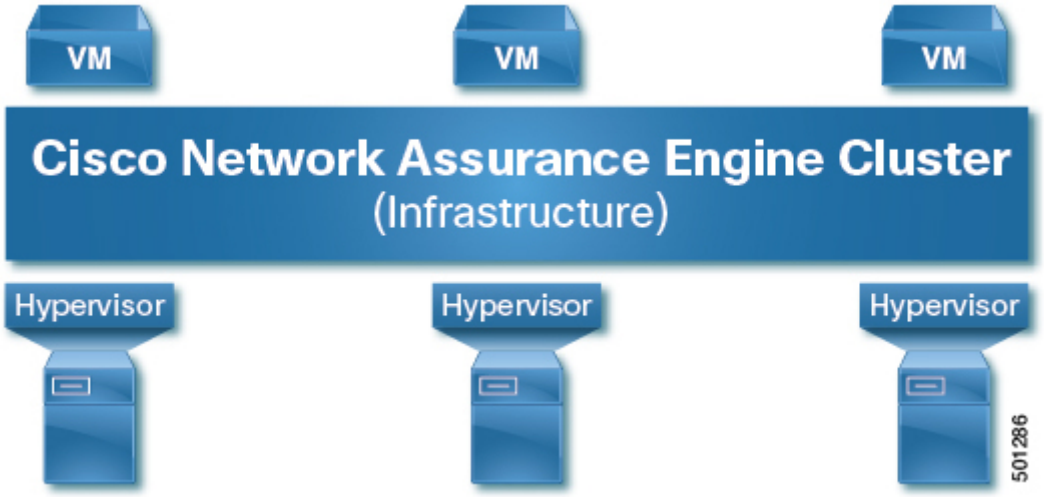

Figure 4. Cisco NAE Appliance

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.

