Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide, Release 1.0.x

First Published: November 02, 2015

Last Modified: November 06, 2015

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 figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in 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)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Audience

This publication is for experienced network administrators who will deploy the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) in their network. Use this guide to deploy, make secure, access, verify, and troubleshoot the Cisco APIC-EM.

For information about using the controller's GUI for the first time, see the *Cisco APIC-EM Quick Start Guide*.

Note The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to within this deployment guide as a controller.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.

Convention	Description
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

- Cisco APIC-EM Documentation:
  - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for Cisco Network Plug and Play*
  - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
  - *Cisco Open Plug-n-Play Agent Configuration Guide*

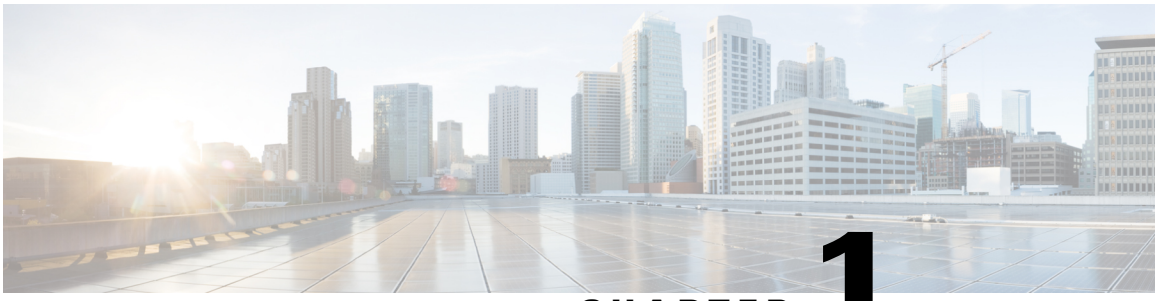
- *Mobile Application User Guide for Cisco Network Plug and Play*

Note For information about developing your own application that interacts with the controller by means of the Northbound REST API, see the developer.cisco.com/site/apic-em Web site.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

Overview

About the Cisco Application Policy Infrastructure Controller Enterprise Module

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's SDN Controller for Enterprise Networks (Access, Campus, WAN and Wireless).

The platform hosts multiple applications (SDN apps) that use open Northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs
- Saves time, resources, and costs through advanced automation
- Transforms business intent policies into a dynamic network configuration
- Provides a single point for network wide automation and control

The following table describes the features and benefits of the Cisco APIC-EM.

Table 1: Cisco APIC Enterprise Module Features and Benefits

Feature	Description
Network Information Database (NIDB)	The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. You can use this interactive feature to troubleshoot your network.
Cisco Plug and Play application	The Cisco Network Plug and Play solution is a converged solution that extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. This feature saves costs by application experience over any connection and using otherwise inactive or backup links.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI server for Trust manager service. It automates the lifecycle management of issuing, renewing, and revoking the PKI X.509 certificate for applications such as IWAN application. With this feature, the IWAN application greatly simplifies the process of establishing and keeping trust in the network.
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.

Primary Components

The following are the primary components required for a Cisco APIC-EM deployment:

- The Cisco APIC-EM software provided as an ISO image downloaded from the Cisco website (for installation on either a physical server or virtual machine), or pre-installed on a dedicated physical appliance
- Supported Cisco routing and switching platforms

The Cisco APIC-EM ISO image consists of the following components:

- Ubuntu 14.04 LTS 64-bit
- Cisco APIC-EM services
- Grapevine Elastic Services Platform, consisting of a Grapevine root and client template

Note The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its core functionality. See Chapter 3, *Cisco APIC-EM Services* for additional information about the services.

The Cisco APIC-EM makes use of the Ubuntu operating system environment and Linux containers (LXC). The Grapevine root runs within the host's operating system. The Grapevine clients run in LXCs within the host.

For this release, you can deploy and run the Cisco APIC-EM on the following:

- Server (bare-metal hardware)—This is the recommended platform. The Cisco APIC-EM ISO is installed directly on a server (bare-metal hardware) rather than within a host operating system (OS).
- Virtual machine—Cisco APIC-EM ISO is installed within a virtual machine within a VMware vSphere environment.

IP Connectivity

The Cisco APIC-EM communicates with its supported platforms using the following protocols:

- SNMPv2c or SNMPv3
- Telnet or SSH

Note Currently, the Cisco APIC-EM supports IPv4 only. IPv6 support is planned for a future release.

System Requirements

System Requirements—Server (Bare-Metal hardware)

The following table lists the minimum system requirements for a successful Cisco APIC-EM server (bare-metal hardware) installation. Review the minimum system requirements for a server installation. The minimum system requirements for each server in a multi-host deployment are the same as in a single host deployment, except that the multi-host deployment requires two or three servers and less memory for each individual server. Three servers are required for high availability and redundancy.

Caution You must dedicate the entire server for the Cisco APIC-EM. You cannot use the server for any other software programs, packages, or data. During the Cisco APIC-EM installation, any other software programs, packages or data on the server will be deleted.

Table 2: Minimum System Requirements—Server

Server Option	Image Format	Bare metal/ISO
Hardware Specifications	CPU (cores)	6
	Memory	64GB **Note** For a multi-host hardware deployment (2 or 3 hosts) only 32GB of RAM is required for each host.
	Disk Capacity	500GB of available/usable storage after hardware RAID
	RAID Level	Hardware-based RAID at RAID Level 10
	CPU Speed	2.4 GHz
	Disk I/O Speed	200 MBps

	Network Adapter	1 **Note** A single network adapter or network interface controller (NIC) is the minimum requirement. For security, we recommend that you use and configure two NICs on the server. See *Security* in the *Limitations and Restrictions* section of the release notes for additional information.
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 46 or later

System Requirements—Virtual Machine

The following table lists the minimum system requirements for a successful Cisco APIC-EM VMware vSphere installation.

Note You must configure at a minimum 64GB RAM for the virtual machine that contains the Cisco APIC-EM when a single host is being deployed. The single host server that contains the virtual machine must have this much RAM physically available. For a multi-host deployment (2 or 3 hosts), only 32GB of RAM is required for each of the virtual machines that contains the Cisco APIC-EM. Three servers are required for high availability and redundancy.

Table 3: Minimum System Requirements—Virtual Machine

Virtual Machine	VMware ESXi Version	5.1/5.5
	Image Format	ISO
Hardware Specifications	Virtual CPU (vCPU)	6

	Memory	64GB **Note** For a multi-host deployment (2 or 3 hosts) only 32GB of RAM is required for each host.
	Disk Capacity	500GB
	CPU Speed	2.4 GHz
	Disk I/O Speed	200 MBps
	Network Adapter	1 **Note** A single network adapter or network interface controller (NIC) is the minimum requirement. For security, we recommend that you use and configure two NICs on the server. See *Security* in the *Limitations and Restrictions* section of the release notes for additional information.
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 46 or later

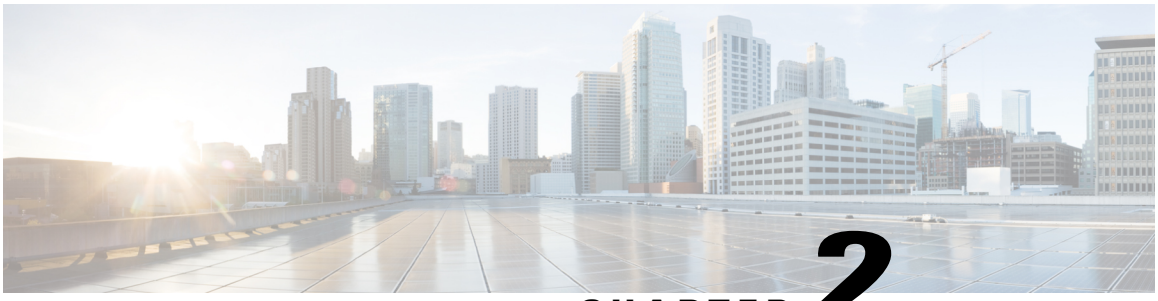
Supported Cisco Platforms and Software Releases

For information about the supported Cisco platforms and software releases:

- See the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module* for the list of supported platforms and software releases for the base controller applications (Discovery, Inventory, Topology, and Path Trace).
- See the *Release Notes for Cisco IWAN on APIC-EM* for the list of supported platforms and software releases for the IWAN application.
- See the *Release Notes for Cisco Network Plug and Play* for the list of supported platforms and software releases for the Cisco Network Plug and Play application.

Supported Northbound REST APIs

The Cisco APIC-EM provides northbound REST APIs that you can use to that you can use to issue requests to the controller and exchange data with the controller in a platform-agnostic way. For detailed information about supported northbound REST APIs, see the internal, interactive documentation located within the GUI itself. Click the **API** button at the top right of the GUI to view this documentation.



CHAPTER 2

Cisco APIC-EM Security

Information about Cisco APIC-EM Security

The Cisco APIC-EM requires a multi-layered architecture to support its basic functionality. This multi-layered architecture consists of the following components:

- External network or networks—The external network exists between administrators and applications on one side of the network, and the Grapevine root and clients within an internal network or cloud on the other side. Both administrators and applications access the Grapevine root and clients using this external network.
- Internal network—The internal network consists of both the Grapevine root and clients.
- Device management network—This network consists of the devices that are managed and monitored by the controller.

Any inter-communications between the layers and intra-communications within the layers are protected through encryption and authentication.

Note For information about the different services running on the clients within the internal network, see Chapter 3, *Cisco APIC-EM Services*.

External Network Security

Northbound REST API requests from the external network to the Grapevine clients located within the internal network are made secure using TLS (either version 1.0, 1.1, or 1.2). The entry point to the internal network is the Grapevine client running the reverse-proxy service. The controller provides an external facing X.509 certificate on this Grapevine client. This certificate is presented by the Grapevine client running the reverse-proxy service to any incoming API request.

The external X.509 certificate that is presented by the controller is one that has been either dynamically generated and self-signed by the controller itself, or one that has been imported (user's X.509 certificate) with a private key into the controller. You have the option to either use the a self-signed X.509 certificate from the controller or to import and use your own X.509 certificate and private key. By default, the self-signed X.509 certificate presented to an API request is signed by Grapevine's internal Certificate Authority (CA). This self-signed X.509 certificate may not be recognized and accepted by your host. To proceed with your API request, you must ignore any warning and trust the certificate to proceed.

Note We recommend against using and importing a self-signed certificate into the controller. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended. Additionally, you must replace the self-signed certificate (installed in the Cisco APIC-EM by default) with a certificate that is signed by a well-known certificate authority for the Network PnP functionality to work properly.

Internal Network Security

Several key intra-Grapevine communications using HTTP are sent over SSL using the internal public key infrastructure (PKI). All the internal Grapevine services, database servers, and the Cisco APIC-EM services themselves listen only on the internal network in order to keep these services segmented and secured.

Device Management Network Security

The Cisco APIC-EM REST API /network-device/management-info allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory, including the administrative credentials (SNMP community strings, CLI username and password, CLI enable password) in cleartext. The purpose of this API is to allow an external application to synchronize it's own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution. Any user account with a ROLE_ADMIN has access to this API.

Information about PKI

The Cisco APIC-EM relies on Public Key Infrastructure (PKI) to provide secure communications. PKI consists of certificate authorities, digital certificates, and public and private keys.

Certificate authorities (CAs) manage certificate requests and issue digital certificates to participating entities such as hosts, network devices, or users. The CAs provide centralized key management for the participating entities.

Digital signatures, based on public key cryptography, digitally authenticate the hosts, devices and/or individual users. In public key cryptography, such as the RSA encryption system, each entity has a key pair that contains both a private key and a public key. The private key is kept secret and is known only to the owning host, device or user. However, the public key is known to everyone. Anything encrypted with one of the keys can be decrypted with the other. A signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by decrypting the message with the sender's public key. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates link the digital signature to the sender. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The CA that signs the certificate is a third party that the receiver explicitly trusts to validate identities and to create digital certificates.

To validate the signature of the CA, the receiver must first know the CA's public key. Typically this process is handled out of band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default.

Cisco APIC-EM Certificate and Private Key Support

The Cisco APIC-EM supports a PKI certificate management feature that is used to authenticate sessions (HTTPS). These sessions use commonly recognized trusted agents called certificate authorities (CAs). The Cisco APIC-EM uses the PKI certificate management feature to import, store, and manage an X.509 certificate from well-known CAs. The imported certificate becomes an identity certificate for the controller itself, and the controller presents this certificate to its clients for authentication. The clients are the NB API applications and network devices.

The Cisco APIC-EM can import the following files (in either PEM or PKCS file format) using the controller's GUI:

- X.509 certificate
- Private key

Note For the private key, Cisco APIC-EM supports the importation of RSA keys. DSA, DH, ECDH, and ECDSA key types should not be imported and are not supported. You should also keep the private key secure in your own key management system.

Prior to import, you must obtain a valid X.509 certificate and private key from a well-known, certificate authority (CA) or create your own self-signed certificate. After import, the security functionality based upon the X.509 certificate and private key is automatically activated. The Cisco APIC-EM presents the certificate to any device or application that requests them. Both the Northbound API applications and network devices can use these credentials to establish a trust relationship with the controller.

In an IWAN configuration and for the Network PnP functionality, an additional procedure involving a PKI trustpool is used to ensure trust between devices within the network. See the following *Cisco APIC-EM Trustpool Support* section for information about this procedure.

Note We recommend against using and importing a self-signed certificate into the controller. Importing a valid X.509 certificate from a well-known, certificate authority (CA) is recommended. Additionally, you must replace the self-signed certificate (installed in the Cisco APIC-EM by default) with a certificate that is signed by a well-known certificate authority for the Network PnP functionality to work properly.

The Cisco APIC-EM supports only one imported X.509 certificate and private key at a time. When you import a second certificate and private key, it overwrites the first (existing) imported certificate and private key values.

Note If the external IP address changes for your controller for any reason, then you need to re-import a new certificate with the changed or new IP address.

Related Topics

Importing a Certificate, on page 55

Cisco APIC-EM Certificate Chain Support

The Cisco APIC-EM is able to import certificates and private keys into the controller through its GUI. The Cisco APIC-EM also supports the importation of subordinate certificates (intermediate certificates) from a subordinate Certificate Authority (CA) through its GUI.

If there are subordinate certificates involved in the certificate chain leading to the certificate that is imported into the controller (controller certificate), then both the subordinate certificates as well as the root certificate of these subordinate CAs must be appended together into a single file to be imported. When appending these certificates, you must append them in the same order as the actual chain of certification.

For example, assume that a well-known and trusted CA with a root certificate (CA root) signed an intermediate CA certificate (CA1). Next, assume that this certificate, CA1 signs another intermediate CA certificate (CA2). Finally, assume that the CA certificate (CA2) was the CA that signed the controller certificate (Controller_Certificate). In this example, the PEM file that needs to be created and imported into the controller should have the following order from the top (beginning) of the file to the bottom of the file (end):

1. Controller_Certificate (top of file)
2. CA2 certificate
3. CA1 certificate

The requirement to append the root and subordinate certificates to the controller certificate to create a single file only applies to a PEM file. The requirement for appending a root and intermediate certificates to a root certificate for import is not required for a PKCS file.

Related Topics

Importing a Certificate, on page 55

Cisco APIC-EM Trustpool Support

The Cisco APIC-EM and Cisco IOS devices support a special PKI certificate store known as the trustpool. The trustpool holds X.509 certificates that identify trusted certificate authorities (CAs). The Cisco APIC-EM and the devices in the network use the trustpool bundle to manage trust relationships with each other and with these CAs. The controller manages this PKI certificate store and has the ability to update it through its GUI when certificates in the pool are due to expire, are reissued, or must be changed for other reasons.

Note The Cisco APIC-EM also uses the trustpool functionality to determine whether any certificate file that is uploaded via its GUI is a valid CA signed certificate or not.

The Cisco APIC-EM contains a pre-installed, default, Cisco-signed trustpool bundle named ios.p7b. This trustpool bundle is trusted by supported Cisco network devices natively, since it is signed with a Cisco digital signing certificate. This trustpool bundle is critical for the Cisco network devices to establish trust with services and applications that are genuine. This Cisco PKI trustpool bundle file is available on the Cisco website (Cisco InfoSec). The link is located at: http://www.cisco.com/security/pki/.

For the controller's Network PnP functionality, the supported Cisco devices that are being managed and monitored by the controller need to import this file. When the supported Cisco devices first boot-up, they contact the controller to import this file.

Note At times, you may need to update this trustpool bundle to a newer version due to certificates in the trustpool expiring, being reissued, or for other reasons. Whenever the trustpool bundle that exists on the controller needs to be updated, you can update it by using the controller's GUI. The controller can access the Cisco cloud (where the Cisco approved trustpool bundles are located) and download the latest trustpool bundle. After download, the controller then overwrites the current, older trustpool bundle file. As a practice, you may want to update the trustpool bundle before a new certificate from a CA is to be imported using the **Certificate** window or the **Proxy Gateway Certificate** window, or whenever the **Update** button is active and not grayed out.

The Cisco APIC-EM trustpool management feature operates in the following way:

1. You boot-up the Cisco devices within your network that supports the Network PnP functionality.

Note Not all Cisco devices support the Network PnP functionality. See the *Release Notes for Cisco Network Plug and Play* for a list of the supported Cisco devices.

2. As part of initial PnP flow, these supported Cisco devices download a trustpool bundle directly from the Cisco APIC-EM using HTTP.
3. The Cisco devices are now ready to interact with the Cisco APIC-EM to obtain further device configuration and provisioning per the Network PnP traffic flows.

Related Topics

Importing a Trustpool Bundle, on page 60

Password Requirements

The Cisco APIC-EM password policy governs password values in logins to the controller GUI, SSH logins to the Grapevine root, northbound API requests, and logins to the Grapevine console for troubleshooting. The Cisco APIC-EM rejects a password that does not conform to the password policy. If a password is rejected, the controller provides an error message that describes the reason for the rejection.

A new or changed password must meet the following criteria:

- Eight character minimum length.
- Does NOT contain a tab or a line break.
- Does contain characters from at least three of the following categories:
  - Uppercase alphabet
  - Lowercase alphabet
  - Numeral
  - Special characters

    Special characters include the space character or any of the following characters or character combinations:

    ```
    ! @ # $ % ^ & * ( ) - =  + _ { } [ ] \\ | ; : " ' , < . > ? /
    :: #! ./ ;; >> << () **
    ```

For example, `Splunge!` is a valid password because it meets the eight-character minimum length, contains at least one uppercase alphabetic character, contains at least one lowercase alphabetic character, and contains at least one special character (`!`).

Related Topics

Configuring Password Policies, on page 72

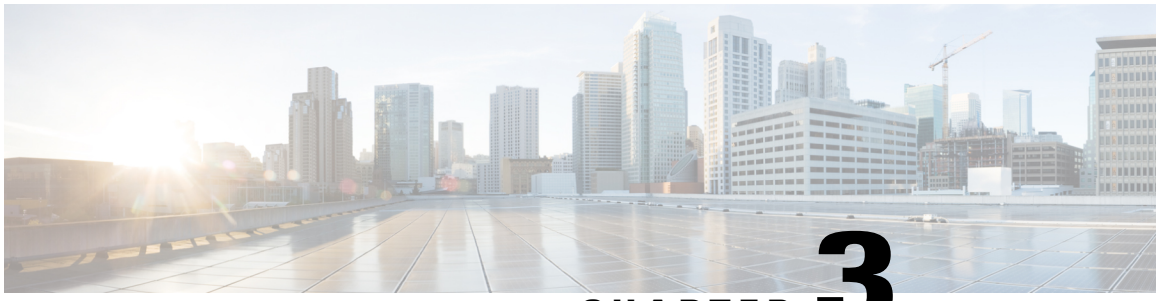
Cisco APIC-EM Ports Reference

The following table lists the ports that permit incoming traffic into the controller:

Table 4: Cisco APIC-EM Ports Reference

Protocol (TCP or UDP)	Port Number	Permitted Traffic
TCP	22	SSH
TCP	80	HTTP
TCP	443	HTTPS
TCP	14141	Grapevine console
UDP	67	bootps

Protocol (TCP or UDP)	Port Number	Permitted Traffic
UDP	123	NTP
UDP	162	SNMP
TCP	16026	SCEP



CHAPTER 3

Cisco APIC-EM Services

About Cisco APIC-EM Services

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network, using Grapevine as an Elastic Services platform to support the controller's infrastructure and services. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

The Cisco APIC-EM controls elasticity at the service level, rather than at the Grapevine client level.

Related Topics

Creating a Service Instance Manually
Removing a Service Instance Manually
Reviewing the Service Version, Status, and Logs, on page 101
Services, on page 18

Service Managers and Monitors

The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its functionality. The Grapevine Elastic Services Platform consists the following components:

- Grapevine root—Handles all policy management in regards to service updates, as well as the service lifecycle for both itself and the Grapevine client.
- Grapevine client—Location where the supported services run.

After installation, service functionality is enabled using the following managers and monitors:

- Grapevine root
  - Service manager—Starts, stops, and monitors service instances across the Grapevine clients.
  - Capacity manager—Provides on-demand capacity to run the services.
  - Load monitor—Monitors the load and health of services across the Grapevine clients.
  - Service catalog—Repository of service bundles that can be deployed on the Grapevine clients.
- Grapevine Client
  - Service manager—Starts, stops, and monitors service instances on the Grapevine client.
  - Service instance manager—Deploys the service.

Service Features

The Cisco APIC-EM provides the following service features:

- Adding capacity on an existing client—When a service load exceeds a specified threshold on a client, the controller can request another service instance to start on a second, preexisting client.
- Adding capacity on a newly instantiated client—When a service load exceeds a specified threshold on a client, the controller can request a new client to be instantiated and then start another service instance on this client.
- Prioritizing services—When a service load on the client starts to exceed a specified threshold, the controller stops the lower priority services running on the client. This action creates capacity for a higher priority service to run on the same client.
- Allows automatic scaling of services—As the service load increases, the controller instantiates additional service instances in response. As the service load decreases, the controller tears down the number of instances in response.
- Resiliency for services—When a service fails, the controller starts a replacement instance. The controller then ensures that the service's minimum instance count requirements are maintained.