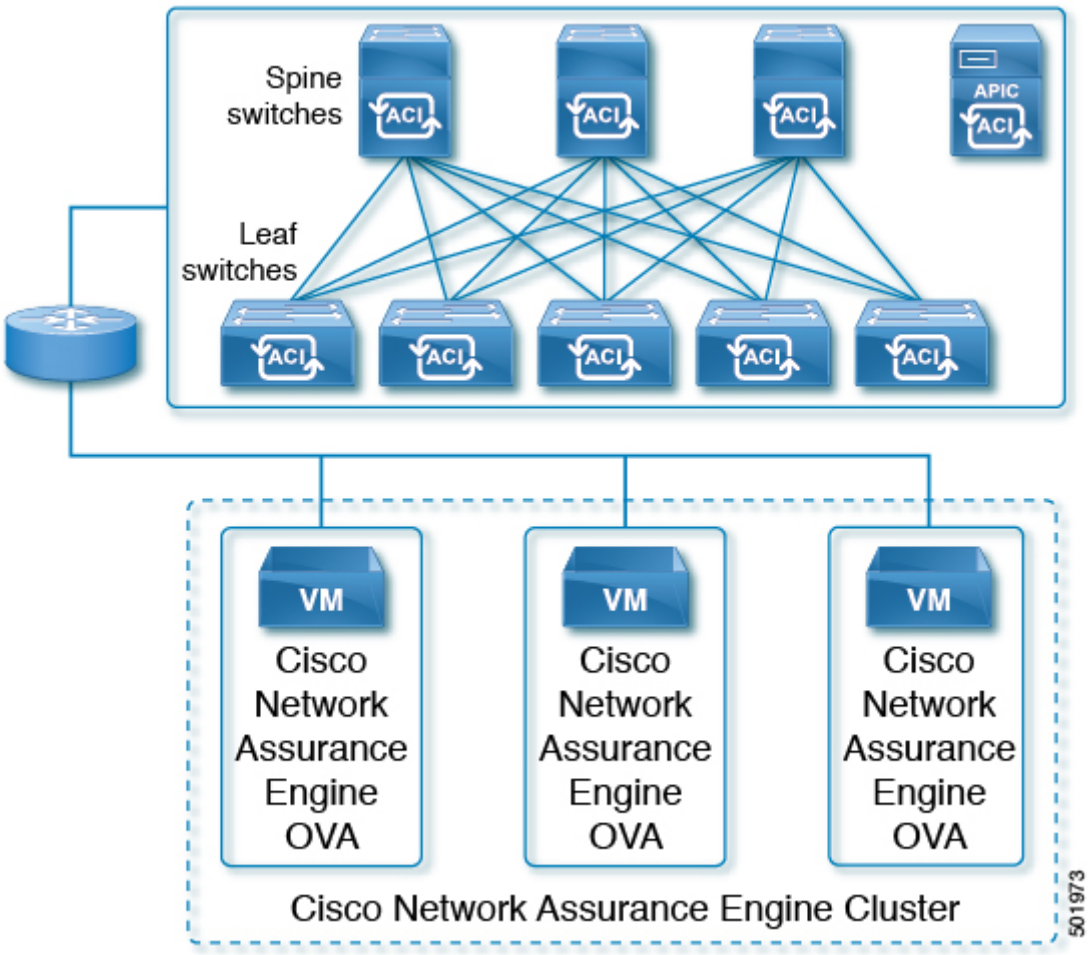

Figure 5. Out-of-Band Management Access

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.