Services

The following are the supported Cisco APIC-EM services for this release.

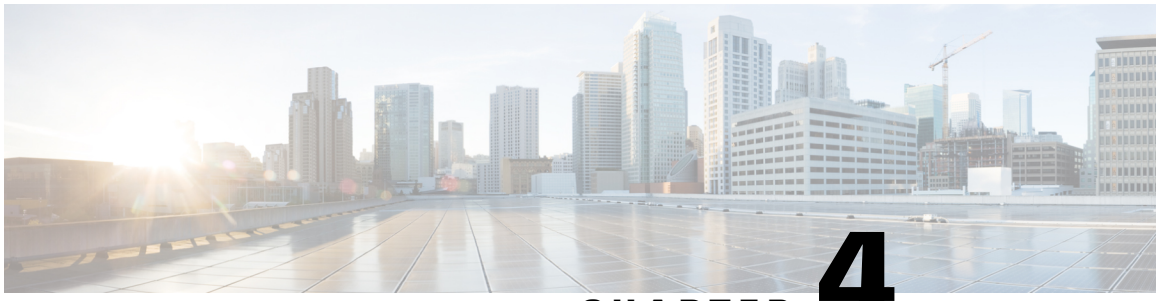
Note For information about troubleshooting services, see Chapter 6, Troubleshooting the Cisco APIC-EM.

- apic-em-inventory-manager-service
- apic-em-jboss-ejbca
- apic-em-network-discovery-service
- apic-em-network-programmer-service

- apic-em-pki-broker-service
- app-vis-policy-programmer-service
- cas-service
- data-access-service
- data-uploader
- file-service
- ipgeo-service
- ip-pool-manager-service
- log-aggregator
- nbar-policy-programmer-service
- pfr-policy-programmer-service
- pnp-service
- policy-analysis-service
- policy-manager-service
- postgres
- rbac-service
- remote-ras
- reverse-proxy
- router
- scheduler-service
- task-service
- telemetry-service
- topology-service
- ui
- visibility-service

Related Topics

Creating a Service Instance Manually
Removing a Service Instance Manually
Reviewing the Service Version, Status, and Logs, on page 101
About Cisco APIC-EM Services, on page 17



CHAPTER 4

Deploying the Cisco APIC-EM

Information about the Cisco APIC-EM Deployment

You can deploy the Cisco APIC-EM on either a server (bare-metal hardware) or within a virtual machine in a VMware vSphere environment. You can also deploy the Cisco APIC-EM as either a single host or in a multi-host environment.

Note We recommend that you deploy the Cisco APIC-EM in a multi-host environment for enhanced scalability and redundancy.

Related Topics

Configuring Cisco APIC-EM as a Single Host Using the Wizard, on page 26

Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 33

Pre-Deployment Checklists

Single Host Checklists

Review the following checklists before beginning your single-host Cisco APIC-EM deployment.

Note A host is defined as physical server or virtual machine with instances of a Grapevine root and clients running. The Grapevine root is located in the host OS and the clients are located within Linux containers. The clients run the services within the Linux containers. You can set up either a single host deployment or multi-host deployment (2 or 3 hosts) for your network. For high availability and scale, your multi-host deployment must contain three hosts. All inbound traffic to the controller in a single host deployment is through the host IP address that you configure using the configuration wizard. All inbound traffic to the controller in a multi-host deployment is through a Virtual IP that you configure using the configuration wizard.

Networking Requirements

This Cisco APIC-EM deployment requires that the network adapters (NICs) on the host (physical or virtual) are connected to the following networks:

- Internet (network access required for **Make A Wish** requests and telemetry collection)
- Network with NTP server(s)
- Network with devices that are to be managed by the Cisco APIC-EM

Note The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment.

IP Address Requirements

Ensure that you have available at least one IP address for the network adapter (NIC) on the host.

The IP address is used as follows:

- Direct access to the Grapevine root
- Direct access to the Cisco APIC-EM controller (for GUI access)

Note If your host has 2 NICs, then you might want to have two IP addresses available and configure one IP address for each NIC.

Multi-Host Checklists

Review the following checklist before beginning your multi-host Cisco APIC-EM deployment.

- You must satisfy the requirements for the single host deployment as described in the previous section for each host.

Note For a multi-host configuration, 32GB of RAM is required for each host in contrast to 64GB of RAM requirement for a single host configuration.

- Additionally, you must establish a network connection between each of the hosts using either a switch or a router. Each host must be routable with the other two hosts.
- You must configure a virtual IP (VIP).

  You configure one or more NICs on each host using the configuration wizard. Each NIC that you configure must point to a non-routable network (if all your networks are routable, then you only need one NIC). A VIP is required per non-routable network. For example, if you configure 2 NICs on all 3 hosts in a multi-host cluster and each NIC points to a separate, non-routable network, then you need to configure 2 VIPs. The VIP provides an interface redundancy feature for your multi-host deployment. With a VIP, the IP address can float between the hosts.

  When deploying the controller in a multi-host configuration:

  - You provide a VIP address when configuring the controller using the wizard.
  - On startup, the controller will bring up the VIP on one of the hosts.
  - All inbound requests into controller from the external network are made via this VIP (instead of the host IP address), and the requests are routed to the services running on different hosts via the reverse-proxy service.
  - If the host on which has the VIP fails, then Grapevine will bring up the VIP on one of the remaining two hosts.
  - The VIP must reside in the same subnet as the three hosts.

Multi-Host Deployment Virtual IP

A multi-host deployment has three physical IP addresses and one virtual IP that floats across the IP addresses by design in order to provide high availability. This capability to float also means that any SSH client that wants to connect to the virtual IP address will see different host-identity public SSH keys each time the virtual IP moves its residence from one host to another host. Most SSH clients will complain that the new host is not trusted, since an entry already exists (as you might have accepted the key earlier for the older host which owned that virtual IP address before). To prevent this inconvenience, you may want to add the host keys of all the three hosts to your known hosts list as described below.

For example on a Linux or Apple Mac OS client machine, run the **ssh-keyscan** command on each of the three host physical IP addresses as follows:

```
$ ssh-keyscan -t rsa 209.165.200.30
# 209.165.200.30 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.30 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRd
SYnuCHfDiY5Pptt3BmaPgC6OlER4wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWq
XSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9oimdv.....


$ ssh-keyscan -t rsa 209.165.200.31
# 209.165.200.31 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
```

```
209.165.200.31 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDF57F90z2His86tEj4s75pTc7h0nfzF
2c3QweHCNN2ov474HJJcPrnWTw4DAoPpPCU6zWvR0QLxunURDb+pMeZrIIyd49xn9+OBSmBpzrnety7UB2uP
XzL1RvVxayw8mkXkj779LhFh9vkXR4DtX7XLjg.....
```

```
$ ssh-keyscan -t rsa 209.165.200.32
# 209.165.200.32 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.32 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9kwzodGzGkh/UFXVa9fptGe+sa3CBR
6SNerXxpCmfT9AOXH8xuk3/CBX+DDUQgGJVmqw6maCYKOy0RtAhGxdsNdPL6ETTKzxYB5uzw3KhcDJ6D6ob6
jdzkR6yRuXVFi2OE+u1Aqs7J8GO66FfdavU8.....
```

Next, change the IP address in the SSH key line of each output to the virtual IP address of the following and append all three key lines to the `~/.ssh/known_hosts` file and save it.

Assuming that 209.165.200.33 is the virtual IP address in the above multi-host example, you would add three lines in the `~/.ssh/known_hosts` file of your client machine as follows:

```
209.165.200.33 ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRdSYnuCHfDiY5Pptt3BmaPgC6OlER4
wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVz1wtHHZdhO6G93MyLLGsWqXSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9
oimdvPbrQPua7Zg9oblDxaBPn0Fqj00YDjKqTkp/IkZHEfHbDM996GLEbWlOvoHeCCqeZ1nWgFIqzAF+ty8+X5Z/fh
hmGe+w2tQlMfrs9pcZDaEEmq/w1W+uRohxLKs+OHnHYAbMzC6O+5fLEr2BwaZf8W016eo1WpPsxUVK6StbXBOQZrcH0
bPsUbIjKJkzafpft9Dp73pSd/vwaoB3DrvNec/PiEJYk+R.....
```

After the above change, the client will have no trouble performing uninterrupted SSH into the virtual IP address of the hosts even with the IP address floating.

Verifying the Cisco ISO Image

Prior to deploying the Cisco APIC-EM, you can verify that the ISO image that you downloaded is a genuine Cisco image.

Note If you are deploying the Cisco APIC-EM from an ISO image that you downloaded, then perform this procedure. This procedure is not required, if deploying the controller with the Cisco APIC-EM Controller Appliance (Cisco APIC-EM ISO image pre-installed and tested).

Before You Begin

You must have received notification of the location of the Cisco APIC-EM ISO image or contacted Cisco support for the location of the Cisco APIC-EM ISO image.

Step 1 Download the ISO image from the location specified by Cisco.

Step 2 Download the Cisco public key for signature verification from the location specified by Cisco.
The Cisco public key is named:

`cisco_image_verification_key.pub`

Step 3 Download the secure hash algorithm (SHA512) checksum file for the ISO image from the location specified by Cisco.

Step 4 Obtain the specific release ISO image's signature file from Cisco support via email or by download from the secure Cisco website (if available).
For example, `apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.sig`.

Step 5 (Optional) Perform a SHA verification to determine whether the ISO image was corrupted due to a partial download. For example, run one of the following commands (depending upon your operating system):

- On a system running MAC OS X version:

```
shasum -a 512 apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

- On a Linux system:

```
sha512sum apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

Microsoft Windows does not include a built-in checksum utility, but you can install a utility from Microsoft at this link: http://www.microsoft.com/en-us/download/details.aspx?id=11533

Compare the output of the above command (or Microsoft Windows utility) to the SHA512 checksum file downloaded earlier in step 3. If the command output fails to match, download the ISO image again and run the appropriate command a second time. If the output still fails to match, contact Cisco support.

Step 6 Verify that the ISO image is genuine and from Cisco by verifying the signature. Run the following command on the ISO image:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.sig apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

If the ISO image is genuine, then running this command should result in a **Verified OK** message. If this message fails to appear, then do not install the ISO image and contact Cisco support.

Note The image name and the signature names used here are only examples. Use the exact names of these files that you downloaded from the Cisco website.

This command will work in both MAC and Linux environments. For Windows, you need to download and implement OpenSSL from www.openssl.org, if you have not already done so.

What to Do Next

After you verify that the ISO image is genuine and from Cisco, install the Cisco ISO image.

Installing the Cisco ISO Image

Perform the steps in the following procedure to install the Cisco ISO image on the host (server or virtual machine).

Note If you are deploying the Cisco APIC-EM from an ISO image that you downloaded, then perform this procedure. This procedure is not required, if deploying the controller with the Cisco APIC-EM Controller Appliance (Cisco APIC-EM ISO image pre-installed and tested).

Before You Begin

You must review the system requirements before beginning this procedure.

You must review the Cisco APIC-EM pre-deployment checklist before beginning this procedure.

You must have downloaded and verified the Cisco ISO image by performing the tasks in the previous procedure.

For installing the Cisco APIC-EM ISO image into a virtual machine using VMware, you must create an empty virtual machine that you will attach the Cisco APIC-EM ISO image to and then boot up. When creating this virtual machine, do not accept the VMware default settings but configure the settings as per the system requirements previously listed in this guide.

Note See the VMware documentation for information about creating and configuring new virtual machines.

Perform one of the following procedures:

- For installing the Cisco APIC-EM ISO image on a server and from local media:
  - Burn the ISO image onto a DVD or a bootable USB flash drive.
  - Insert the DVD into the DVD drive of the physical appliance.

    If your physical appliance does not come with a DVD drive, you can connect an external USB DVD drive to the appliance and insert the disk into that external drive.
  - You can also connect a bootable USB flash drive where you burnt the ISO image to into the appliance.

    Note Cisco UCS servers provide an additional method of installing a remote ISO using a Virtual KVM console. See your Cisco UCS server documentation for information about this procedure. Note that installing the ISO image using a Virtual KVM console may take longer than the above methods.
- For installing the Cisco APIC-EM ISO image on a virtual machine:
  - Upload the Cisco APIC-EM ISO image directly to the virtual machine's datastore.
  - Attach the Cisco APIC-EM ISO image as a virtual CD-ROM drive of the virtual machine.

What to Do Next

Boot up the host (server or virtual machine) and run the wizard to configure the Cisco APIC-EM.

Configuring Cisco APIC-EM as a Single Host Using the Wizard

Perform the steps in the following procedure to configure Cisco APIC-EM as a single host using the wizard.

Before You Begin

You must have either received the Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a server or virtual machine as described in the previous procedures.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option to begin.
You are then prompted to enter values for the **NETWORK ADAPTER #1 (eth0)**.

Step 4 Enter configuration values for the **NETWORK ADAPTER #1 (eth0)** on the appliance.
The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your appliance. For example, if your appliance has two network adapters you are prompted to confirm configuration values for network adapter #1 (eth0) and network adapter #2 (eth1).

Note On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter the host IP address to use for the network adapter. This IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.
Netmask	Enter the netmask for the network adapter's IP address.
Default Gateway IP address	Enter a default gateway IP address to use for the network adapter. **Note** If no other routes match the traffic, traffic will be routed through this IP address.
DNS Servers	Enter the DNS server or servers IP addresses (separated by spaces) for the network adapter.

Static Routes	If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway> Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes.

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation and if your appliance has two network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)**.

Step 5 Enter configuration values for the **NETWORK ADAPTER #2 (eth1)** on the appliance.
If you do not have two network adapters or if you do not have more than one non-routable network, then proceed to the next step.

Host IP address	Enter the host IP address to use for the network adapter. This IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.
Netmask	Enter the netmask for the network adapter's IP address.
Default Gateway IP address	Enter a default gateway IP address to use for the network adapter. **Note** If no other routes match the traffic, traffic will be routed through this IP address.
DNS Servers	Enter the DNS server or servers IP addresses (separated by spaces) for the network adapter.

Static Routes	If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway> Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes.

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation, you are then prompted to enter values for the **LINUX USER SETTINGS**.

Step 6 Enter configuration values for the **LINUX USER SETTINGS**.

Linux Password	Enter a Linux password. The Linux password is used to ensure security for both the Grapevine root and clients located on the host (appliance, server, or virtual machine). Access to the Grapevine root and clients by you or the controller requires this password. The default username is grapevine. For information about the requirements for a Linux password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security. **Note** The Linux password is encrypted and hashed in the controller database.
Re-enter Linux Password	Confirm the Linux password by entering it a second time.
Seed Phrase Password Generation	(Optional) Instead of creating and entering your own password in the above **Linux Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase. Enter a seed phrase and then press <**Generate Password**> to generate the password.

Auto Generated Password	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password. **Note** When finished with the password, be sure to save it to a secure location for future reference. Press <**Use Generated Password**> to save the password.

After configuring the Linux password, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for the **APIC-EM ADMIN USER SETTINGS**.

Step 7 Enter configuration values for the **APIC-EM ADMIN USER SETTINGS**.

Administrator Username	Enter an administrator username. Your administrator username and password are used to ensure security for the controller itself. Access to the controller's GUI requires that you enter this username and password.
Administrator Password	Enter an administrator password. For information about the requirements for an administrator password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security. **Note** The administrator password is encrypted and hashed in the controller database.
Re-enter Administrator Password	Confirm the administrator password by entering it a second time.
Seed Phrase Password Generation	(Optional) Instead of creating and entering your own password in the above **Administrator Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase. Enter a seed phrase and then press <**Generate Password**> to generate the password.
Auto Generated Password	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password. **Note** When finished with the password, be sure to save it to a secure location for future reference. Press <**Use Generated Password**> to save the password.

After configuring the administrator password, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for the **NTP SERVER SETTINGS**.

Step 8 Enter configuration values for **NTP SERVER SETTINGS**.

NTP servers	Enter a single NTP server address or a list of NTP servers each separated by a space. The Elastic Services Platform (Grapevine) manages a Network Time Protocol (NTP) server to provide time synchronization for the Grapevine clients. You must configure the NTP server for the clients. The NTP server is external to the cluster.

Note Cisco routers can also be configured as NTP servers.

After configuring the NTP server(s), enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for the **CLOUD CONNECTIVITY**.

Step 9 Enter configuration values for **CLOUD CONNECTIVITY**.

CCO Username	Enter a Cisco Connection Online (CCO) username for cloud connectivity. For example, enter the username that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner.
CCO Password	Enter a Cisco Connection Online (CCO) password for the CCO *username*. For example, enter the password that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner.
Company Name	Enter the company or organization's name with which you are affiliated.
HTTPS Proxy	If your network is configured behind a proxy server, enter the IP address and port number of the HTTPS proxy. You must configure an IP address and port number for your HTTPS proxy server to enable communications to the development team using the Cisco APIC-EM "I wish this page would…" GUI.

Once satisfied with the cloud connectivity settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values entered. After validation, you are then prompted to enter values for the **CONTROLLER CLEAN-UP**.

Step 10 Enter configuration values for **CONTROLLER CLEAN-UP**.

Harvest All Virtual Disks	Entering **yes** will delete all Grapevine virtual disks that belong to the controller for this specific deployment. For an initial configuration, enter **no**.

Delete All Clients	Entering **yes** will delete all Grapevine clients that belong to the controller for this specific deployment. For an initial configuration, enter **no**.

For an initial configuration, enter **no** for both options.

After configuring the controller clean-up, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values to finish the configuration and begin the configuration wizard installation.

Step 11 A final message appears stating that the wizard is now ready to proceed with applying the configuration. The following options are available:

- **[back]—**Review and verify your configuration settings.
- **[cancel]—**Discard your configuration settings and exit the configuration wizard.
- **[save & exit]—**Save your configuration settings and exit the configuration wizard.
- **[proceed]—**Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

Note

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Step 12 Open a Google Chrome browser and enter the host IP address to access the Cisco APIC-EM GUI. You can use the displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Step 13 After entering the IP address in the browser, a message stating that "Your connection is not private" appears. Ignore the message and click the **Advanced** link.

Step 14 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears. Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 15 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to Do Next

For a multi-host deployment, perform the following procedure to configure another host and join it with this host to create a cluster.

For a single-host deployment, begin to use the Cisco APIC-EM to manage and configure your network.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens a comments field. Use this field to make a comment on the current window or to make a request to the Cisco APIC-EM development team.

Related Topics

Information about the Cisco APIC-EM Deployment, on page 21

Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard

Perform the steps in this procedure to configure Cisco APIC-EM on your host and to join it to another, pre-existing host to create a cluster. Configuring the Cisco APIC-EM on multiple hosts to create a cluster is best practice for both high availability and scale.

Caution

- When joining a host to a cluster as described in the procedure below, there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined to.
- When joining the additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- You should also expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.

Before You Begin

You must have either received a Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a second server or virtual machine.

You must have already configured Cisco APIC-EM on the first host (server or virtual machine) in your planned multi-host cluster following the steps in the previous procedure. This procedure must be run on the second host that you are joining to the cluster. When joining the new host to the cluster, you must specify an existing host in the cluster to connect to.

Note The Cisco APIC-EM multi-host configuration supports the following two workflows:

- You first configure a single host running Cisco APIC-EM in your network. After performing this procedure, you then use the wizard to configure and join two additional hosts to form a cluster.
- If you already have several single hosts configured with Cisco APIC-EM, you can use the configuration wizard to join two additional hosts to a single host to form a cluster.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed with the deployment.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose one of the two displayed options to begin.

- **Create a new APIC-EM cluster**
- **Add this host to an existing APIC-EM cluster**

For the multi-host deployment, click the **Add this host to an existing APIC-EM cluster** option.

Step 4 Enter configuration values for the **NETWORK ADAPTER #1 (eth0)** on the host.
The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has two network adapters you are prompted to confirm configuration values for network adapter #1 (eth0) and network adapter #2 (eth1).

Note On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter a host IP address to use for the network adapter. This host IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.
Netmask	Enter the netmask for the network adapter's IP address.

Later in this procedure, the following information will be discovered and copied from the cluster to the configuration file of this host:

- Default Gateway IP address

- DNS Servers
- Static Routes

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation, you are then prompted to enter values for the **APIC-EM CLUSTER SETTINGS**.

Step 5 Enter configuration values for the **APIC-EM CLUSTER SETTINGS**.

Remote Host IP	Enter the eth0 IP address of the pre-configured host that you are now joining to form a cluster. **Note** If a virtual IP address has already been configured on another host for a multi-host cluster, you may also enter that IP address value. This field accepts either the IP address of a pre-configured host to the cluster or the virtual IP address of the cluster.
Administrator Username	Enter an administrator username. This is the administrator username on the pre-configured host that you are now joining to form a cluster.
Administrator Password	Enter an administrator password. This is the administrator password on the pre-configured host that you are now joining to form a cluster. For information about the requirements for an administrator password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security. **Note** The administrator password is encrypted and hashed in the controller database.

After configuring the administrator cluster settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard then proceeds to prepare the host to join the cluster.

You will receive a message to please wait, while the remote cluster is being queried and data is retrieved.

Step 6 (Optional) Enter configuration values for the **Virtual IP address**.

Note If you are joining the host to a cluster where the VIP has already been configured, then you will not be prompted for VIP configuration values. If you are joining the host to a cluster where the VIP has not yet been configured, then you will be prompted for VIP configuration values.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to.

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 7 (Optional) Enter additional configuration values for the **Virtual IP address**.

The configuration wizard proceeds to continue its discovery of any pre-existing configuration values on the hosts in the cluster. Depending upon what the configuration wizard discovers, you may be prompted to enter additional configuration values:

- If eth1 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth1. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth2 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth2. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth3 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for this eth3. You are also prompted for a VIP, if it has not yet been configured for this NIC.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to.
IP address	Enter an IP address to use for this network adapter. This IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 8 A final message appears stating that the wizard is now ready to proceed to join the host to the cluster.
The following options are available:

- **[back]—**Review and verify or modify your configuration settings.
- **[cancel]—**Discard your configuration settings and exit the configuration wizard.
- **[proceed]—**Save your configuration settings and begin the process to join this host to the specified Cisco APIC-EM.

Enter **proceed>>** to proceed. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

Note

At the end of the configuration process, a successful configuration message appears.

Step 9 Open a Google Chrome browser and enter an IP address to access the Cisco APIC-EM GUI.
You can use the first displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Note The first displayed IP address can be used to access the Cisco APIC-EM GUI. The second displayed IP address accesses the network where the devices reside.

Step 10 After entering the IP address in the browser, a message stating that "Your connection is not private" appears.
Ignore the message and click the **Advanced** link.

Step 11 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 12 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to Do Next

Proceed to follow the same procedure described here to join the third and final host to the multi-host cluster.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens a comments field. Use this field to make a comment on the current window or to make a request to the Cisco APIC-EM development team.

Related Topics

Information about the Cisco APIC-EM Deployment, on page 21

Removing Cisco APIC-EM from a Multi-Host Cluster Using the Wizard

Perform the steps in the following procedure to remove the Cisco APIC-EM from a multi-host configuration. You use the Cisco APIC-EM configuration wizard perform this procedure.

Note The configuration wizard option to remove a host only appears if the host on which you are running the configuration wizard is part of a cluster. If the host is not part of a cluster, then the option to remove a host does not display.

Before You Begin

You should have installed the Cisco APIC-EM as a member of a multi-host cluster following the procedure in this guide.

Note This procedure must be run on the host that is to be removed from the cluster.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 5 A message appears with the following options:

- **[cancel]—**Exit the configuration wizard.
- **[proceed]—**Begin the process to remove this host from its cluster.

Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from its cluster.
At the end of this process, you must then either run the configuration wizard again to configure the host as a new Cisco APIC-EM or join the Cisco APIC-EM to a cluster.

What to Do Next

If you wish to use this host again as either a stand-alone controller or operating within a cluster, then you must run the configuration wizard again and re-install the Cisco APIC-EM. Do not attempt to use this host again as either a standalone host or within a cluster without re-installing the Cisco APIC-EM.

Powering Down and Powering Up the Cisco APIC-EM

Under certain circumstances such as troubleshooting, you might want to power down and then power up the Cisco APIC-EM. This procedure describes how to gracefully power down and then power up the Cisco APIC-EM.

Before You Begin

You should have deployed the Cisco APIC-EM following the procedures in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **grape host display** command to review the command output and determine the *host_id* of the host that you want to power off.

Step 4 Enter the **grape host evacuate** command to harvest (gracefully shut down) the services on the host. Use the *host_id* for this command that you determined in the previous step.

```
$ grape host evacuate host_id
```

This command harvests all services running on the specified host (*host_id*) using the **grape host evacuate** command. In a multi-host cluster, the services on the specified host are harvested and transferred to the other two hosts in the cluster.

Step 5 Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

Note Enter your password a second time when prompted.

Step 6 Review the command output as the host shuts down.

Note The **sudo shutdown** command also powers off the host.

Step 7 Power up the Grapevine root process by turning the host back on.

Step 8 Using a Secure Shell (SSH) client, log back into the host with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 9 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 10 Enable Grapevine, by entering the following command on the Grapevine root:

```
$ grape host enable host_id
```

The host ID to enter for this command must be the same as the host ID used in the **grape host evacuate** command in step 3.

Wait a few minutes for the Cisco APIC-EM services to start up again.

What to Do Next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

Uninstalling the Cisco APIC-EM

The following procedure describes how to uninstall the Cisco APIC-EM.

Note If you plan to reinstall the Cisco APIC-EM after uninstalling it, then you must follow the procedure described below to avoid any possible problems. You should have also contacted Cisco support for the link to download the latest Cisco APIC-EM ISO image. Be aware that this procedure shuts down both the Cisco APIC-EM and the host (physical or virtual) on which it resides. At the end of this procedure and if you are reinstalling the Cisco APIC-EM, then you will need to access the host and restart it.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 Enter the Linux username ('grapevine') and password when prompted.

Step 3 Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

Step 4 Enter your Linux grapevine password a second time to start the reset process.

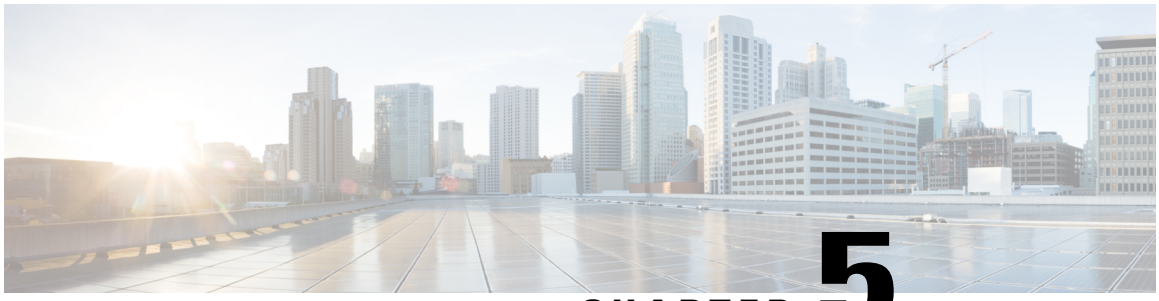
```
$ sudo password for grapevine *********
```

After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your intent to run the **reset_grapevine factory** command.

Step 5 Enter **Yes** to confirm that you want to run the **reset_grapevine factory** command.
The controller then performs the following tasks:

- Stops all running clients and services
- Stops and shuts down any Linux containers
- Deletes all cluster data
- Deletes all user data
- Deletes the configuration files including secrets and private keys
- Shuts down the controller
- Shuts down the host (physical or virtual)



CHAPTER 5

Configuring the Cisco APIC-EM Settings

Logging into the Cisco APIC-EM

You access the Cisco APIC-EM GUI by entering the IP address that you configured for the network adapter using the configuration wizard. This IP address connects to the external network. Enter the IP address in your Google Chrome browser in the following format:

https://*IP address*

Step 1 In your Google Chrome browser, enter the IP address of the Cisco APIC-EM.

Step 2 On the launch page, enter the administrator username and password.
The **Home** page of the APIC-EM controller appears.

What to Do Next

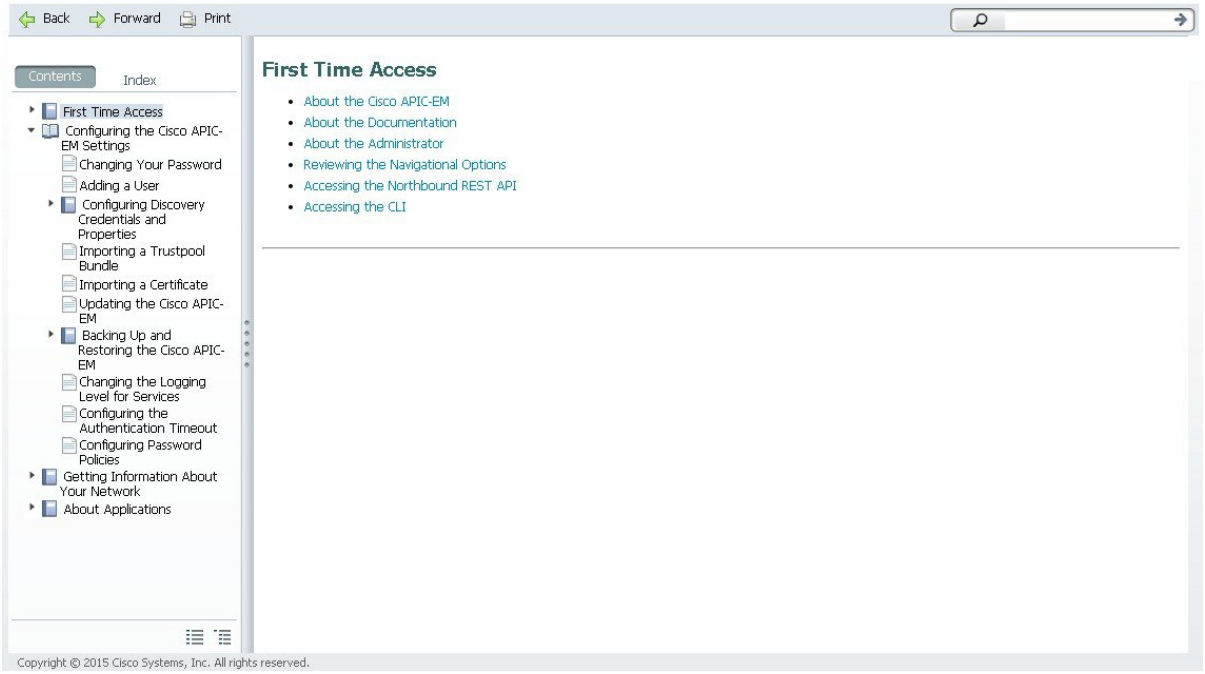
Proceed to take a quick tour of the Cisco APIC-EM Graphical User Interface (GUI).

Quick Tour of the APIC-EM Graphical User Interface (GUI)

For a quick introduction to the Cisco APIC-EM GUI, log into the Cisco APIC-EM controller as an administrator and follow the procedure below.

Step 1 Click the **Quick Start Guide** link that appears on the Cisco APIC-EM **Home** page.
The *Quick Start Guide* opens in a separate window.

Figure 1: Quick Start Guide



Step 2 Take a few moments to review the contents of the *Quick Start Guide*, which provides a short introduction to the main components of the Cisco APIC-EM graphical user interface and briefly describes how to configure some of the Cisco APIC-EM settings.

What to Do Next

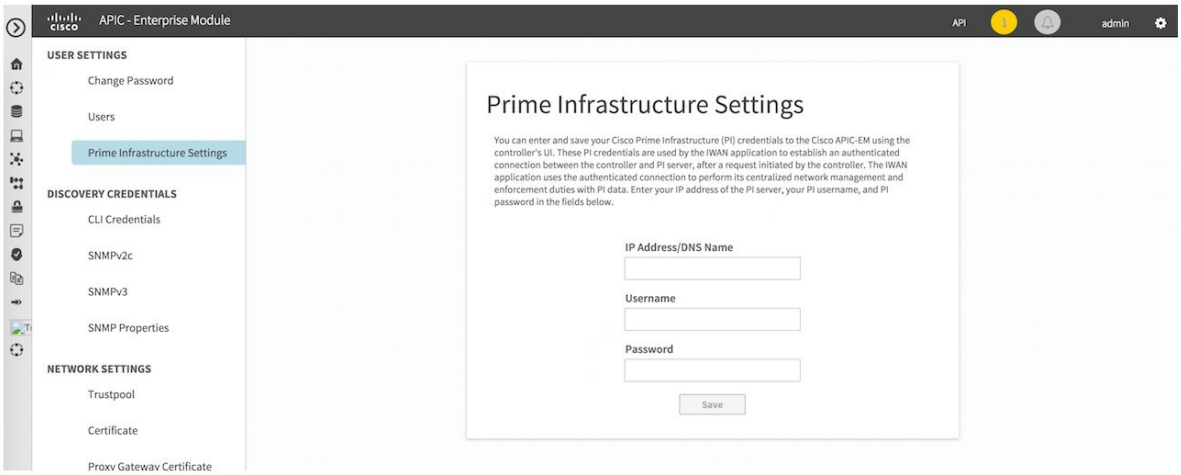
If you are using the IWAN application with Cisco Prime Infrastructure for your network, then proceed to configure your Prime credentials. If you are not using the IWAN application with Cisco Prime Infrastructure, then proceed to configure the discovery credentials for your network.

Configuring the Prime Infrastructure Settings

You can enter and save your Cisco Prime Infrastructure (PI) settings to the Cisco APIC-EM using the controller's UI. These PI settings are used by the IWAN application to establish an authenticated connection between the controller and PI server, after a request initiated by the controller. The IWAN application uses the authenticated connection to perform its centralized network management and enforcement duties with PI data.

You can configure the PI settings using the **Prime Infrastructrue Settings** window in the Cisco APIC-EM GUI.

Figure 2: Prime Infrastructure Settings Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to configure and save your Prime Infrastructure settings as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Prime Infrastructure Settings** to view the **Prime Infrastructure Settings** window.

Step 4 Enter either the IP address of the PI server or the DNS domain name of the PI server.

Step 5 Enter the PI Credentials username.

Step 6 Enter the PI Credentials password.

Step 7 Click the **Save** button to save the PI credentials to the Cisco APIC-EM database.

What to Do Next

Proceed to configure the discovery credentials for your network.

Discovery Credentials

The Cisco APIC-EM supports the following types of discovery credentials:

- CLI Credentials (Global and Exception)
- SNMPv2 (Read and Write Community)
- SNMPv3 (Mode, Authentication Type, Privacy Type)

For a successful device discovery note the following:

- CLI credentials (global and/or exception) and SNMP (v2c and/or v3) are configured using the controller's GUI. The CLI global credentials and SNMP credentials (v2c or v3) are configured in the **Discovery Credentials** windows as described in this chapter, and are used in addition to any CLI exception credentials that are configured in the **Discovery** window.

  Note For information about the procedure to configure CLI exception credentials in the Discovery window, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

- Both the CLI and SNMP credentials are required for a successful device discovery.

  You should enter at least one set of SNMP credentials, either SNMPv2c or SNMPv3 for device discovery. If you are going to configure SNMPv2 settings, then SNMP Read Only (RO) community string values should be entered to assure a successful discovery and populated inventory. However, if an SNMP RO community string is not provided, as a *best effort*, discovery will run with the default SNMP RO community string "public."

  Note The CLI credentials are used for capturing device configurations for the controller's inventory.

- You can enter values for both SNMP versions (SNMPv2c and SNMPv3) for a discovery.
- The controller supports multiple SNMP credential configurations, but if you configure more than 5 credential sets (global and/or exception, SNMPv2c and/or SNMPv3 credentials), you will receive an error message.

CLI Credentials—Global

CLI credentials (global) are defined as preexisting *device* credentials that are common to the devices in a network. Device credentials are credentials that were previously configured on the devices in your network, permit successful login to the devices, and are currently associated with the devices. CLI global credentials

are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this device credential when performing network discoveries.

You configure the CLI global credentials in the **CLI Credentials** window. You access this window, by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane.

Note Multiple credentials can be configured in the **CLI Credentials** window.

Related Topics

Configuring CLI Credentials—Global, on page 47

CLI Credentials—Exception

CLI credentials (exception) are defined as preexisting *device* credentials for a specific network device or set of devices that do not share the CLI global credentials. The CLI exception credentials provide the following features:

- These credentials can be provided when creating a new network discovery, but only a single set of the CLI exception credentials is allowed per network discovery.
- These credentials take precedence over any configured CLI global credentials.
- If the CLI exception credentials cause an authentication failure, then discovery is attempted a second time with the configured CLI global credentials. If discovery fails with the CLI global credentials then the device discovery status will result in an authentication failure.
- If the CLI exception credentials are not provided as part of network discovery, then the CLI global credentials are used to authenticate devices.

Note You configure the CLI exception credentials in the **Discovery** window. You access this window by clicking **Discovery** on the Navigation pane.

Discovery Credentials Example

The following discovery credentials example describes how a user would configure and run a series of discoveries to authenticate and access all of the devices in a network by the Cisco APIC-EM.

Assume a network of 20 devices that form a CDP neighborship. In this network, 15 devices share a CLI global credential (Credential-0) and the 5 remaining devices each have their own unique or CLI exception credentials (Credential 1- 5).

To properly authenticate and access the devices in this network by the Cisco APIC-EM, you perform the following tasks:

1 Configure the CLI global credentials as Credential-0 for the controller.

You configure the CLI global credentials in the **CLI Credentials** window. You access this window, by clicking either **admin** or the **Settings** icon (gear) on the menu bar at the upper right of the screen. You then click the **Settings** link from the drop-down menu and then click **CLI Credentials** on the Setting Navigation pane.

2. Configure SNMP (v2c or v3) credentials. You access these GUI windows by clicking the **Settings** button at the top right and then clicking **SNMPv2c** or **SNMPv3** on the Setting Navigation pane.
3. Run a **CDP** discovery using one of the 15 device IP addresses (15 devices that share the CLI global credentials).

   You run a **CDP** discovery in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.
4. Run 5 separate **Range** discoveries for each of the remaining 5 devices using the appropriate CLI exception credentials (for example, Credential-1, Credential-2-5, etc.).

   You configure the CLI exception credentials in the **Discovery** window. You access this window, by clicking **Discovery** on the Navigation pane.
5. Review the **Device Inventory** table in the **Device Inventory** window to check the discovery results.

Discovery Credentials Caveats

The following are caveats for the Cisco APIC-EM discovery credentials:

- If a device credential changes in a network device or devices after Cisco APIC-EM discovery is completed for that device or devices, any subsequent polling cycles for that device or devices will fail. To correct this situation, an administrator has following options:
  - Update the CLI global credentials with the new device credential. The devices would then be authenticated in a subsequent polling cycle.
  - Start a new discovery with the changed CLI exception credentials that matches the new device credential.
- If the ongoing discovery fails due to a device authentication failure (for example, the provided discovery credential is not valid for the devices discovered by current discovery), then the administrator has following options:
  - Stop or delete the current discovery. Create one or more new network discovery jobs (either a **CDP** or **Range** discovery type) with a CLI exception credential that matches the device credential.
  - Modify one of the CLI global credentials to the new device credential (if possible), so the same discovery can discover the device in a subsequent polling cycle.
- Deleting a CLI global credential does not affect already discovered devices. These already discovered devices will not report an authentication failure.
- The Cisco APIC-EM provides a REST API which allows the retrieval of the list of managed network devices in the Cisco APIC-EM inventory, including the administrative credentials (SNMP community strings, CLI username and password, CLI enable password) in cleartext. The purpose of this API is to allow an external application to synchronize its own managed device inventory with the devices that have been discovered by the Cisco APIC-EM. For example, for Cisco IWAN scenarios, Prime Infrastructure makes use of this API in order to populate its inventory with the IWAN devices contained

in the Cisco APIC-EM inventory in order to provide monitoring of the IWAN solution. Any user account with a ROLE_ADMIN has access to this API.

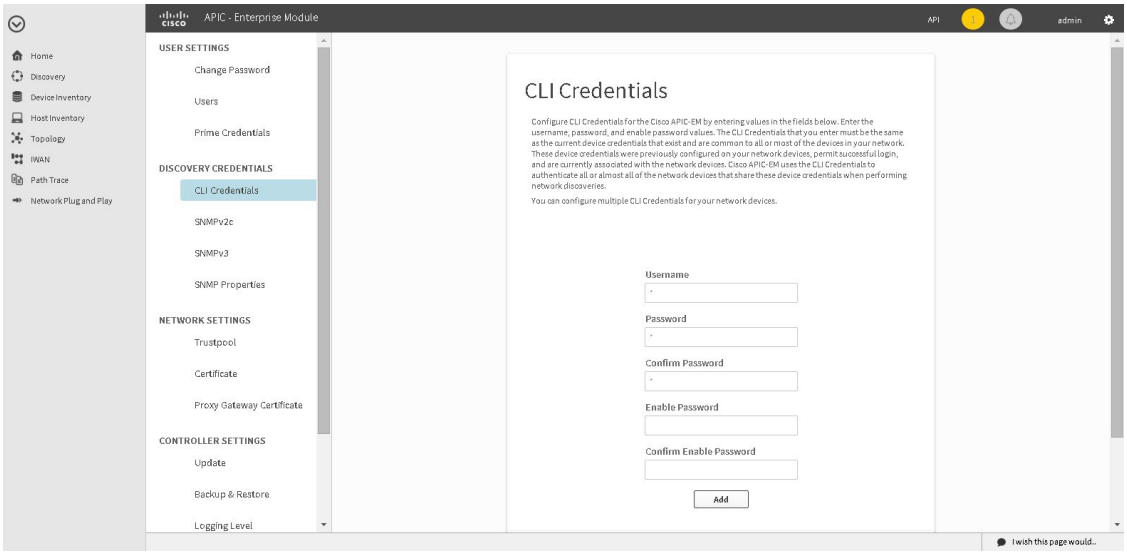
Configuring CLI Credentials—Global

CLI credentials are defined as preexisting *device* credentials that are common to most of the devices in a network. CLI credentials are used by the Cisco APIC-EM to authenticate and access the devices in a network that share this CLI credential when performing devices discoveries.

You configure the CLI global credentials in the **CLI Credentials** window.

Note You can configure up to five CLI credentials.

Figure 3: CLI Credentials Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to configure the CLI global credentials as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **CLI Credentials** to view the **CLI Credentials** window.

In the **CLI Credentials** window, enter the appropriate CLI global credentials for the devices within your network or networks.

Step 4 Enter the CLI Credentials username in the **Username** field.

Step 5 Enter the CLI Credentials password in the **Password** field.

Step 6 Reenter the CLI Credentials password in the **Confirm Password** field to confirm the value that you just entered.

Step 7 If your network devices have been configured with an enable password, then enter the CLI Credentials for the enable password in the **Enable Password** field.

Note Both the CLI credentials password and enable password are saved in the device's configuration in encrypted form. You cannot view these original passwords after you enter them.