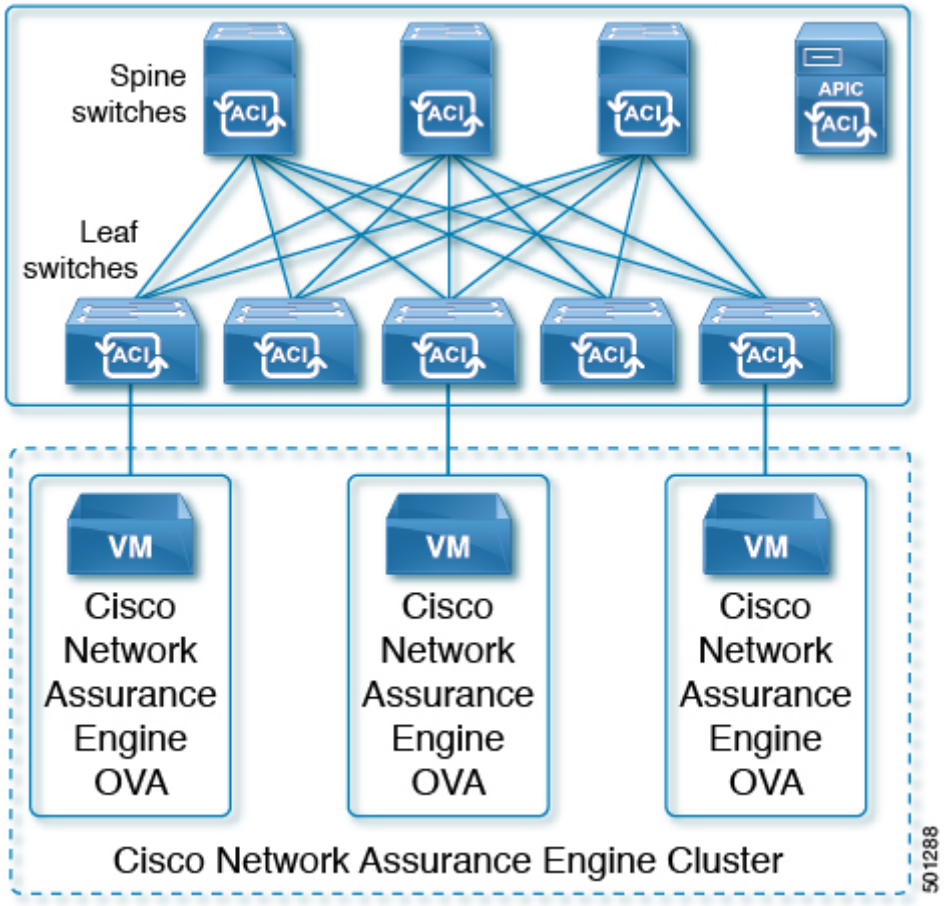

Figure 6. In-Band Management Access

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

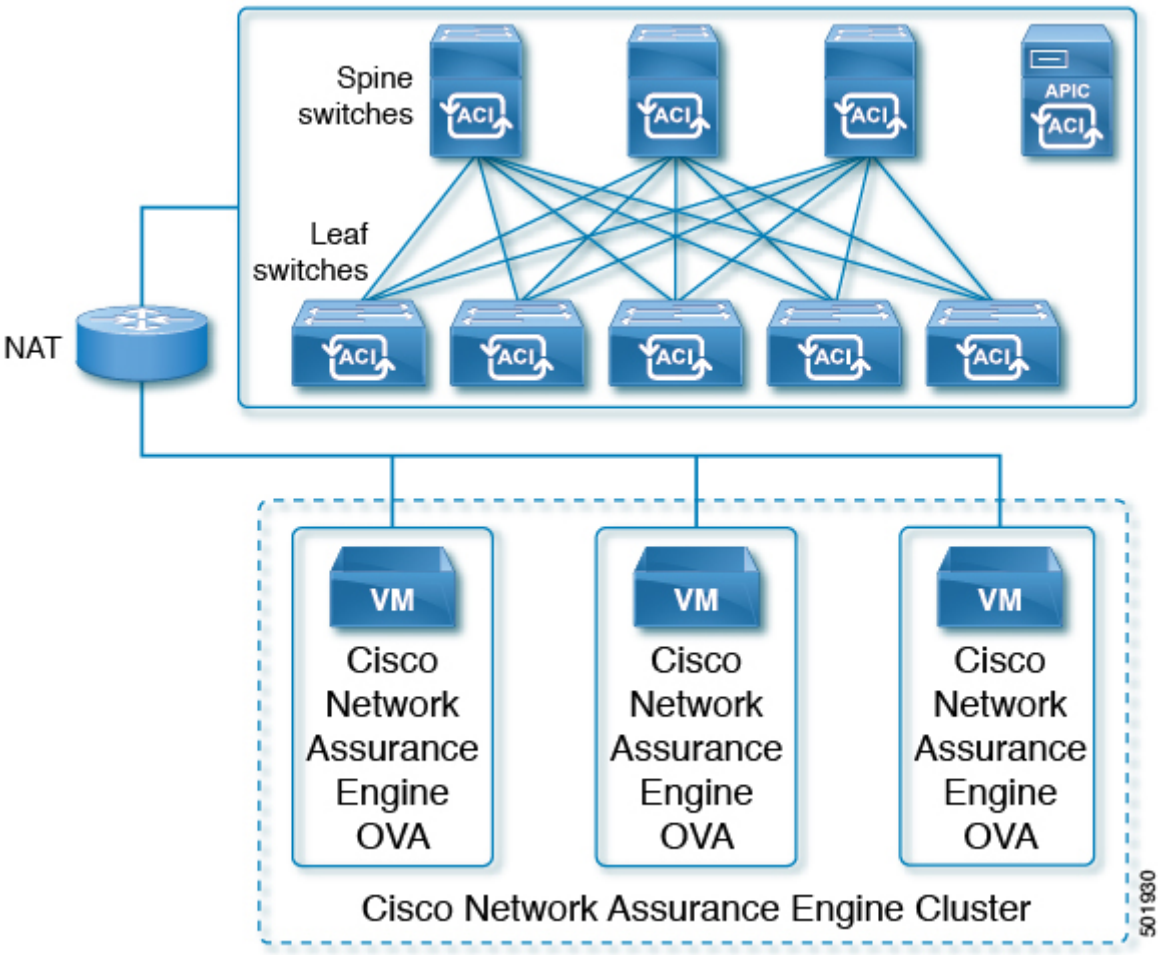

Figure 7. NAT with Out-of-Band Management Access

- NAT with in-band management interface

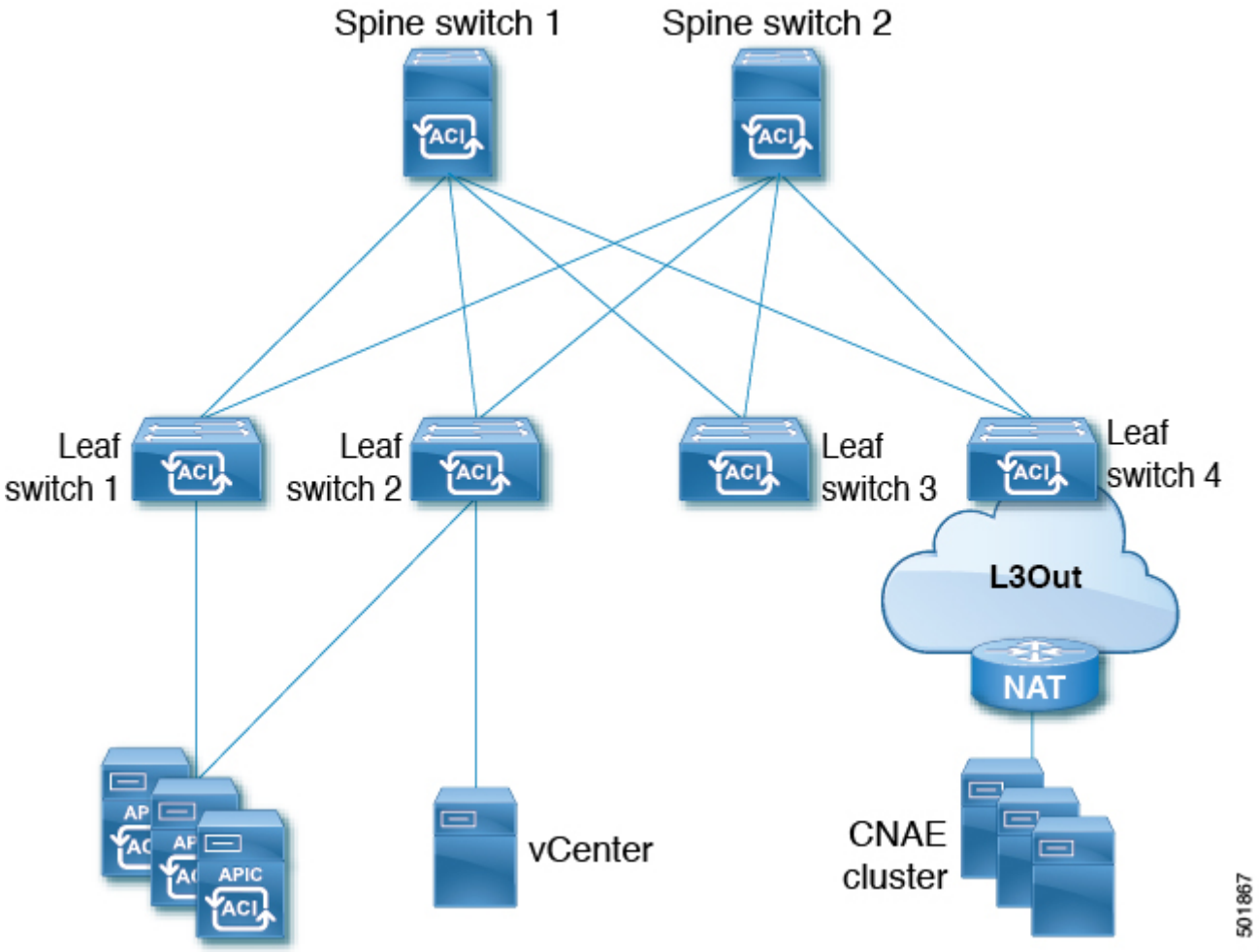

Figure 8. NAT with In-Band Management Access

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 is comprised of the entire ACI fabric. An ACI fabric is made up of the APIC host and all leaf switches and spine switches controlled by the APIC controller. All the network nodes (APIC controller, leaf switches and spine switches) are analyzed together as part of the Assurance Group.

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 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 a later 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.

Beginning with release 4.0(1), you can analyze multiple Assurance Groups. See the *Cisco NAE Getting Started Guide* for more information.

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
  - Network latency requirement for reachability to APIC or fabric <30ms latency and 500Mbps bandwidth.

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`.

- VMware vSphere vMotion or live migration must be disabled for all three VMs in the NAE cluster.

Supported Browsers

- Chrome

Cisco HyperFlex Systems Support

The following section lists the system requirements for Cisco NAE on Cisco HyperFlex Systems.

Requirement	Description
HyperFlex Model	HX240c M5 SFF Hybrid (HX240C-M5SX)
HyperFlex Release	4.0(1b)
VMware vSphere Release	VMware ESXi 6.5
Number of servers	3
Memory	• Free: 433.58 GB • Used: 78.07 GB • Capacity: 511.65 GB
Storage	SSD
Disk	1.5 TB * 18
Processor	Intel® Xeon® Platinum 8176 CPU @ 2.10GHz

Software Compatibility Information

The following table lists the compatibility information for the Cisco NAE.