Step 8 If you entered an enable password in the **Enable Password** field, reenter it in the **Confirm Enable Password** field to confirm the value that you just entered.

Step 9 In the **CLI Credentials** window, click **Add** to save the credentials to the Cisco APIC-EM database.

What to Do Next

Proceed to configure SNMP values for your network device discovery.

For a successful device discovery (with all the device information to be collected), CLI credentials (global and/or exception) and SNMP (v2c and/or v3) should be configured using the controller. The CLI global credentials and SNMP (v2c or v3) are configured in the **Discovery Credentials** windows as described in this chapter, and are used in addition to any CLI exception credentials that are configured in the **Discovery** window.

Related Topics

CLI Credentials—Global, on page 44

Configuring SNMP

You configure SNMP for device discovery using the following **Discovery Credentials** windows in the Cisco APIC-EM GUI:

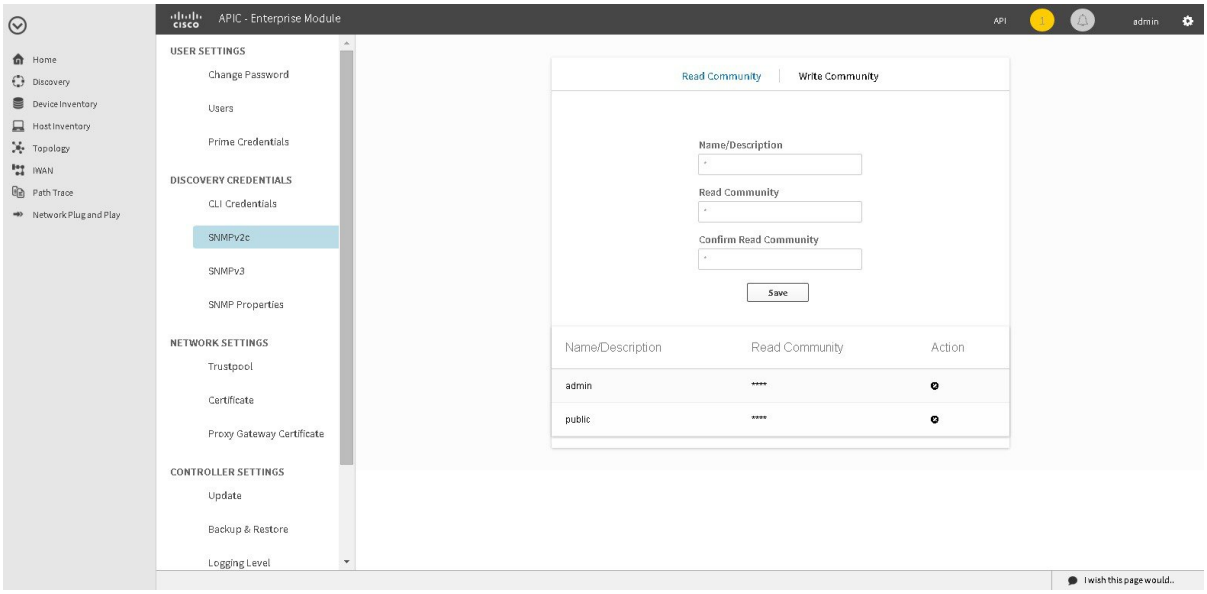
- **SNMPv2c**
- **SNMPv3**
- **SNMP Properties**

Configuring SNMPv2c

You configure SNMPv2c for device discovery in the **SNMPv2c** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv2c for the controller must match the SNMPv2c values that have been configured for your network devices.

Note You can configure up to five read community strings and five write community strings.

Figure 4: Configuring SNMPv2c



SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv2c is the community string-based administrative framework for SNMPv2. Community string is a type of password, which is transmitted in clear text. SNMPv2c does not provide authentication or encryption (noAuthNoPriv level of security).

Note In addition to configuring SNMPv2c for device discovery in the controller, a "best effort" Cisco APIC-EM discovery is in place, meaning that devices having SNMP with Read-Only (RO) community string set to "public" will be discovered all the time irrespective of the configured SNMP Read/Write community string.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator permissions to configure the discovery credentials (SNMPv2c) as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM,

see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMPv2c** to view the **SNMPv2c** window.

Step 4 In the **SNMPv2c** window, click **Read Community**.
Enter your **Read Community** values:

- **Name/Description—**Description of the Read-Only (RO) community string value and/or the device or devices that are configured with it.
- **Read Community—**Read-Only community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Read Community—**Reenter the Read-Only community string to confirm the value that you just entered.

Note If you are configuring SNMPv2c for your discovery, then configuring **Read Community** values is mandatory.

Step 5 Click **Save** to save your **Read Community** values.
The **Read Community** values will appear in the table below.

Step 6 (Optional) In the **SNMPv2c** window, click **Write Community**.
Enter your **Write Community** values:

- **Name/Description—**Description of the Write community string value and/or the device or devices that are configured with it.
- **Write Community—**Write community string value configured on devices that you need the controller to connect to and access. This community string value must match the community string value pre-configured on the devices that the controller will connect to and access.
- **Confirm Write Community—**Reenter the Write community string to confirm the value that you just entered.

Step 7 (Optional) Click **Save** to save your **Write Community** values.
The **Write Community** values will appear in the table below.

What to Do Next

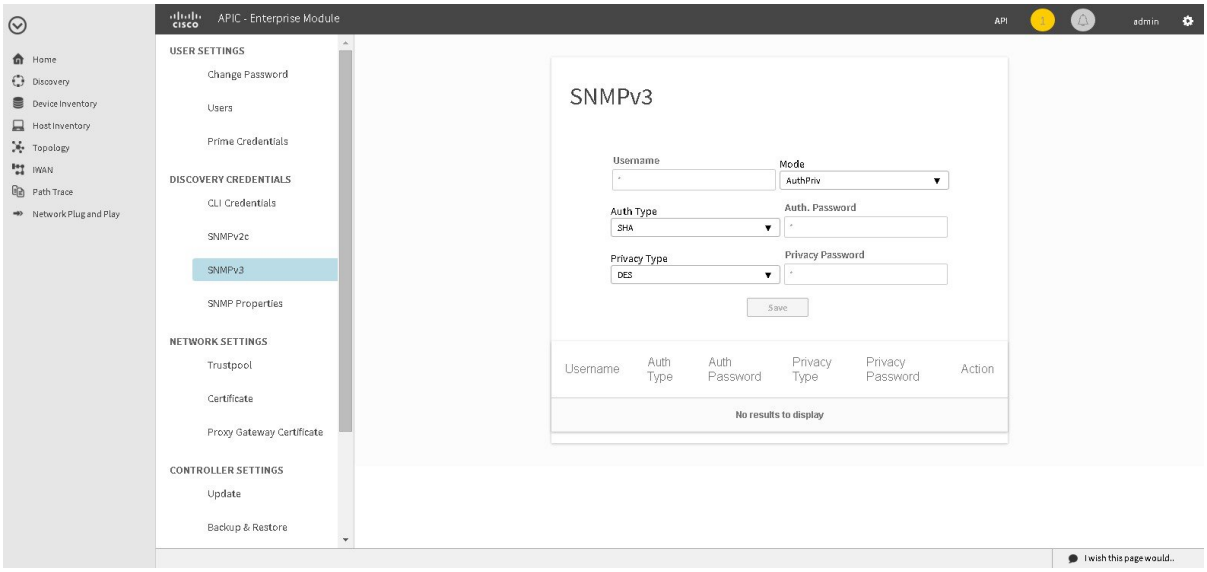
If required for your SNMP configuration, proceed to configure either **SNMPv3** or **SNMP Properties** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

Configuring SNMPv3

You configure SNMPv3 for device discovery in the **SNMPv3** window in the Cisco APIC-EM GUI. The SNMP values that you configure for SNMPv3 for the controller must match the SNMPv3 values that have been configured for your network devices. You can configure up to five SNMPv3 settings.

Figure 5: Configuring SNMPv3



SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. The different versions of SNMP are SNMPv1, SNMPv2, SNMPv2c, and SNMPv3.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The following are supported SNMPv3 security models:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption
- AuthNoPriv—Security level that provides authentication but does not provide encryption
- AuthPriv—Security level that provides both authentication and encryption

The following table identifies what the combinations of security models and levels mean:

Table 5: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	User Name	No	Uses a username match for authentication.
v3	AuthNoPriv	Either: • HMAC-MD5 • HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash algorithm (SHA)
v3	AuthPriv	Either: • HMAC-MD5 • HMAC-SHA	Either: • CBC-DES • CBC-AES-128	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard or CBC-mode AES for encryption.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator permissions to configure the discovery credentials (SNMPv3) as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM,

see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMPv3** to view the **SNMPv3** window.
If you use SNMPv3 in your network to monitor and manage devices, then configure the SNMPv3 values for discovery for your network.

Step 4 In the **SNMPv3** window, enter a **Username** value and choose a **Mode** from the drop down menu.
The following **Mode** options are available:

- **AuthPriv**
- **AuthNoPriv**
- **NoAuthNoPriv**

Note Subsequent **SNMPv3** configuration options might or might not be available depending upon your selection for this step.

Step 5 If you selected **AuthPriv** or **AuthNoPriv** as a **Mode** option, then choose an **Authentication** type from the drop down menu and enter an authentication password.
The following **Authentication** options are available:

- **SHA—**Authentication based on the Hash-Based Message Authentication Code (HMAC), Secure Hash algorithm (SHA) algorithm
- **MD5—**Authentication based on the Hash-Based Message Authentication Code (HMAC), Message Digest 5 (MD5) algorithm

Step 6 If you selected **AuthPriv** as a **Mode** option, then choose a **Privacy** type from the drop down menu and enter a SNMPv3 privacy password.
The SNMPv3 privacy password is used to generate the secret key used for encryption of messages exchanged with devices that support DES or AES128 encryption.

The following **Privacy** type options are available:

- **DES—**Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.
- **AES128—**Cipher Block Chaining (CBC) mode AES for encryption.

Step 7 Click **Save** to save your SNMPv3 configuration values.
The **SNMPv3** configured values will appear in the table below.

What to Do Next

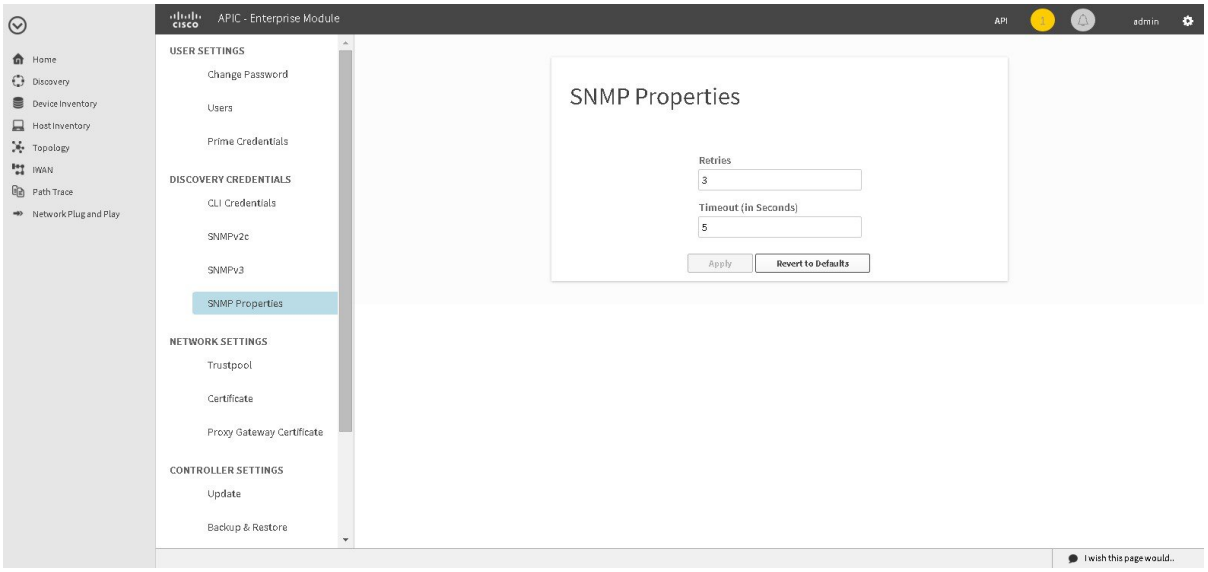
If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMP Properties** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

Configuring SNMP Properties

You configure SNMP properties for device discovery in the **SNMP Properties** window in the Cisco APIC-EM GUI.

Figure 6: Configuring SNMP Properties



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have your network's SNMP information available for this configuration procedure.

You must have administrator permissions to configure the discovery credentials (SNMP properties) as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **SNMP Properties** to view the **SNMP Properties** window.
Configure the SNMP property settings for discovery in your network.

Step 4 In the **SNMP Properties** window, enter a value in the **Retries** field.
The value entered in this field is the number of attempts the controller attempts to use SNMP to communicate with your network devices.

Step 5 In the **SNMP Properties** window, enter a value in the **Timeout** field.

The value entered in this field is the length of time in seconds the controller attempts to use SNMP to communicate with your network devices.

Step 6 Click **Apply** to save your SNMP configuration values.
You can also click **Revert to Defaults** to revert to the SNMP property default values. The following are the SNMP property default values:

- **Retries—**3
- **Timeout—**5

What to Do Next

If required for your SNMP configuration, proceed to configure either **SNMPv2c** or **SNMPv3** using the GUI.

If you are finished with your SNMP configuration, then proceed to import an X.509 certificate and private key into the controller, if necessary for your network configuration.

Security

Importing a Certificate

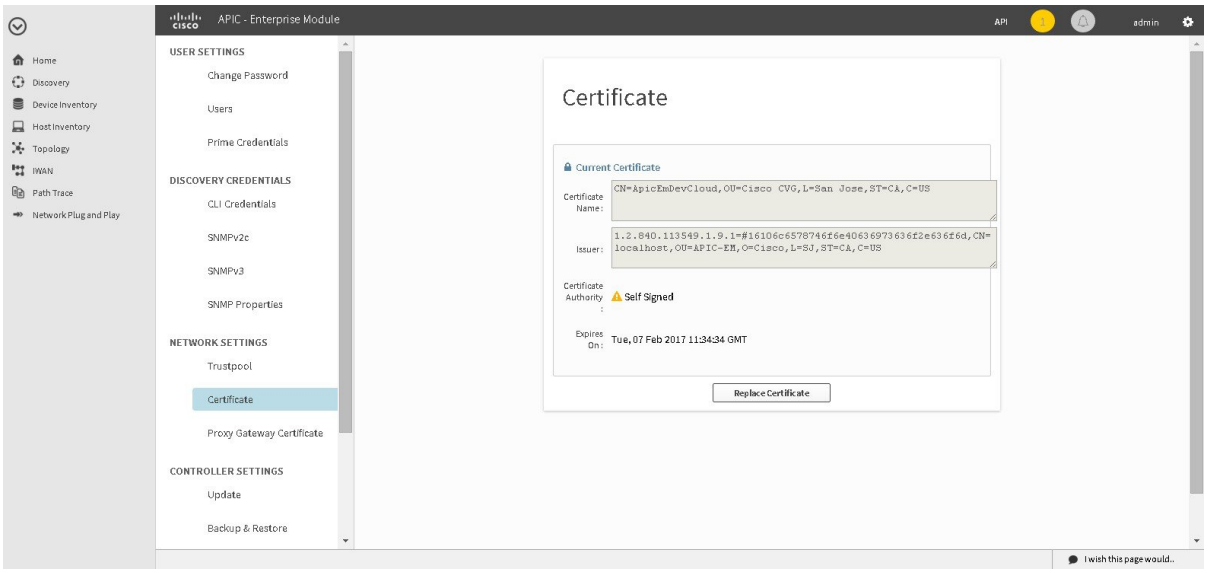
The Cisco APIC-EM supports the import and storing of an X.509 certificate and private key into the controller. After import, the certificate and private key can be used to create a secure and trusted environment between the Cisco APIC-EM, NB API applications, and network devices.

Note If you have a multi-host deployment and you plan to acquire a valid CA-issued certificate for your controller HTTPS server, then use the virtual IP address that you assigned to the multi-hosts as the Common Name for the certificate when you order. If you are using a host name instead, make sure the host name is DNS-resolvable to the virtual IP address of the multi-host deployment.

If you already have a single host Cisco APIC-EM with a previously purchased CA-issued certificate for its external IP address, then it is ideal to use that original physical IP address of the single host as the virtual IP address of the multi-host deployment. This way you can save your investment in the CA-issued certificate and also keep the external client applications, using your Cisco APIC-EM services to continue using the same IP address.

You import a certificate and private key using the **Certificate** window in the Cisco APIC-EM GUI.

Figure 7: Certificate Configuration Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have acquired an X.509 certificate and private key from a well-known certificate authority (CA) for the import.

You must have administrator permissions to import a certificate as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Certificate** to view the **Certificate** window.

Step 4 In the **Certificate** window, view the current certificate data.
When first viewing this window, the current certificate data that is displayed is the controller's self-signed certificate. The self-signed certificate's expiration is set for several years in the future.

Note The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the controller's GUI 2 months before the expiration date and time of the certificate.

Additional displayed fields in the **Certificate** window include:

- Certificate Name—The name of the certificate.
- Issuer—The issuer name identifies the entity that has signed and issued the certificate.
- Certificate Authority—Either self-signed or name of the CA.

- Expires On—Expiration date of the certificate.

Step 5 To replace the current certificate, click the **Replace Certificate** button.
The following new fields appear:

- **Certificate—**Fields to enter certificate data
- **Private Key—**Fields to enter private key data

Step 6 In the **Certificate** fields, choose the file format type of the certificate:

- **PEM—**Privacy enhanced mail file format
- **PKCS—**Public-key cryptography standard file format

Choose one of the above file types for the certificate that you are importing into the Cisco APIC-EM.

Step 7 If you choose **PEM**, then perform the following tasks:

- For the **Certificate** field, import the **PEM** file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

  Note For a PEM file, it must have a valid PEM format extension (.pem, .cert, .crt). The maximum file size for the certificate is 10KB

- For the **Private Key** field, import the private key by dragging and dropping this file into the **Drag n' Drop a File Here** field.
  - Choose the encryption option from the **Encrypted** drop-down menu for the private key.
  - If encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

    Note For the private keys, they must have a valid private key format extension (.pem or .key).

Step 8 If you choose **PKCS**, then perform the following tasks:

- For the **Certificate** field, import the **PKCS** file by dragging and dropping this file into the **Drag n' Drop a File Here** field.

  Note For a PKCS file, it must have a valid PKCS format extension (.pfx, .p12). The maximum file size for the certificate is 10KB

- For the **Certificate** field, enter the passphrase for the certificate using the **Passphrase** field.

  Note For PKCS, the imported certificate also requires a passphrase.

- For the **Private Key** field, choose the encryption option for the private key using the drop-down menu.
- For the **Private Key** field, if encryption is chosen, enter the passphrase for the private key in the **Passphrase** field.

Step 9 Click the **Upload/Activate** button.

Step 10 Return to the **Certificate** window to view the updated certificate data.

The information displayed in the **Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Related Topics

Cisco APIC-EM Certificate and Private Key Support, on page 11
Cisco APIC-EM Certificate Chain Support, on page 12

Importing a Proxy Gateway Certificate

In some network configurations, proxy gateways may exist between the Cisco APIC-EM and network devices. Common ports such as 80 and 443 pass through the gateway proxy in the DMZ, and for this reason SSL sessions from the network devices meant for the controller terminate at the proxy gateway. Therefore, these network devices can only communicate with the controller via the proxy gateway. In order for the network devices to establish secure and trusted connections with the controller, or if present, a proxy gateway, then the network devices should have their PKI trust stores appropriately provisioned with the relevant CA root certificates or the server's own certificate under certain circumstances.

Cisco Network Plug and Play

With the Cisco Network Plug and Play (PnP) application, the Cisco APIC-EM responds to HTTPS requests from supported Cisco network devices and permits these devices to download and install an image and desired configuration. Before a device can download such information from the controller, the initial interaction between the controller and device involves the establishment of a trust relationship.

At first interaction with a PnP enabled device, that PnP enabled device is provisioned by the controller with trust information that includes a CA root certificates bundle or at the least the certificate of the CA that issued the server side certificate. Note that in latter case, the CA may or may not be a well known CA.

In certain Cisco Network Plug and Play scenarios, your network configuration may have a proxy gateway present between the controller and PnP enabled devices. For instance in an IWAN deployment a branch router might communicate to the Cisco APIC-EM through a proxy gateway at the DMZ at initial provisioning. Depending on whether there is a proxy gateway present or not, the trust information provided by the controller at the initial transaction with the devices may correspond to the proxy gateway's or to the controller's certificate issuer (if the corresponding server certificates are not valid CA signed). On the other hand, in either proxy or non-proxy cases, if the certificate is a simple self-signed certificate, then that certificate will be downloaded by the device into its trust store.