Release versions of the Cisco APIC and the Cisco NX-OS software that are not listed in the table below are not supported.

Table 2. Cisco ACI Compatibility Information

Cisco APIC Release	Cisco ACI-Mode NX-OS Switch Software Release for Cisco Nexus 9000 Series ACI-Mode Switches
4.1	14.1
4.0	14.0
3.2	13.2
3.1	13.1
3.0	13.0
2.3	12.3
2.2	12.2
2.1	12.1
2.0	12.0
1.3	11.3
1.2	11.2

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
- Remote Leaf

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
- Contract and Filters: For contracts, Policy CAM Optimization is supported. Standard contracts with deny action are also supported. Earlier, standard contracts with permit action only were supported. (To get further details, see Policy CAM Optimization Is Assured.)

EPG

- Application EPG
- External L3Out EPG
- Contract Preferred Group

Access Domain Profile

- Physical
- L3OutP

Smart Event Use Cases

- Policy Analysis
- Tenant End Points
- Tenant Forwarding
- Tenant Security
- Policy CAM Optimization (To get further details, see Policy CAM Optimization Is Assured.)

APIC Connectivity to Cisco NAE

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

Policy CAM Optimization Is Assured

Policy CAM Optimization is assured by Cisco NAE.

In Cisco NAE release 4.0(1), for Policy CAM optimization, the **Enable no stats** directive in contract subjects is supported. Policy CAM optimization using the **Enable Policy Compression** directive in contract subjects is not supported. The **Enable no stats** directive is available starting in the Cisco APIC Release 3.2(x) feature set. The **Enable Policy Compression** directive is available in the Cisco APIC Release 4.0(x) feature set.

ACI Features Not Supported by Cisco NAE

The following ACI features are not supported by the Cisco NAE

- Cisco ACI Multi-Site
- Microsegmentation
- vPOD
- 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.

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
Policy CAM Rules	200 K	400 K	400 K
Endpoints	50 K	100 K	100 K
Number of Prefix Matches	25 K	50 K	50 K
Total number of smart events, endpoints, and prefixes	300 K	500 K	600 K
Number of Concurrent Assurance Analysis	1	1	1
Analysis Interval in ACI Network Mode	15 minutes or more	15 minutes or more	30 minutes or more
Analysis Interval in ACI Application Mode	25 minutes or more	15 minutes or more	Not Supported

Table 4. Verified Scalability Limits for Compliance

Compliance Checks	Scale Limit
Total number of Requirement Sets that can be active at a given time	3
Number of Requirements per Requirement Set	10
EPG pair limit check per Requirement (includes both directions)	1000
Fabric wide rules	150 K

Table 5. Verified Scalability Limits for Explorer

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

Important Notes

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

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

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

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.
- If the 3 Cisco NAE VMs are being deployed across multiple servers, then the servers must be time synced to the same time source before setting up the Cisco NAE appliance or the installation will fail during database setup. See Seeting Up Cisco NAE Appliance.

Guidelines and Limitations

Cisco NAE release 4.0(1) introduces the global search feature. In order to support this feature without increasing the VM footprint of the Cisco NAE cluster, Cisco NAE will only function if all three VMs are up and running. This differs from previous releases, where Cisco NAE would continue to function in a degraded mode if a single VM was lost.

In the event of a single VM being lost, you may access the NAE GUI on either of the two remaining VMs.

To view the details about the state of the cluster, navigate to **Settings** > **Appliance Status** > **Appliance Installation Status**.

You may be able to recover the single VM that was lost by rebooting that VM. If more assistance is needed in recovering the cluster, contact Cisco TAC.

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 the *Cisco NAE Getting Started Guide*.
    b. To perform offline analysis, see the *Cisco NAE Getting Started Guide*.
4. Configure local users or configure authentication domains .
    a. To configure local users for accessing the Cisco NAE appliance, see the *Cisco NAE Getting Started Guide*.
    b. To configure authentication domains, see the *Cisco NAE Getting Started Guide*.

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**.

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.

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.

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.