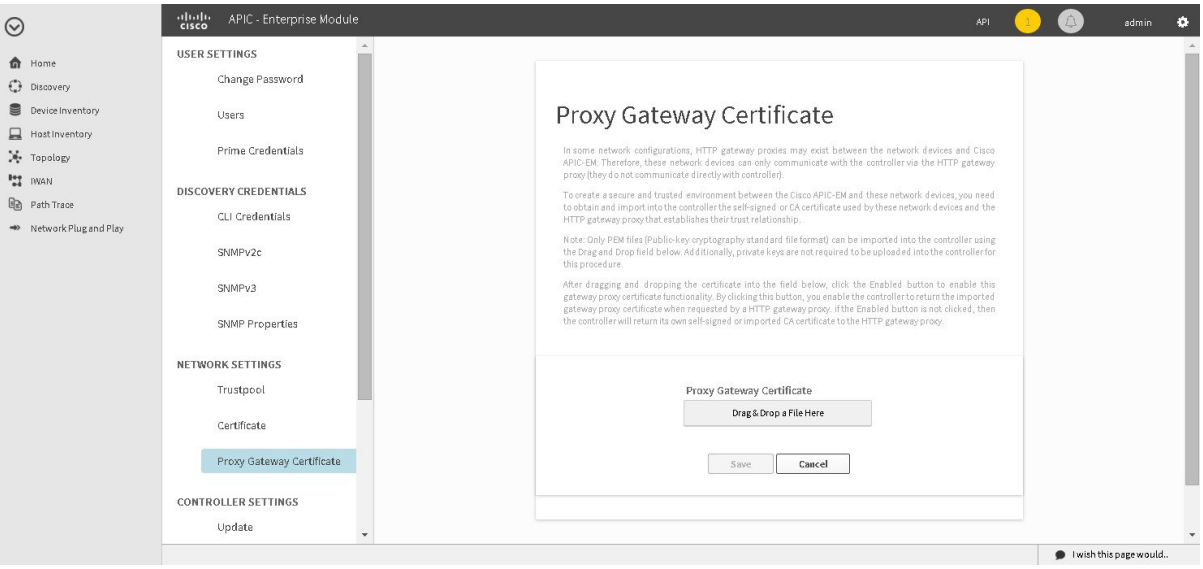
Note Using a self-signed certificate for either the Cisco APIC-EM or the proxy gateway is strongly discouraged. We strongly recommend using a publicly verifiable CA issued certificate to be installed for the controller, as well as the proxy gateway if one is present.

With a valid CA issued certificate for the controller or the proxy gateway (if present), the PnP enabled devices can download the trustpool bundle (ios.p7b) containing all the well known CA root certificates. This permits the devices to establish secure connections to the controller or to the proxy gateway for further provisioning and operation of those devices. If such a certificate is not a valid CA issued or self-signed, then the devices will have to download the issuing CA's or self-signed certificate to proceed further with a secure connection to the controller or a proxy gateway in front of the controller. The Cisco APIC-EM facilitates automatic

downloads of the relevant trusted certificates on the devices, depending on the nature of the certificate installed on it. However; when a proxy gateway is present, it provides a provisioning GUI to facilitate similar pre-provisioning.

In network topologies where there is a proxy gateway present between controller and PnP enabled devices, follow the procedure below to import a proxy gateway certificate into the controller.

Figure 8: Proxy Gateway Certificate Window



Before You Begin

You have successfully deployed the Cisco APIC-EM and it is operational.

In your network, an HTTP proxy gateway exists between the controller and PnP enabled network devices. The PnP enabled network devices will use the proxy gateway's IP address to reach the Cisco APIC-EM controller and its services.

You have the certificate file currently being used by the proxy gateway. The certificate file contents can consist any of the following:

- The proxy gateways's certificate in PEM format, with the certificate being self-signed.
- The proxy gateway's certificate in PEM format, with the certificate being issued by a valid, well-known CA, such as the Comodo Group, Symantec, or DigiCert.
- The proxy gateway's certificate and the issuing CA root certificate.

Note The certificate file is structured in the above order as a chain and in PEM format. This is required if the CA is not a valid, well-known CA. For example, a CA not present in the Cisco ios.p7b trust pool bundle.

- The proxy gateways's certificate and a Sub CA certificate.

Note The certificate file is structured in the above order and as a chain in PEM format. This is required if the issuing Root CA, Sub CA is a well-known valid CA such as the Comodo Group, Symantec, or DigiCert.

You must have administrator permissions to import the certificate as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

The certificate used by the devices and proxy gateway must be imported into the controller by following this procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Proxy Gateway Certificate** to view the **Proxy Certificate** window.

Step 4 In the **Proxy Gateway Certificate** window, view the current proxy gateway certificate data (if this exists).

Note The **Expiration Date and Time** is displayed as a Greenwich Mean Time (GMT) value. A system notification will appear in the controller's GUI 2 months before the expiration date and time of the certificate.

Step 5 To add a proxy gateway certificate, drag and drop the self-signed or CA certificate to the **Drag n' Drop a File Here** field.

Note Only PEM files (Public-key cryptography standard file format) can be imported into the controller using this field. Additionally, private keys are neither required nor uploaded into the controller for this procedure.

Step 6 Click the **Enable** checkbox to enable the proxy gateway certificate functionality.
By clicking on this checkbox, you enable the controller to return the imported proxy gateway certificate when requested by a proxy gateway. if this checkbox is not checked, then the controller will return its own self-signed or imported CA certificate to the proxy gateway.

Step 7 Click the **Save** button.

Step 8 Refresh the **Proxy Gateway Certificate** window to view the updated proxy gateway certificate data.
The information displayed in the **Proxy Gateway Certificate** window should have changed to reflect the new certificate name, issuer, and certificate authority.

Importing a Trustpool Bundle

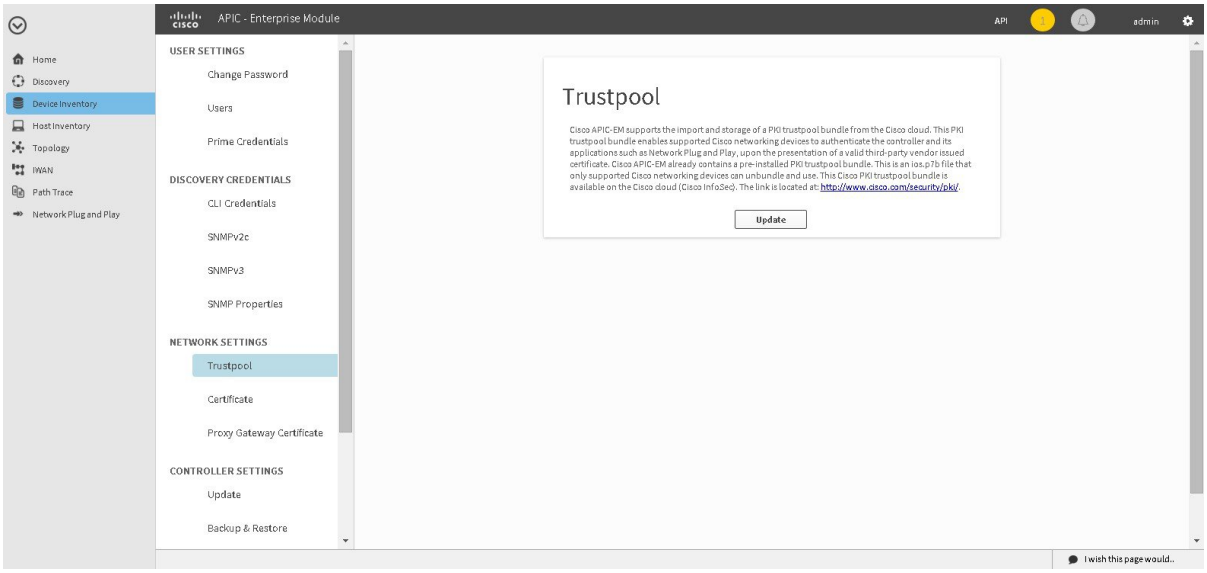
The Cisco APIC-EM contains a pre-installed Cisco trustpool bundle (Cisco Trusted External Root Bundle). The Cisco APIC-EM also supports the import and storage of an updated trustpool bundle from Cisco. The trustpool bundle is used by supported Cisco networking devices to authenticate the controller and its applications, such as Network PnP upon the presentation of its CA signed certificate, as well as any other third party that presents a valid CA signed certificate.

Note The Cisco trustpool bundle is an ios.p7b file that only supported Cisco devices can unbundle and use. This ios.p7b file contains root certificates of valid certificate authorities including Cisco itself. This Cisco trustpool bundle is available on the Cisco cloud (Cisco InfoSec). The link is located at: http://www.cisco.com/security/pki/.

The trustpool bundle provides you with a safe and convenient way to use the same CA to manage all your network device certificates, as well as your controller certificate. The trustpool bundle is used by the controller to validate its own certificate as well as a proxy gateway certificate (if any), to determine whether it is valid CA signed certificate or not. Additionally, the trustpool bundle is available to be uploaded to the Network PnP enabled devices at the beginning of their PnP workflow so that they can trust the controller for subsequent HTTPS-based connections.

You import the Cisco trust bundle using the **Trustpool** window in the Cisco APIC-EM GUI.

Figure 9: Trustpool Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to import a trustpool bundle as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Trustpool** to view the **Trustpool** window.

Step 4 In the **Trustpool** window, click the **Update** button.

After clicking this button, the following actions occur:

- The controller checks to see if a new trustpool bundle exists in the Cisco cloud URL location.
- If the trustpool bundle in the Cisco cloud is the same as the installed trustpool bundle on the controller, then the controller does not initiate a new download and install.
- If the trustpool bundle in the Cisco cloud is a new version of the trustpool bundle, then the controller initiates a new download and install of the trustpool bundle.
- After a new trustpool bundle is downloaded and installed on the controller, the controller makes this trustpool bundle available to the supported Cisco devices to download.

Note The **Update** button in the controller's **Trustpool** window will become active when an updated version of ios.p7b file is available and Internet access is present. The **Update** button will remain inactive if there is no Internet access.

Related Topics

Cisco APIC-EM Trustpool Support, on page 13

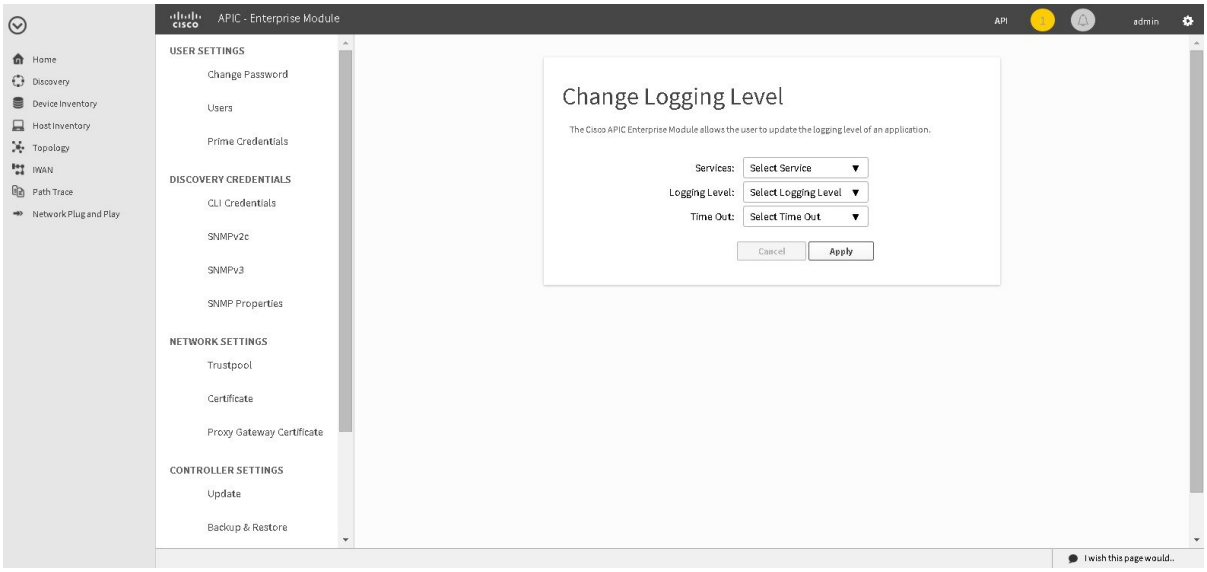
Service Logs

Changing the Logging Level for Services

You can change the logging level for the Cisco APIC-EM services by using the **Changing the Logging Level** window in the Cisco APIC-EM GUI.

A logging level determines the amount of data that is captured to the log files. Each logging level is cumulative, that is, each level contains all the data generated by the specified level and any higher levels. For example, setting the logging level to **Info** also captures **Warn** and **Error** logs.

Figure 10: Service Logging Level Window



The default logging level for services in the controller is informational (**Info**). You can change the logging level with the GUI to set it to debug or trace to capture more information.

Caution Any logs collected at the **Debug** level or higher should be handled with restricted access.

Note The log files are created and stored in a centralized location on your controller. From this location, the controller can query and display them in the GUI The total compressed size of the log files is 2GB. If log files created are in excess of 2GB, then the pre-existing log files are overwritten with the newer log files.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to change the logging level for services as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Changing the Logging Level** to view the **Changing Logging Level** window. The **Logging Level** table appears with the following columns:

- **Services**
- **Logging Level**
- **Timeout**

Step 4 In the **Changing Logging Level** window, choose a service from the **Services** column to adjust its logging level.
Note The **Services** column displays any services that are currently configured and running on the controller.

Step 5 In the **Changing Logging Level** window, choose the new logging level for the service from the **Logging Level** column.
The following logging levels are supported on the controller:

- **Trace—**Trace messages
- **Debug—**Debugging messages
- **Info—**Normal but significant condition messages
- **Warn—**Warning condition messages
- **Error—**Error condition messages

Step 6 In the **Changing Logging Level** window, choose the time period for the logging level from the **Timeout** column for the logging level adjustment.
You configure logging level time periods in increments of 15 minutes up to an unlimited time period.

Step 7 Review your selection and click the **Apply** button.
To cancel your selection click the **Cancel** button.

The logging level for the specified service is set.

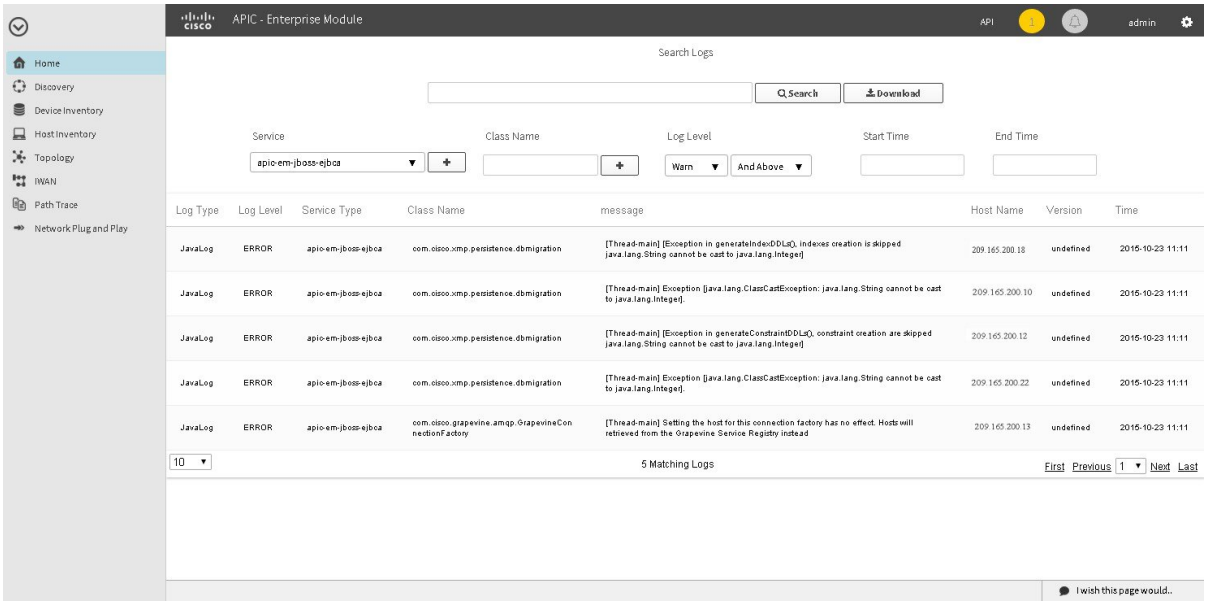
Related Topics

Services

Searching the Service Logs

You can search various controller service logs using the **Search Logs** window in the Cisco APIC-EM GUI.

Figure 11: Search Logs



The following log files are reviewed during a search:

- Linux logs
- Grapevine logs
- Grapevine service logs
- Database logs

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Logs** link from the drop-down menu.
The **Search Logs** window appears. In the **Search Logs** window, you can search the controller service logs by performing the following tasks:

- Search service logs by entering text in the **Search** field.
- Search service logs by configuring the GUI drop-down fields and menus.
- Search service logs by both entering search text and by using the GUI drop-down fields and menus as filters to that text.

Note There are no mandatory fields in the GUI that must have a value entered to conduct a search. You do not have to configure any specific field to run a search.

Step 3 (Optional) Enter a string value in the **Search Logs** field at the top of the **Search Log** window and click the **Search** button.
The log search results are displayed at the bottom of the **Search Logs** window in a table. You can view the following information from the search:

- **Log Level—**Log level (Error, Warn, Trace, Debug, Info)
- **Service Type—**Type of service (also including Grapevine and Linux services)
- **Class Name—**Java class that executed the request.
- **Message—**Actual detail of message that was sent to the log file. For example, "File not found" or "Resource xxx not found".
- **Host Name—**Grapevine host name that generated the request.
- **Version—**Version of the service.
- **Time—**Time message was sent to the log file.

Below the table are numerical filters. Adjust these filters to limit the number of logs displayed in the table (10, 25, 50, 100) or to view groups of a logs at a time (First, Previous, Next, Last, or 1-3).

Step 4 (Optional) In the **Search Logs** window, choose a service from the **Services** drop-down menu for the search and click the plus sign (+).
You can add several different services to your search, by choosing from the drop-down menu and then clicking the plus sign(+).

Note The **Services** drop-down menu displays any services that are currently configured and running on the controller.

Step 5 (Optional) In the **Search Log** window, type in a Java class in the **Class Name** field and click the plus sign (+).
You can add several different Java classes to your search, by choosing from the drop-down menu and then clicking the plus sign(+).

Step 6 (Optional) In the **Search Logs** window, choose a logging level from the **Log Level** drop-down menu.
The following logging levels are supported:

- **Trace—**Trace messages
- **Debug—**Debugging messages
- **Info—**Normal but significant condition messages
- **Warn—**Warning condition messages
- **Error—**Error condition messages

Step 7 (Optional) Adjust the logging level by choosing an appropriate condition in the second **Log Level** drop-down menu.
The following logging level adjustments are supported:

- **And Below—**Search for the specified logging level and any other logging level that has a lower level. For example, a **Trace** has a lower logging level than a **Warn**.
- **Only—**Search only for the specified logging level. Ignore any other logging levels in the results.

- **And Above—**Search for the specified logging level and any other logging level with a higher level. For example, a **Warn** has a higher logging level than a **Debug**.

Step 8 (Optional) In the **Search Logs** window, enter a start time for the logs in the **Start Time** field for the search or use the calendar icon.
If entering a date and time directly, use the following formats:

- Hour: Minutes, AM or PM
- MM/DD/YYYY

Step 9 (Optional) In the **Search Logs** window, enter an end time for the logs in the **End Time** field for the search or use the calendar icon.
If entering a date and time directly, use the following formats:

- Hour: Minutes, AM or PM
- MM/DD/YYYY

Step 10 Review your log search settings and then click the **Search** button.
The log search results are displayed at the bottom of the **Search Log** window in a table.

Below the table are numerical filters. Adjust these filters to limit the number of logs displayed in the table (10, 25, 50, 100) or to view groups of a logs at a time (First, Previous, Next, Last, or 1-3).

What to Do Next

Proceed with any additional service log searches.

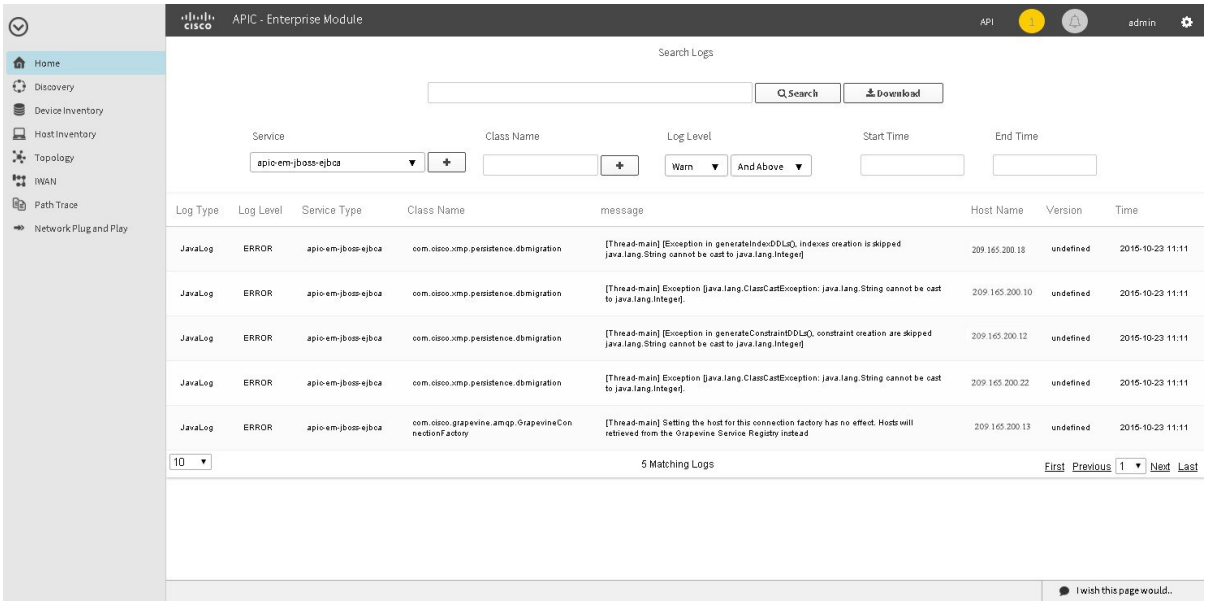
Related Topics

Services

Downloading the Service Logs

You can download various controller service logs using the **Search Logs** window in the Cisco APIC-EM GUI.