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 LDAP Certificate

Use this procedure to upload a LDAP certificate.

Before you begin

- You have obtained the LDAP server certificate.
- You have the permission to access and upload the certificate.
- You have the certificate path and certificate alias.

Procedure

1. Obtain the LDAP server certificate from your LDAP server administrator.
2. Upload the file (.crt, .cer or .pem) to the server.

`scp ldapserver.crt admin@` *VM IP address* `:/tmp`

The certificate file must be in PEM format.

3. Log in to a VM in the Cisco NAE appliance as the admin user.
4. Change the file permissions to 755.

Example:

```
chmod 755 /tmp/ldapserver.crt
```

5. Run the command:

`python /lib/candid/python/InstallLdapCertificate.py.`

6. Enter the admin password.
7. Enter the certificate path. Certificate path is the location of the LDAP certificate in PEM format.

Example:

`/tmp/ldapserver.crt`

8. Enter the certificate alias. Certificate alias name is human readable alpha numeric assigned to the certificate in the application.

Once the certificate in installed, you will receive the message *LDAP certificate installation is successful.*

9. To use the installed certificate, log in to the Cisco NAE appliance using the chrome browser. In the Log in page from the drop-down list, select the authentication domain.
10. (Optional) Run the command `python /lib/candid/python/GetLdapCertificate.py` to check the installed certificates.
11. (Optional) Run the command `python /lib/candid/python/DeleteLdapCertificate.py` to delete installed LDAP certificate. You cannot delete the default certificate.

Troubleshooting

The following table describes how to troubleshoot installation issues.

Table 6. Error Messages

Error Messages	Solution
Given certificate path `/tmp/ldapserver.crt` is not present	Verify the file path and permission as mentioned step 4.
Given certificate `/tmp/ldapserver.crt` is not in the expected file extensions (.cer, .pem, .crt)	Verify the file extension. The supported file extensions are .cer, .pem, and .crt.
Given certificate `tmp/ldapserver.crt` is not valid	Verify the integrity of certificate.
Provided LDAP certificate already exists	The LDAP certificate is already installed.

Uploading A Certificate Authority Signed Certificate for the Web Server

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

After installing the Cisco NAE appliance, you can replace the default web server certificate 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 web server certificate, the certificate path and certificate key path are available.

Procedure

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. Choose one of the IP addresses in your NAE cluster and create a DNS entry for that IP address with the desired server name.

For example, if you installed the NAE cluster on IP addresses 10.0.0.7, 10.0.0.8, and 10.0.0.9, you should create the DNS entry to map `cisco-nae.your-domain.com` to 10.0.0.9.

2. Generate a Certificate Signing Request (CSR) with OpenSSL. You must use RSA, and we recommend a key size of 2048 bits.

Example:

```
openssl req -new -newkey rsa:2048 -nodes -keyout webserver.key -out webserver.csr
```

3. When prompted to enter the common name for the certificate, enter the fully-qualified domain name (FQDN). Ensure that it matches the DNS entry you created in step 1.
4. Order your CA signed web server certificate using the contents of the Certificate Signing Request (.csr) file you just created.

Too access all the VM's with the same certificate, add the hostnames as Subject Alternative Names (SANs) while requesting the certificate.

5. Keep the Private Key (.key) file in a safe location, following your organization's Information Security recommendations.
6. Once you receive your CA signed web server certificate file, upload both the certificate file (.crt, .cer, or .pem) and the private key file (.key) to the server:

```
scp webserver.crt admin@cisco-nae.your-domain.com:/tmp
```

```
scp webserver.key admin@cisco-nae.your-domain.com:/tmp
```

The certificate file must be in PEM or DER format, and the private key file must be in PEM format.

7. Log in to a VM in the Cisco NAE appliance as the admin user.
8. Change the file permissions to 755.

Example:

```
chmod 755 /tmp/webserver.crt chmod 755 /tmp/webserver.key
```

9. Run the command:

```
python /lib/candid/python/InstallWebCertificate.py
```

10. Enter the admin password.
11. Enter the certificate path. Certificate path is the location of the CA signed web server certificate in PEM or DER format.

Example:

```
/tmp/webserver.crt
```

12. Enter the private key path. Private key path is the location of the key for the certificate file in PEM format.

Example:

```
/tmp/webserver.key
```

The private key path must not be protected by a password.

Once the web certificate in installed, you will receive the message *Web Certificate installation is successful. Delete the additional copy of the private key*. You must delete the additional copy of the private key that has 755 permissions.

13. To view the certificate, log in to the Cisco NAE appliance using the Chrome browser.

Click More Tools > Developer Tools > Security > View Certificate to view the certificate.

The certificate will be installed on the VM on which the script is executed. Repeat the procedure to install the certificate on the remaining virtual machines in the Cisco NAE cluster.

Troubleshooting

The following table describes how to troubleshoot installation issues.

Table 7. Error Messages

Error Messages	Solution
Given certificate path `/tmp/webserver.crt` is not present	Verify the file path and permission as mentioned in step 8.
Given certificate key path `/tmp/webserver.key` is not present	Verify the file path and permission as mentioned in step 8.
Given certificate `/tmp/webserver.crt` is not in the expected file extensions (.cer, .pem, .crt)	Verify the file extension. The supported file extensions are .cer, .pem, and .crt.
Given certificate key `/tmp/webserver.key` is not in the expected file extensions (.key)	Verify the file extension. The supported file extension is .key.

Error Messages	Solution
Given certificate `tmp/webpserver.crt` is not valid	Verify the integrity of certificate.
Given certificate `tmp/webpserver.key` is not valid	Verify the integrity of certificate.
Could not start Apache server with the given certificate/key. Verify the certificate-key pair. Restored old certificates.	Verify if the certificate-key pair is valid.

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 8. Supported Upgrade Paths for Cisco NAE

From	To
4.0(1a)	4.0(1b)
4.0(1)	4.0(1b)
3.1(1)	4.0(1b)
3.0(1a)	3.1(1)
2.1(1b)	3.0(1a)
2.0(1b)	2.1(1b)

Important Notes

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).

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

- When you upgrade from Cisco NAE release 2.0(1) or 2.1(1) to release 4.0(1), the epochs from the releases 2.0(1) and 2.1(1) will not be visible in the GUI . To access the epochs from the releases 2.0(1) and 2.1(1), contact your Cisco account team before the upgrade.
- Prior to upgrading to Cisco NAE release 4.0(1), you must delete all the unnecessary offline analysis files using the **Offline File Management** page in the NAE GUI. See the section *Managing Offline Analysis* in the *Cisco NAE Getting Started Guide* for more information.
- If a large number of offline analysis files (100 or more) were uploaded to the previous releases

of NAE, then after upgrading to NAE release 4.0(1), there may be a lag of up to two hours before the uploaded files from the previous releases are available for analysis. This lag does not impact the offline analysis files that are uploaded to NAE release 4.0(1).

- To address the issue in CSCvo182291, Cisco has released the Security Advisory, Cisco Network Assurance Engine CLI Access with Default Password Vulnerability. The default password vulnerability affects Cisco NAE Release 3.0(1) and is fixed in Cisco NAE Release 3.0(1a). To upgrade to Cisco NAE Release 3.1(1), you must first upgrade to Cisco NAE Release 3.0(1a). After upgrading from Cisco NAE Release 3.0(1) to Cisco NAE Release 3.0(1a), you must change the administrator password using the GUI to fix the vulnerability.

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. Download the Cisco Network Assurance Engine Virtual Appliance upgrade bundle from Cisco.com.
2. Unzip the file. When you unzip the file, the following 2 files are displayed
   - nae_ova-*release number*.bundle
   - nae_ova-*release number*.bundle.md5sum

   

   You must upload the nae_ova-*release number*.bundle file to the Cisco NAE appliance.

3. Choose **Settings** > **Appliance Administration**.
4. Click the details icon on the **Software Management** tile.
5. Click **Upload Bundle File** to upload the bundle file (nae_ova-*release number*.bundle) targeted for upgrade.
6. 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.
7. In the Upload table, select the bundle file.
8. 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.

9. Enter your credentials to access the Cisco NAE GUI.

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 the *Cisco NAE Getting Started Guide* 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.

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.
- After you upgrade to the release 4.0(1), 3.1(1), 3.0(1a) or 2.1(1b), you cannot downgrade back to the release 3.1(1), 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.