Figure 12: Downloading Logs



The following log files are reviewed during a search and download:

- Linux logs
- Grapevine logs
- Grapevine service logs
- Database logs

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Logs** link from the drop-down menu.
The **Search Logs** window appears. In the **Search Logs** window, you can download the controller service logs by performing the following tasks:

- Download service logs by entering a string value.
- Download service logs by configuring the GUI drop-down menus and fields.

- Download service logs by both entering a string value and by configuring the GUI drop-down menus and fields as filters to that string value.

Step 3 (Optional) Enter a string value in the **Search Logs** field at the top of the **Search Logs** window and click the **Download** button.
The log download results are displayed at the bottom of the **Search Logs** window.

Step 4 (Optional) In the **Search Log** window, choose a service from the **Services** drop-down menu for the download and click the plus sign (+).
You can add several different services to your download, by choosing from the drop-down menu and then clicking the plus sign(+).

Note The **Services** drop-down menu displays any services that are currently configured and running on the controller.

Step 5 (Optional) In the **Search Log** window, choose a Java class from the **Class** drop-down menu for the download and click the plus sign (+).
You can add several different Java classes to your download, by choosing from the drop-down menu and then clicking the plus sign(+).

Step 6 (Optional) In the **Search Logs** window, choose a logging level from the **Log Level** drop-down menu.
The following logging levels are supported:

- **Trace—**Trace messages
- **Debug—**Debugging messages
- **Info—**Normal but significant condition messages
- **Warn—**Warning condition messages
- **Error—**Error condition messages

Step 7 (Optional) Adjust the logging level by choosing an appropriate condition in the second **Log Level** drop-down menu.
The following logging level adjustments are supported:

- **And Below—**Search for the specified logging level and any other logging level that has a lower level. For example, a **Trace** has a lower logging level than a **Warn**.
- **Only—**Search only for the specified logging level. Ignore any other logging levels in the results.
- **And Above—**Search for the specified logging level and any other logging level with a higher level. For example, a **Warn** has a higher logging level than a **Debug**.

Step 8 (Optional) In the **Search Logs** window, enter a start time for the logs in the **Start Time** field for the download or use the calendar icon.
If entering a date and time directly, use the following formats:

- Hour: Minutes, AM or PM
- MM/DD/YYYY

Step 9 (Optional) In the **Search Logs** window, enter an end time for the logs in the **End Time** field for the download or use the calendar icon.
If entering a date and time directly, use the following formats:

- Hour: Minutes, AM or PM
- MM/DD/YYYY

Step 10 Review your log search settings and then click the **Download** button.
The log download results are displayed at the bottom right of the **Search Log** window as a page icon displaying the number of logs using the following format: `Search Results (5).log`.

Step 11 Click on the icon for the log download results.
A new window opens that displays the log download data. This data is organized using the following parameters:

- **Timestamp—**Time message was sent to the log file
- **Service type—**Service
- **Class—**Java class that executed the request.
- **Log level—**Log level
- **Message—**Actual detail of message that was sent to the log file. For example, "File not found" or "Resource xxx not found".
- **Version Number—**Version of the service.

What to Do Next

Proceed with any additional service log downloads.

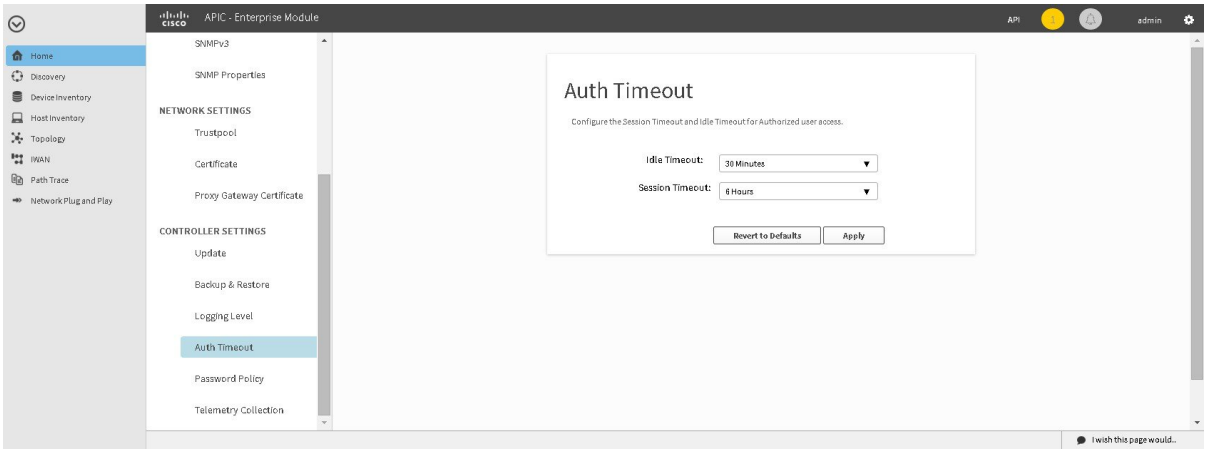
Related Topics

Services

Configuring the Authentication Timeout

You can configure authentication timeouts that require the user to log back into the controller with their credentials (username and password) using the **Authentication Timeout** window in the Cisco APIC-EM GUI.

Figure 13: Authentication Timeout Window



The following authentication timeout values can be configured:

- Idle timeout—Time interval that you can configure before the controller requires re-authentication (logging back in with appropriate credentials) due to Cisco APIC-EM inactivity. Idle timeouts are API-based, meaning that idle timeout is the time the controller is idle between API usages and not GUI mouse clicks or drags.
- Session timeout—Time interval that you can configure before the controller requires re-authentication (logging back in with appropriate credentials). This is a forced re-authentication.

Note Approximately 2-3 minutes before your session is about to idle timeout, a pop-up warning appears in the GUI stating that your session is about to idle timeout and asking if you wish to continue with the current session. Click **Cancel** to ignore the warning and idle timeout of the session within approximately 2-3 minutes. Click **OK** to continue the session for another 30 minutes.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to configure the authentication timeout as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the

chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Authentication Timeout** to view the **Authentication Timeout** window.

Step 4 (Optional) Configure the idle timeout value using the **Idle Timeout** drop-down menu.
You can configure the idle timeout value in increments of 5 minutes, up to an hour. The default value is 30 minutes.

Step 5 (Optional) Configure the session timeout value using the **Session Timeout** drop-down menu.
You can configure the session timeout value in increments of 30 minutes, up to 24 hours. The default value is six hours.

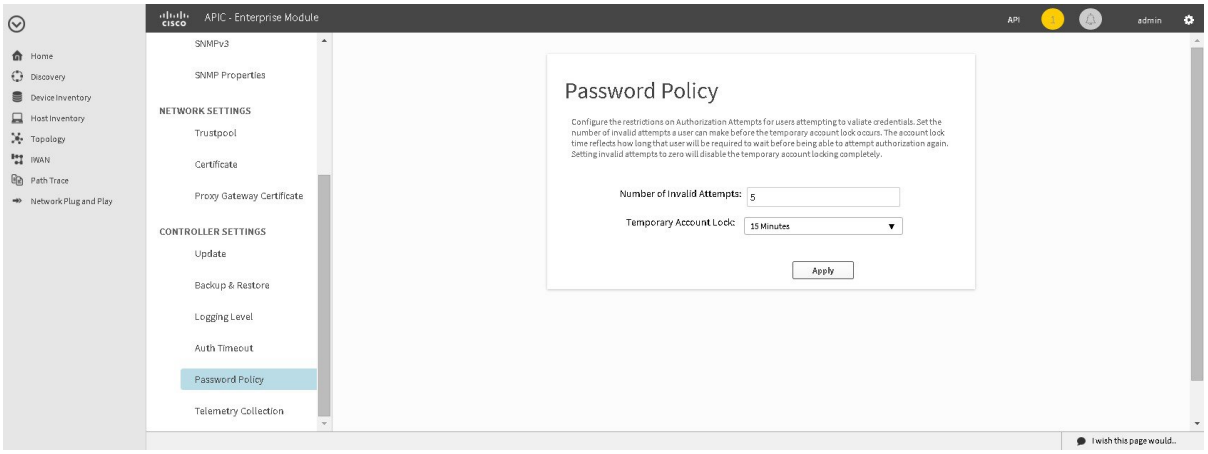
Step 6 Click the **Apply** button to apply your configuration to the controller.
To restore the authentication timeout defaults to the controller, click the **Revert to Defaults** button.

Configuring Password Policies

As an administrator, you can control the number of consecutive, invalid user login attempts to the Cisco APIC-EM. Once a user crosses the threshold set by you as administrator, the user's account is locked and access is refused. Additionally, as an administrator, you can also configure the length of time that the user account is locked. The user account will remain locked until the configured time period expires.

You configure these controller access parameters for the Cisco APIC-EM using the **Password Policy** window.

Figure 14: Password Policy Window



The following password policy functionality is supported:

- As an administrator, you can set the number of consecutive, invalid user login attempts to the controller. These consecutive, invalid user login attempts can be set from 0 to 10 attempts, with 8 attempts being

the default value. Setting invalid attempts to 0 will disable the feature of locking a user with invalid password attempts.

- As an administrator, you can set the length of time a user account is locked. Permitted lock time intervals for a user account range from 1-3600 seconds, with 900 seconds being the default value.
- When a user account is locked due to the number of consecutive, invalid login attempts, entering correct credentials will still result in a login failure until the expiration of the configured lock out time period.
- An administrator can unlock the user account at any time.

  We recommend that you create at least two administrator accounts for your deployment. With two administrator accounts, if one account is locked for whatever reason then the other account can be used to unlock that locked account.

Note For information about how to unlock a user account, see the Chapter 4, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

- A locked user account is unlocked when the configured lock out time period expires.
- A user account can never be permanently locked, but to deny access permanently, an administrator can delete the account.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to configure password policies as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Password Policy** to view the **Password Policy** window.

Step 4 (Optional) Configure the number of permitted consecutive, invalid password attempts by choosing from the **Number of Invalid Attempts** drop-down menu.

Step 5 (Optional) Configure the time interval for locking a user account by choosing from the **Temporary Account Lock** drop-down menu.

Step 6 Click the **Apply** button to apply your configuration to the controller.

Related Topics

Password Requirements, on page 14

Updating the Cisco APIC-EM Software

You can update the Cisco APIC-EM to the latest version using the controller's software update procedure. This procedure requires that you perform the following tasks:

1. Download the release upgrade pack from the secure Cisco cloud.
2. Run a checksum against the release upgrade pack.
3. Upload the release upgrade pack to the controller using the GUI.
4. Update the controller's software with the release upgrade pack.

Note In a multi-host cluster, you only need to update a single host. After updating that single host, the other two hosts are automatically updated with the release upgrade pack.

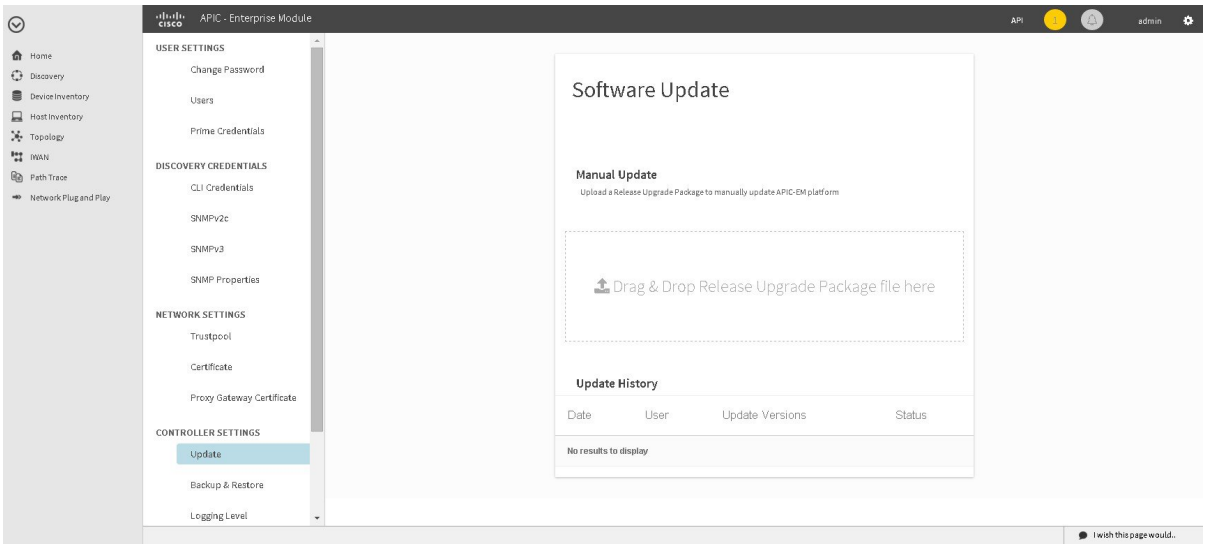
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

You perform the upload and update procedure using the **Software Update** window in the Cisco APIC-EM GUI.

Figure 15: Software Update Window



Note After a successful upload and software update, you are not permitted to rollback to an earlier Cisco APIC-EM version.

Before You Begin

You must have administrator permissions to update the Cisco APIC-EM as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You must have received notification from Cisco that the Cisco APIC-EM software update is available for you to download from the secure Cisco website.

You can be notified about the availability of a Cisco APIC-EM software update in the following ways:

- Email notification from Cisco support and/or updated release notes.
- System notification through the controller GUI.

Note Notification about available release upgrade packs can be viewed by clicking the **System Notifications** icon on the menu bar.

Step 1 Review the information in the Cisco notification about the Cisco APIC-EM update file and checksum.

The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific update. The release upgrade pack can be as large as several Gigabits.

Step 2 Download the release upgrade pack from the secure Cisco website to your laptop or to a location within your network.

Step 3 Run a checksum against the release upgrade pack using your own checksum verification tool or utility (either MD5 or SHA512).

Step 4 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 5 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 6 Click the **Settings** link from the drop-down menu.

Step 7 In the **Settings** navigation pane, click **Software Update** to view the **Software Update** window.

Step 8 If the release upgrade pack is acceptable to use for updating the controller (checksum value match in step 4), then drag and drop the release upgrade pack from the download location on your laptop or in your network onto the **Manual Update** field in the **Software Update** window.
After dropping the release upgrade pack onto the **Manual Update** field, the upload process begins.

The upload process may take several minutes depending upon the size of the release upgrade pack and your network connection. During the upload process, you can continue to work with the controller. Once the upload process ends and the update process begins, you will not be able to work with the controller.

Note If you close the **Software Update** window for any reason, then the upload process stops. To start the upload process again, open the **Software Update** window and drag and drop the release upgrade pack onto the **Manual Update** field again. The upload process starts where it previously stopped. To avoid any interruptions to the upload process while working with the controller, open additional windows in the GUI for any other tasks. Keep the **Software Update** window open during the upload process.

Step 9 Once the upload process finishes, the update process automatically begins. A message appears in the GUI stating that the update process has started and is in progress.
You should refrain from working with the controller during the update process. During the update process, the controller may shut down and restart. The shut down process may last for several minutes.

Note At the beginning of the update process, the controller performs a second verification test on the release upgrade pack. The release upgrade pack itself contains an encrypted security value (signature) that will be decrypted and reviewed by the controller. This second verification test ensures that the release upgrade pack that has been uploaded is from Cisco. The release upgrade pack must pass this second verification test before the update process can continue.

Step 10 Once the update process finishes, you will receive a success or failure notification.
If the update was successful, you will receive a successful update notification and can then proceed working with the controller. If the update was unsuccessful, you will receive an unsuccessful update notification with suggested remedial actions to take.

Note An unsuccessful update will cause a rollback to the current controller software. For example, if the current version is 1.0.0.1 and an unsuccessful update to version 1.0.0.2 occurs, then the controller rolls back to the current version, 1.0.0.1.

After the update (or attempted update), information about it will also appear in the **Update History** field of the **Software Update** window. The following update data is displayed in this field:

- **Date—**Local date and time of the update
- **User—**Username of the person initiating the update
- **Update Version—**Update path of release upgrade pack version represented with an arrow.
- **Update Status—**Success or failure status of the update.

Note If you place your cursor over (mouseover) a failure status in this field, then additional details about the failure is displayed.

Backing Up and Restoring the Cisco APIC-EM

As with any other system upon which your company or organization relies, you need to ensure that the Cisco APIC-EM is backed up regularly, so that it can be restored in case of hardware or other failure.

Caution For the IWAN solution application, you must review the *Software Configuration Guide for Cisco IWAN on APIC-EM* before attempting a back up and restore. There is important and detailed information about how these processes work for the IWAN solution application that includes what is backed up, what is not backed up, recommendations, limitations, and caveats.

Information about Backing Up and Restoring the Cisco APIC-EM

The back up and restore procedure for the Cisco APIC-EM can be used for the following purposes:

- To create a single backup file to support disaster recovery on the controller
- To create a single backup file on one controller to restore to a different controller (if required for your network configuration)

When you perform a back up using the controller's GUI, you copy and export the controller's database and files as a single file to a specific location on the controller. When you perform a restore, you copy over the existing database and files on the controller using this single backup file.

Note The Cisco APIC-EM uses PostgreSQL as the preferred database engine for all network data. PostgreSQL is an open source object-relational database system.

The following files and data are copied and restored when performing a back up and restore:

- Cisco APIC-EM database
- Cisco APIC-EM file system and files
- X.509 certificates and trustpools
- Usernames and passwords

- Any user uploaded files (for example, any Network Plug and Play image files)

The database and files are compressed into a single *.backup* file when performing the back up and restore. The maximum size of the *.backup* file is 30GB. This number consists of a permitted 20GB maximum size for a file service back up and a 10GB permitted maximum size for the database back up.

Note The .backup file should not be modified by the user.

The following are benchmarks for backing up the Cisco APIC-EM database based upon the size of the backup file:

- 1GB backup file—approximately 5 minutes
- 30GB backup file—approximately 20 minutes

Only a single back up can be performed at a time. Performing multiple back ups at once are not permitted. Additionally, only a full back up is supported. Other types of back ups (for example, incremental back ups) are not supported.

Note After saving the backup file, you can also download it to another location in your network. You can restore the backup file from its default location in the controller or drag and drop the backup file from its location in your network to restore.

When performing a backup and restore, we recommend the following:

- Perform a back up everyday to maintain a current version of your database and files.
- Perform a back up and restore after making any changes to your configuration. For example, when changing or creating a new policy on a device.
- Only perform a back up and restore during a low impact or maintenance time period.

When a back up is being performed, you will be unable to delete any files that have been uploaded to the file service and any changes you make to any files may not be captured by the back up process. When a restore is being performed, the controller is unavailable.

Note You cannot schedule nor automate a back up and restore at this time. Additionally, once started you cannot manually cancel either the back up or restore process.

Related Topics

Backing Up the Cisco APIC-EM, on page 79
Restoring the Cisco APIC-EM, on page 80

Multi-Host Cluster Back Up and Restore

In a multi-host cluster, the database and files are replicated and shared across three hosts. When backing up and restoring in a multi-host cluster, you need to first back up on one of the three hosts in the cluster. You

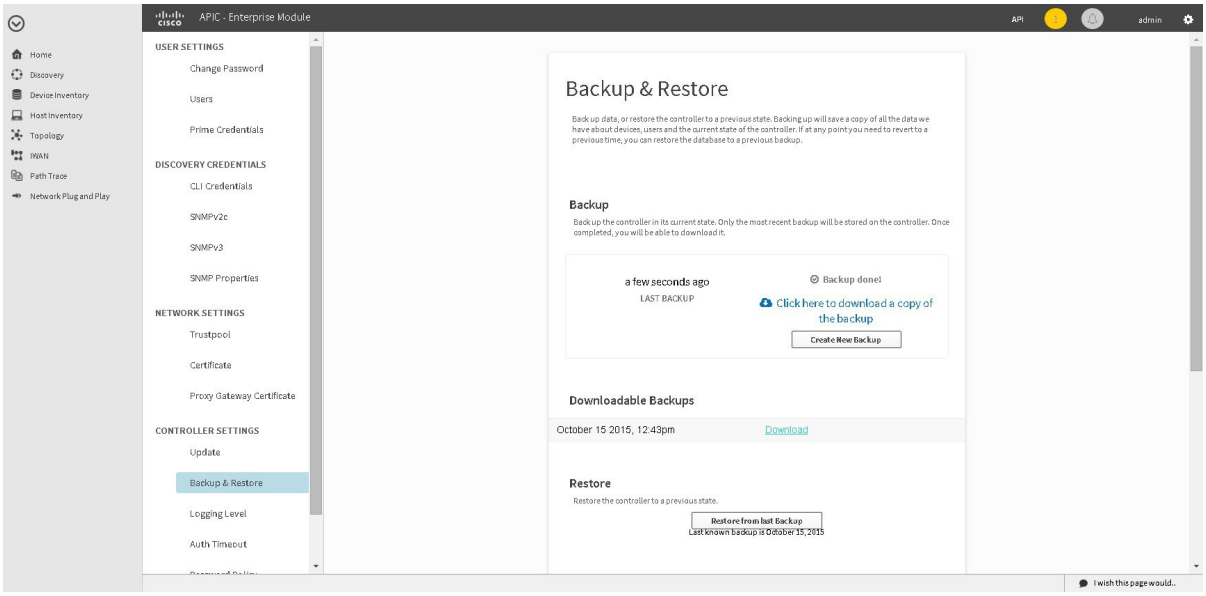
can then use that backup file to restore all three hosts in the cluster. However, you need not perform the restore operation on each of the hosts. You simply restore one of the hosts in the cluster. The controller replicates the restored data to the other hosts automatically.

Note The back up and restore process in a multi-host cluster requires that the Cisco APIC-EM software and version must be the same for all three hosts.

Backing Up the Cisco APIC-EM

You can back up your controller using the **Backup & Restore** window.

Figure 16: Backup & Restore Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to initiate a back up and restore as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Backup & Restore** to view the **Backup & Restore** window.

Step 4 In the **Backup & Restore** window, create a backup file by clicking on the **Create New Backup** button.

After clicking the **Create New Backup** button, a **Backup in Progress** window appears in the GUI.

During this process, the Cisco APIC-EM creates a compressed *.backup* file of the controller database and files. This backup file is also given a time and date stamp that is reflected in its file name. The following file naming convention is used: *yyyy-mm-dd-hh-min-seconds* (year-month-day-hour-seconds).

For example:

backup_2015_08_14-08-35-10

Note If necessary, you can rename the backup file instead of using the default time and date stamp naming convention.

This backup file is then saved to a default location within the controller. You will receive a **Backup Done!** notification, once the back up process is finished. Only a single backup file at a time is stored within the controller.

Note If the back up process fails for any reason, there is no impact to the controller and its database. Additionally, you will receive an error message stating the cause of the back up failure. The most common reason for a failed back up is insufficient disk space. If your back up process fails, you should check to ensure that there is sufficient disk space on the controller and attempt another back up.

Step 5 (Optional) Create a copy of the backup file to another location.
After a successful back up, a **Download** link appears in the GUI. Click the link to download and save a copy of the backup file to a location on your laptop or network.

What to Do Next

When necessary and at an appropriate time, proceed to restore the backup file to the Cisco APIC-EM.

Related Topics

Information about Backing Up and Restoring the Cisco APIC-EM, on page 77

Restoring the Cisco APIC-EM

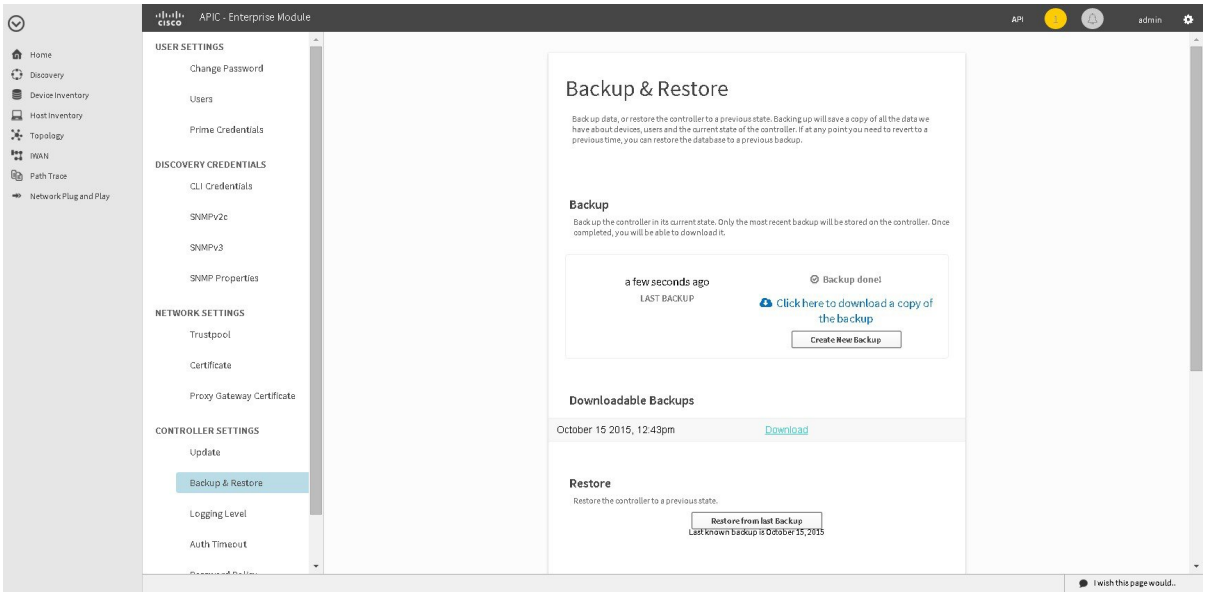
You can restore your controller using the **Backup & Restore** window.

The following restore options are available:

- You can restore from the last know backup file on the controller.
- You can also restore from an archived backup file that was saved and moved to another location on your network.

Caution The Cisco APIC-EM restore process restores the controller's database and files. The restore process does not restore your network state and any changes made by the controller since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates/trustpool bundles.

Figure 17: Backup & Restore Window



Note You can only restore a backup from a controller that is the same software version as the controller where the backup was originally taken from.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to initiate a backup and restore as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

You must have successfully performed a back up of the Cisco APIC-EM database and files following the steps in the previous procedure.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Backup & Restore** to view the **Backup & Restore** window.

Step 4 To restore the backup file, click on the **Restore from last Backup** button.

You can also drag and drop the backup file from its location in your network onto the **Drag and Drop a backup file** field in this window.

During a restore, the backup file copies over the current database.

Note When a restore is in progress, you are not be able to open and access any windows in the GUI.

Step 5 After the restore process completes, log back into the controller's GUI.
If the restore process was successful, you will be logged out of the controller and its GUI. You will need to log back in.

Note The Cisco APIC-EM restore process restores the controller's database and files. The restore process does not restore your network state and any changes made by the controller since the last backup, including any new network policies that have been created, any new or updated passwords, or any new or updated certificates/trustpool bundles.

Proceed to now access the Grapevine root and to run the **reset_grapevine** command.

Caution

If the restore process was unsuccessful, you will receive an unsuccessful restore notification. Since the database may be in an inconsistent state, we recommend that you do not use the database and contact technical support for additional actions to take.

Step 6 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 7 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 8 Enter the **grape backup display** command at the prompt to confirm that the restore process was completed and successful.

```
$ grape backup display
```

Check the command output to ensure that the restore process was completed and successful. Look for the property operation marked "restore" in the command output, with the latest start_time and ensure that the status is marked as a "success".

Step 9 Enter the **reset_grapevine** command at the prompt to run the reset grapevine script.

```
$ reset_grapevine
```

You are then prompted to reenter your Grapevine password.

Step 10 Enter your Grapevine password a second time.

```
[sudo] password for grapevine:********
```

You are then prompted to delete all virtual disks The virtual disks are where the Cisco APIC-EM database resides. For example, data about devices that the controller discovered are saved on these virtual disks. If you enter yes (**y**), all of this data is deleted. If you enter no (**n**), then the new cluster will come up populated with your existing data once the reset procedure completes.

Step 11 Enter **n** to prevent the deletion all of the virtual disks.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete all VIRTUAL DISKS in your APIC-EM cluster? (y/n):n
```

You are then prompted to delete all Cisco APIC-EM authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

Step 12 Enter **n** to prevent the deletion of all authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete authentication timeout policies, user password policies,
and Cisco APIC-EM user accounts other than the primary administrator account? (y/n): n
```

You are then prompted to delete any imported certificates.

Step 13 Enter **n** to prevent the deletion of any imported certificates.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete the imported certificates? (y/n): n
```

The controller then resets itself with the configuration values that were originally set using the configuration wizard the first time. When the controller is finished resetting, you are presented with a command prompt from the controller.

Step 14 Using the Secure Shell (SSH) client, log out of the appliance.

Step 15 Return to the controller's GUI and review the **Backup History** field of the **Backup & Restore** window.
After the restore, information about it appears in the **Backup History** field of the **Backup & Restore** window. The following update data is displayed in this field:

- **Date—**Local date and time of the restore
- **ID—**Controller generated identification number of the backup file
- **Operation—**Type of operation, either backup or restore
- **Update Status—**Success or failure status of the operation.

  Note If you place your cursor over (mouseover) a failure status in this field, then additional details about the failure is displayed.

Related Topics

Information about Backing Up and Restoring the Cisco APIC-EM, on page 77

Telemetry Collection

The Cisco APIC-EM uses telemetry to collect information about the user experience with the controller. This information is collected for the following reasons:

- To proactively identify any issues with the controller

- To better understand the controller features that are most frequently used
- To improve and enhance the overall user experience

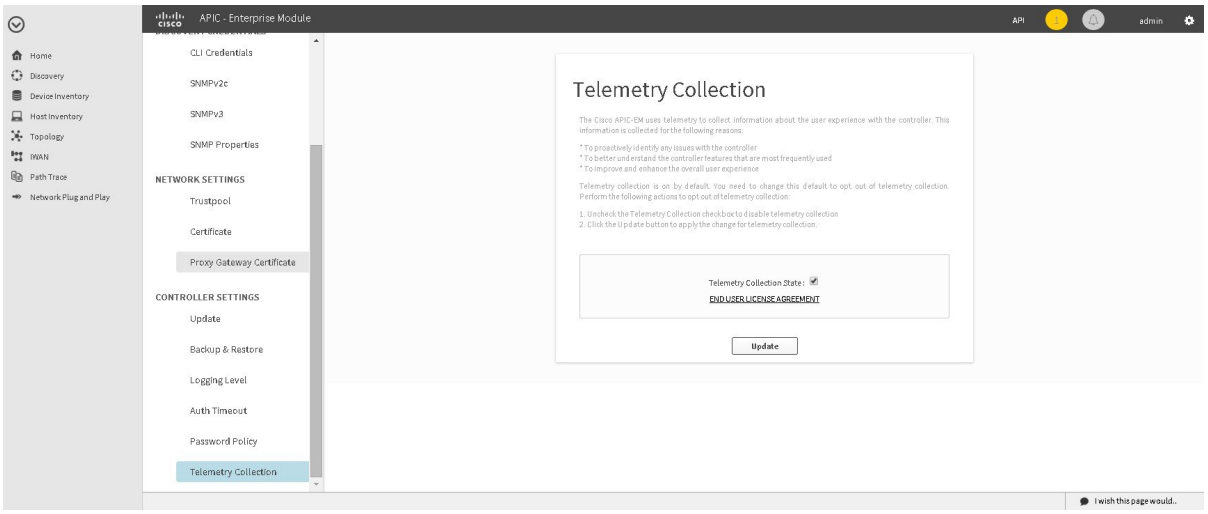
You are able to view the some of the collected telemetry data using the following methods:

- View the logs using the Cisco APIC-EM GUI—For information about this method, see *Searching the Services Logs* in Chapter 5, Configuring the Cisco APIC-EM Settings.
- View the logs using the Grapevine console— For information about this method, see *Troubleshooting Services* in Chapter 6, Troubleshooting the Cisco APIC-EM.

Telemetry is enabled with a telemetry service that collects data from the many other controller services. The telemetry service supports Data Access Service (DAS). The telemetry service uploads data to the Cisco Clean Access Agent (CAA) infrastructure on the Cisco cloud using HTTPS.

Telemetry collection is on by default. If you wish to opt out of telemetry collection, then perform the steps in the following procedure.

Figure 18: Telemetry Collection Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator permissions to configure the authentication timeout as described in this procedure. For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

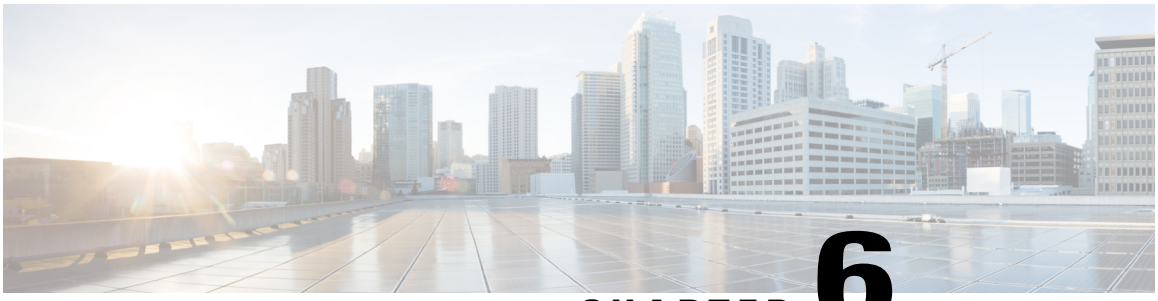
Step 3 In the **Settings** navigation pane, click **Telemetry Collection** to view the **Telemetry Collection** window.

When accessing the **Telemetry Collection** window for the first time, the GUI displays a blue box with a check that indicates that telemetry collection is enabled.

Step 4 (Optional) Click the **End User License Agreement** to review the agreement for telemetry collection.

Step 5 (Optional) Uncheck the **Telemetry Collection** blue box to disable telemetry collection.

Step 6 (Optional) Click the **Update** button to apply the change for telemetry collection.



CHAPTER 6

Troubleshooting the Cisco APIC-EM

Cisco APIC-EM Components and Architecture

This section describes the components and basic architecture of the Cisco APIC-EM. You should review this section to better understand how the controller and its components operate before performing any of the troubleshooting procedures described in this chapter.

The Cisco APIC-EM consists of the following components:

- Hosts
- Linux containers (LXC)
- Grapevine
- Roots and clients
- Services
- Databases
- Networks (internal and external)
- Network connections and NICs

Related Topics

Hosts, on page 88

Hosts

A host can be either an appliance, server or virtual machine where Cisco APIC-EM has been installed. Within the hosts are the Linux containers running instances of the Grapevine clients. The Grapevine clients run the different services. The Grapevine root runs as an application on the host itself and not in any Linux containers.

You can set up either a single host or multi-host deployment for your network.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Linux Containers

Linux containers is a virtualization technology that provides a software virtualization system for systems running GNU/Linux. These containers enable multiple virtual environments to be set up and run simultaneously.

The Cisco APIC-EM components (Grapevine roots and clients) make use of the Ubuntu operating system environment and Linux containers (LXC). The Grapevine root runs as an application on the host itself. The Grapevine clients run in LXCs within the host.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Grapevine

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network, using Grapevine as an Elastic Services platform to support the controller's infrastructure and services. The Grapevine root and clients are key components of this infrastructure.

Note You can use a tool called the Grapevine developer console to troubleshoot roots and clients running services. The Grapevine developer console was bundled with the deployment files and installed when you first deployed the Cisco APIC-EM. You can access the Grapevine developer console at this controller IP address and port number: `https://<controller IP address>:14141`

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Root and Clients

The Grapevine root handles all policy management in regards to service updates, as well as the service lifecycle for both itself and the Grapevine client. The Grapevine client is where the supported services run.

Note You can remotely log into the root using SSH (Secure Shell) to troubleshoot any issues. A default idle timeout of 1 hour has been set for an SSH console login. You will be automatically logged out after 1 hour of inactivity on the SSH console.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Services

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when demand increases, and frees instances of itself when demand decreases.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Databases

The Cisco APIC-EM supports two databases: application and Grapevine. The application database is used for the application and external networking data. The Grapevine database is used for the Grapevine and internal network data. Both databases are replicated in a multi-host environment for scale and high availability.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Networks

The Cisco APIC-EM architecture requires both external and internal networks to operate:

- The external network(s) consists of the network hosts, devices, and NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.
- The internal network consists of the Grapevine roots and clients that are connected to and communicate with each other (service to service). For forwarding to or receiving traffic from the larger external network (that consists of the connected devices and hosts, as well as NTP servers), all inbound and outbound traffic for this internal network passes through a subset of clients connected to the external network. The internal network is isolated and nonroutable from the external network(s), as well as any other internal network.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Network Connections and NICs

The network adapters (NICs) on the host (physical or virtual) are connected to the following external networks:

- Internet (network access required for **Make A Wish** requests, Telemetry, and trustpool updates)
- Network with NTP server(s)
- Network with devices that are to be managed by the Cisco APIC-EM

Note The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment.

Related Topics

Cisco APIC-EM Components and Architecture, on page 87

Troubleshooting an Unsuccessful Installation

After performing an installation using the configuration wizard, you should have received an 'installation was successful' message. If you did not receive this message and your installation was unsuccessful, you can perform the following troubleshooting procedures.

Confirming that Core Services are Running

Before You Begin

You should have attempted to deploy the Cisco APIC-EM following the procedure described in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to display the status of the core services:

```
$ sudo service grapevine status
```

Step 4 Enter your password a second time when prompted.

```
$[sudo] password for grapevine: ********
```

Command output similar to the following should appear. The core services should have a RUNNING status.

```
grapevine is running
grapevine_beacon                 RUNNING    pid 30243, uptime 0:11:11
grapevine_capacity_manager       RUNNING    pid 30549, uptime 0:11:02
grapevine_capacity_manager_lxc_plugin RUNNING    pid 30247, uptime 0:11:11
grapevine_cassandra              RUNNING    pid 30244, uptime 0:11:11
grapevine_root                   RUNNING    pid 30537, uptime 0:11:03status
```

Step 5 If any of the core services are not in the RUNNING state, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files
- Command output

Step 6 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue.

Confirming the Multi-Host Cluster Configuration Values

Before You Begin

You should have attempted to deploy the Cisco APIC-EM following the procedure described in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to display the multi-host configuration.

```
$ grape root display
```

Command output similar to the following should appear.

```
ROOT                                PROPERTY            VALUE
```

```
------------------------------------------------------------------------

4cbe3972-9872-4771-800d-08c89463f1eb   hostname             root-1
4cbe3972-9872-4771-800d-08c89463f1eb   interfaces           [{'interface': 'eth0', 'ip':
'209.165.200.10', 'mac': '00:50:56:100:d2:14', 'netmask': '255.255.255.0'}, {'interface': 'eth1',
'ip': '209.165.200.10', 'mac': '00:50:56:95:5c:18', 'net  mask': '255.255.255.0'}, {'interface':
'grape-br0', 'ip': '209.165.200.11', 'mac': 'ba:ed:c4:19:0d:77', 'netmask': '255.255.255.0'}]
4cbe3972-9872-4771-800d-08c89463f1eb   is_alive             True
4cbe3972-9872-4771-800d-08c89463f1eb   last_heartbeat       Wed Sep 09, 2015 11:02:52 PM (just now)

4cbe3972-9872-4771-800d-08c89463f1eb   public_key           ssh-rsa

c2EAAAADAQABAAABAQDYlyCfidke3MTjGkzsTAu73MtG+lynFFvxWZ4xVIkDkhGC7KCs6XMhORMaABb6
bU4EX/6osa4qyta4NYaijxjL6GL6kPkSBZiEKcUekHCmk1+H+Ypp5tc0wyvSpe5HtbLvPicLrXHHI/TS
Fsa+gLPqg55TflX8RH3i8dHf1Zwq6v4nHVryjAzMXeFYnFHST9e0P62QnkAGh29ktxUpS3fKua9iCVIE
V44t+VvtFaLurG9+FW/ngZwGrR/N0ZJZl6/MQTN3 grapevine@grapevine-root

4cbe3972-9872-4771-800d-08c89463f1eb   root_id              4cbe3972-9872-4771-800d-08c89463f1eb
4cbe3972-9872-4771-800d-08c89463f1eb   root_index           0
4cbe3972-9872-4771-800d-08c89463f1eb   root_version         0.3.0.958.dev140-gda6a16
4cbe3972-9872-4771-800d-08c89463f1eb   vm_password          ******
(grapevine)

#

ROOT                                   PROPERTY             VALUE
------------------------------------------------------------------------

4cbe3972-9872-4771-800d-08c89463f1eb   hostname             root-2
4cbe3972-9872-4771-800d-08c89463f1eb   interfaces           [{'interface': 'eth0', 'ip':
'209.165.200.101, 'mac': '00:50:56:100:d2:14', 'netmask': '255.255.255.0'}, {'interface': 'eth1',
'ip': '209.165.200.11', 'mac': '00:50:56:95:5c:18', 'net  mask': '255.255.255.0'}, {'interface':
'grape-br0', 'ip': '209.165.200.11', 'mac': 'ba:ed:c4:19:0d:77', 'netmask': '255.255.255.0'}]
4cbe3972-9872-4771-800d-08c89463f1eb   is_alive             True
4cbe3972-9872-4771-800d-08c89463f1eb   last_heartbeat       Wed Sep 09, 2015 11:02:52 PM (just now)

4cbe3972-9872-4771-800d-08c89463f1eb   public_key           ssh-rsa

c2EAAAADAQABAAABAQDYlyCfidke3MTjGkzsTAu73MtG+lynFFvxWZ4xVIkDkhGC7KCs6XMhORMaABb6
bU4EX/6osa4qyta4NYaijxjL6GL6kPkSBZiEKcUekHCmk1+H+Ypp5tc0wyvSpe5HtbLvPicLrXHHI/TS
Fsa+gLPqg55TflX8RH3i8dHf1Zwq6v4nHVryjAzMXeFYnFHST9e0P62QnkAGh29ktxUpS3fKua9iCVIE
V44t+VvtFaLurG9+FW/ngZwGrR/N0ZJZl6/MQTN3 grapevine@grapevine-root

4cbe3972-9872-4771-800d-08c89463f1eb   root_id              4cbe3972-9873-4771-800d-08c89463f1eb
4cbe3972-9872-4771-800d-08c89463f1eb   root_index           0
4cbe3972-9872-4771-800d-08c89463f1eb   root_version         0.3.0.958.dev140-gda6a16
4cbe3972-9872-4771-800d-08c89463f1eb   vm_password          ******
(grapevine)
```

The following data is displayed by this command:

- `hostname`—The configured hostname.
- `interfaces`—The configured interface values, including Ethernet port, IP address, and netmask.
- `is_alive`—Status of the host. `True` indicates a running host, `False` indicates a host that has shut down.

- `last_heartbeat`—Date and time of last heartbeat message sent from the host.
- `public_key`—Public key used by host.
- `root_id`—Individual root identification number.
- `root_index`—Individual root index number.
- `root_version`—Software version of root.
- `vm_password`—VMware vSphere password that is masked.

Step 4 If any of the fields in the command output appear incorrect, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files
- Command output

Step 5 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue.

Resolving Access to the Cisco APIC-EM GUI

You access the Cisco APIC-EM GUI by entering the IP address that you configured for the network adapter using the configuration wizard. This IP address connects to the external network. Enter the IP address in your Google Chrome browser in the following format:

https://*IP address*

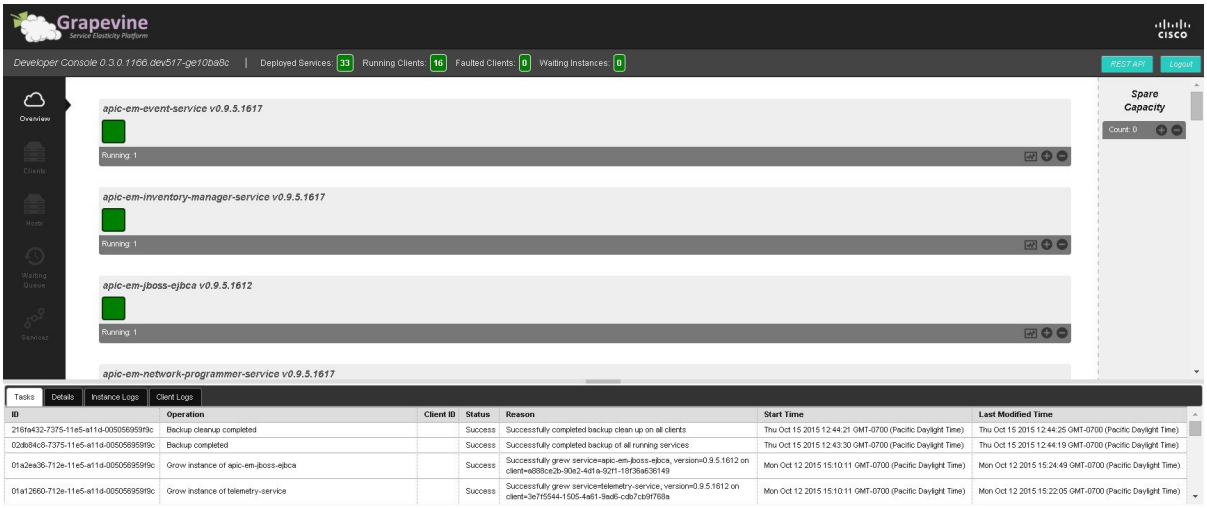
If you are unable to access the Cisco APIC-EM GUI, you must access the Grapevine developer console to check for faulty or failed services.

The Grapevine developer console allows you to monitor the health of your Cisco APIC-EM deployment. The Grapevine developer console is part of the Service Elasticity Platform (Grapevine). You access the Grapevine developer console by entering the IP address that you configured for the network adapter using the configuration wizard, but with a specific port number (**14141**).

For a multi-host cluster, you do not have to log into each host. In a multi-host cluster, you get a single, consolidated view of all of the services running on all three hosts. Multiple instances of services running on different hosts will appear in the Grapevine developer console in a multi-host cluster.

Note A default idle timeout of 1 hour has been set for the Grapevine developer console. You will be automatically logged out after 1 hour of inactivity on the Grapevine developer console.

Figure 19: Grapevine Developer Console



To access the Grapevine developer console to check for faulty or failed services, follow the procedure described below.

Before You Begin

You should have attempted to deploy the Cisco APIC-EM following the procedure described in this guide.

Step 1 Access the Grapevine developer console by opening a Google Chrome browser window and entering the IP address that you configured for the network adapter using the configuration wizard.

Note This IP address connects the appliance to the external network.

For example, enter the following IP address with required port number:

https://*external network IP address:***14141**

Step 2 Enter your administrative username and password when prompted.
The administrative username and password were configured by you using the configuration wizard.

After you enter the username and password, the Grapevine developer console appears. Each installed service with its version number appears in the console in an alphabetical list. Below each service is a square icon that represents the health of the service. Services that have been installed and are operational are green. Faulty or failed services are red.

Step 3 Scroll down the list and confirm that the following services are installed and running for your deployment:

- reverse-proxy
- router
- ui

Note whether the service is operational or faulty.

Step 4 Review the console **Tasks** tab below the list of services for any error messages about any faulty services. Note the reason given for the faulty or failed service.

Step 5 Contact Cisco support with the following information:

- Whether any of the services listed in **Step 3** are inoperable or faulty.
- Whether any errors are in the console **Tasks** tab located at the bottom of the console.

Troubleshooting the Configuration

Perform the following procedures to troubleshoot possible configuration issues.

Updating the Configuration Using the Wizard

You can troubleshoot the Cisco APIC-EM deployment by running the configuration wizard a second time and updating any earlier configuration entries.

Note You can rerun the configuration wizard and correct any settings that you have previously entered. The configuration wizard saves and displays your previous settings, so you do not have to reenter them.

Before You Begin

You have deployed Cisco APIC-EM using the procedures described in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Restart the configuration wizard using the following command.

```
$ config_wizard
```

Step 4 Review the current configuration values in the configuration wizard and click **next>>**, until you access the specific step where you wish to update your previous configuration entry.
For example, if you need to enter a new NTP server IP address, click **next >>** until you get to the **NTP SERVER SETTINGS** screen.

Step 5 Update the value that was previously entered in the configuration wizard and is currently displayed.
For example, you can update the NTP server settings by entering a new IP address.

Step 6 Click **next>>** until the last step of the configuration wizard process.

Step 7 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM deployment.

Resetting the Cisco APIC-EM

You can troubleshoot a Cisco APIC-EM deployment by resetting the controller back to configuration values that were originally set using the configuration wizard the first time. A reset of the controller is helpful, when the controller has gotten itself into an unstable state and other troubleshooting activities have not resolved the situation.

In a multi-host environment, you need to perform this procedure on only a single host. After performing this procedure on a single host, the other two hosts will be automatically reset.

Note The **reset_grapevine backup_restore** command also returns the configuration settings back to values that you configured when running the configuration wizard for the first time. Additionally, this command also retains task information, release information, update history, and backup information during a Grapevine reset. This retained information is needed for any future backup/restore process. Therefore, to return to the earlier configuration settings as well as preserve information for a future backup and restore, use this command.

Before You Begin

You have deployed the Cisco APIC-EM using the procedures described in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Navigate to the `bin` directory on the Grapevine root. The `bin` directory contains the grapevine scripts.

Step 4 Enter the **reset_grapevine** command at the prompt to run the reset grapevine script.

```
$ reset_grapevine
```

The **reset_grapevine** command returns the configuration settings back to values that you configured when running the configuration wizard for the first time. The configuration settings are saved to a .JSON file. This .JSON file is located at: `/etc/grapevine/controller-config.json`. The **reset_grapevine** command uses the data in the `controller-config.json` file to return to the earlier configuration settings, so do not delete this file. If you delete this file, you must run the configuration wizard again and reenter your configuration data.

You are then prompted to reenter your Grapevine password.

Step 5 Enter your Grapevine password a second time.

```
[sudo] password for grapevine:********
```

You are then prompted to delete all virtual disks The virtual disks are where the Cisco APIC-EM database resides. For example, data about devices that the controller discovered are saved on these virtual disks. If you enter yes (**y**), all of this data is deleted. If you enter no (**n**), then the new cluster will come up populated with your existing data once the reset procedure completes.

Step 6 Enter **n** to prevent the deletion all of the virtual disks.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete all VIRTUAL DISKS in your APIC-EM cluster? (y/n):n
```

You are then prompted to delete all Cisco APIC-EM authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

Step 7 Enter **n** to prevent the deletion of all authentication timeout policies, user password policies, and user accounts other than the primary administrator account.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete authentication timeout policies, user password policies,
and Cisco APIC-EM user accounts other than the primary administrator account? (y/n): n
```

You are then prompted to delete any imported certificates.

Step 8 Enter **n** to prevent the deletion of any imported certificates.

```
THIS IS A DESTRUCTIVE OPERATION
Do you want to delete the imported certificates? (y/n): n
```

The controller then resets itself with the configuration values that were originally set using the configuration wizard the first time. When the controller is finished resetting, you are presented with a command prompt from the controller.

Step 9 Using the Secure Shell (SSH) client, log out of the host.

Restoring the Controller to the Factory Default

In certain situations, you may want to restore the Cisco APIC-EM to its original factory default settings. For example, if your controller appliance is being replaced or simply has an undesirable configuration that needs to be completely removed. Under these circumstances, you can restore the controller to its factory defaults and then proceed to reconfigure it as a new controller.

This procedure describes how to a restore the factory defaults to the controller.

Caution This procedure shuts down both the Cisco APIC-EM and the host (physical or virtual) on which it resides. At the end of this procedure, you will need to access the host and restart it.

Before You Begin

You have already deployed the Cisco APIC-EM using the procedures described in this guide.

You have access to the Cisco APIC-EM using either a physical console or a Telnet connection.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

Step 4 Enter your Linux grapevine password a second time to start the reset process.

```
$ sudo password for grapevine *********
```

After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your desire to run the **reset_grapevine factory** command.

Step 5 Enter **Yes** to confirm that you want to run the **reset_grapevine factory** command.
The controller then performs the following tasks:

- Stops all running clients and services
- Stops and shuts down any Linux containers
- Deletes all cluster data
- Deletes all user data
- Deletes the configuration files including secrets and private keys
- Shuts down the controller
- Shuts down the host (physical or virtual)

What to Do Next

Perform the following tasks:

- Start up the host (physical or virtual).
- After start up, the configuration wizard appears and prompts you to re-deploy the Cisco APIC-EM.
- Proceed to re-deploy the Cisco APIC-EM using the configuration wizard.

Creating a Support File for the Cisco APIC-EM

You can troubleshoot the Cisco APIC-EM deployment by creating a support file. This support file consists of logs, configuration files, and command output. After you create this support file, you can then email it to Cisco support for assistance.

Before You Begin

You have deployed the Cisco APIC-EM using the procedures described in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Navigate to the `bin` directory on the host. The `bin` directory contains the grapevine scripts.

Step 4 To create the support file, enter the **rca** command in this directory.

```
$ rca
mkdir: created directory '/tmp grapevine-rca-2014-05-27_04-22-20-PM_PDT-0700'

----------------------------------------------------------------------
RCA package created On Tues May 27 16:22:20 PDT 2014
----------------------------------------------------------------------

[INFO] Generating log for 'vmstat 1 10'
[sudo] password for grapevine:
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains log files, configuration files, and the command output.

What to Do Next

Send the `tar` file created by this procedure to Cisco support for assistance in resolving your issue.

Troubleshooting Services

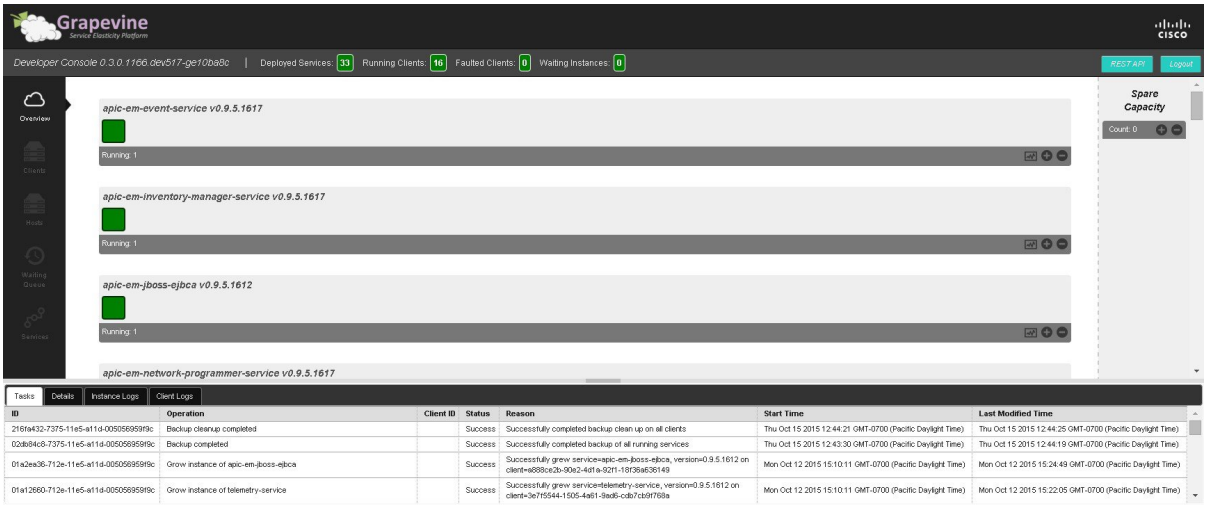
You can use the troubleshooting procedures in this section to assist in troubleshooting service issues.

You can use the Grapevine developer console to review the status of a service instance (active, inactive, or failed) to assist in identifying a service problem. You can also use the Grapevine developer console to check the service logs to identify any problems. After identifying a failed or faulty service, you can then manually grow and/or harvest service instances to try to resolve the problem.

Grapevine Developer Console

The Cisco APIC-EM creates a Platform as a Service (PaaS) environment for your network. A service in this PaaS environment is a horizontally scalable application that adds instances of itself when increasing loads occur on a client within the network. You use the Grapevine developer console to troubleshoot these services. The Grapevine developer console tools were bundled with the deployment files and installed when you first deployed the Cisco APIC-EM.

Figure 20: Grapevine Developer Console



Note For a multi-host cluster, you do not have to log into each host to view the Grapevine developer console. In a multi-host cluster, you get a single, consolidated view of all of the services running on all three hosts.

The Grapevine developer console provides the following windows and functionality:

- **Overview—**Provides a list of services with information about their version and status. You can add or remove services in this window.
- **Clients—**Provides detailed client information in this window.
- **Hosts—**Provides detailed host information in this window.
- **Waiting Queue—**Provides information about the waiting queue.
- **Services—**Provides detailed service information. You can add or remove services in this window.
- **Logs—**Provides detailed task, instance, and client logs

Note You cannot access the Grapevine developer console as a Linux root user. You can only access the Grapevine developer console using the administrator username and password that you configured during the deployment process.

Related Topics

Creating a Service Instance Manually
Removing a Service Instance Manually
Reviewing the Service Version, Status, and Logs, on page 101

Reviewing the Service Version, Status, and Logs

You are able to perform the following tasks using the Grapevine developer console:

- Review the status of each service
- Review the version of each service
- Review the logs of each service

Note Only advanced users should access the console to perform the tasks described in this procedure or attempt to troubleshoot the services.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

Step 1 Access the Grapevine developer console by opening a Google Chrome browser window and entering the IP address that you configured for the network adapter using the configuration wizard.
Note This IP address connects the appliance to the external network.

For example, enter the following IP address with required port number:

https://*external network IP address:***14141**

Step 2 Enter your administrative username and password when prompted.
The administrative username and password were configured by you using the configuration wizard.

The console for the Elastic Service Platform (Grapevine) appears.

Step 3 Review the status of each service listed in the **Overview** window in the console.
Each service is represented by a square. A green colored square represents an active instance of the service, and a red colored square represents a service with a faulty or failed instance. Squares without color represents inactive services (no instances initiated and running).

In a multi-host environment, a service may be represented by two green colored squares, indicating that the service is running on two different hosts within your cluster. Place your cursor over each square to view the host that the service is running on.

Step 4 Review the version of each service in the **Overview** window in the console.
The version is located in the header of each listed service.

Step 5 Review the service logs by clicking a specific active instance of a service (green square icon) and then viewing the **Instance** or **Client** logs located at the bottom of the window.

What to Do Next

When finished with the Grapevine developer console, click the **Logout** button to log out of the console.

Related Topics

About Cisco APIC-EM Services, on page 17
Services, on page 18
Grapevine Developer Console, on page 100

Monitoring Services and Clients Using the CLI

In addition to the developer console, a command-line interface on the host is also provided for troubleshooting purposes. This CLI allows you to monitor the health of the Cisco APIC-EM from the command line.

Before You Begin

You have deployed the Cisco APIC-EM using the procedures described in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Display all of the Cisco APIC-EM services currently installed by entering the **grape service display** command. Key data about each service is then displayed separated by hash marks.

```
$ grape service display

...

#
rabbitmq                  config                    {}
rabbitmq                  core_service              True
rabbitmq                  enabled                   False
rabbitmq                  endpoint_config           {u'default':
{u'backend_protocol': u'amqp', u'backend_path': u'',
u'frontend_protocol': u'', u'frontend_path': u'', u'frontend_port':
0, u'backend_port': 5672}}
rabbitmq                  kill_as_group             True
rabbitmq                  max_instances             1
rabbitmq                  min_instances             0
rabbitmq                  priority                  1
rabbitmq                  queue_config              {u'queues': [],
u'bindings': [], u'exchanges': []}
rabbitmq                  requirements              {u'template_id':
u'default', u'persistent_disk': False}
rabbitmq                  run_as_group              grapevine
```

```
rabbitmq                  run_as_user               grapevine
rabbitmq                  service_type              rabbitmq
rabbitmq                  spare_count               0
rabbitmq                  start_secs                10
rabbitmq                  static_load               10
rabbitmq                  status_interval           60
rabbitmq                  stop_as_group             True
rabbitmq                  stop_signal               TERM
rabbitmq                  version                   1.0.0
#

...
```

Step 4 Display running instances of the Cisco APIC-EM services by entering the **grape instance display** command. Key data about running instances of service is then displayed separated by hash marks.

```
$ grape instance display

...

#
4c4c83db-2da6-4a04-9af6-96c8dac692d1   client_id
4c4c83db-2da6-4a04-9af6-96c8dac692d1
4c4c83db-2da6-4a04-9af6-96c8dac692d1   endpoint_config
{u'default': {u'backend_port': 5672, u'backend_protocol': u'amqp'}}
4c4c83db-2da6-4a04-9af6-96c8dac692d1   interfaces
[{'interface': 'eth0', 'ip': '192.168.0.1', 'mac': '00:50:56:9f:6c:c4'},
{'interface': 'eth1', 'ip': '172.16.0.15', 'mac': '00:50:56:9f:71:46'}]
4c4c83db-2da6-4a04-9af6-96c8dac692d1   is_error           None
4c4c83db-2da6-4a04-9af6-96c8dac692d1   service_type       rabbitmq
4c4c83db-2da6-4a04-9af6-96c8dac692d1   state              running
4c4c83db-2da6-4a04-9af6-96c8dac692d1   task_id            None
4c4c83db-2da6-4a04-9af6-96c8dac692d1   timestamp
Fri Oct 03, 2014 02:05:43 PM (4 days ago)
4c4c83db-2da6-4a04-9af6-96c8dac692d1   version            1.0.0
#

...
```

Note All services should have a *state* property value of *running*.

Step 5 Display all Grapevine clients currently running in Cisco APIC-EM by entering the **grape client display** command. Key data about each client is then displayed separated by hash marks.

```
$ grape client display

CLIENT                                  PROPERTY             VALUE
------------------------------------------------------------------------
ae63a6c1-a946-4df7-a68d-33227eed8134   client_id        ae63a6c1-a946-4df7-a68d-33227eed8134
ae63a6c1-a946-4df7-a68d-33227eed8134   client_version   0.1.0.212.dev633-gf7e21de
ae63a6c1-a946-4df7-a68d-33227eed8134   interfaces       [{'interface': 'eth0', 'ip': '192.168.0.32',

'mac': '00:50:56:9f:3a:90'}]
ae63a6c1-a946-4df7-a68d-33227eed8134   is_alive         True
```

```
ae63a6c1-a946-4df7-a68d-33227eed8134   last_heartbeat   Wed Oct 08, 2014 10:22:50 AM (15 secs ago)
ae63a6c1-a946-4df7-a68d-33227eed8134   template_id      default
ae63a6c1-a946-4df7-a68d-33227eed8134   vm_id            ce0a634a-5475-4450-9dce-f3217d855ac4
#

...
```

All clients should have a *is alive* property of *True*.

Troubleshooting Passwords

Perform the following procedures to troubleshoot password issues.

Performing Password Recovery with an Existing Administrator

To perform password recovery for a user (administrator, installer or observer) where there exists at least one controller administrator (ROLE_ADMIN) user account, take the following steps:

1. Contact the existing administrator to set up a temporary password for the user that requires password recovery.

Note The administrator can set up a temporary password by deleting the user's account and then recreating it with the lost password. The user can then log back into the controller to regain access and change the password once again to whatever he or she desires.

2. The user then needs to log into the controller with the temporary password and change the password.

Note Passwords are changed in the controller GUI using the **Change Password** window. For information about changing passwords, see Chapter 4, Managing Users and Roles in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Performing Password Recovery with No Existing Administrator

The following procedure describes how to perform password recovery where there exists only one controller administrator (ROLE_ADMIN) user account and this account cannot be successfully logged into.

Note We recommend that you create at least two administrator accounts for your deployment. With two administrator accounts, if one account is locked for whatever reason then the other account can be used to unlock that locked account.

Step 1 If there are no other existing administrator (ROLE_ADMIN) user accounts, use an SSH client from your terminal to log into the host (physical or virtual) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 Enter the Linux username ('grapevine') and password when prompted.

Step 3 On the console, enter the following command on the Grapevine root.

```
$ config_wizard
```

This command starts up the Cisco APIC-EM configuration process.

Step 4 Choose the **<Advanced Install>** option.

Step 5 Proceed through the configuration process until reaching the step to configure the **APIC-EM ADMIN USER SETTINGS**.

Step 6 Specify a new administrator user password.

Step 7 Reenter the new administrator user password for confirmation.

Step 8 Proceed through the configuration wizard and its process until completion.

Caution To save the data in the Cisco APIC-EM database as part of the reset, ensure that **no** is chosen when prompted in **HARVEST ALL VIRTUAL DISKS**.

This final step will bring down the cluster and then bring it back up again (similar to running the **reset_grapvine** command).

Performing Password Recovery for the Linux Grapevine User Account

You can use the following procedure to recover from the loss of the Linux grapevine user password. This procedure reconfigures the Linux grapevine user password that is required for accessing the host's Linux operating system.

Before You Begin

You should be logged into the host (physical or virtual) using a Linux console to access the Linux kernel.

Step 1 Reboot the host (physical or virtual) while logged into the Linux console.

Step 2 Press "e" upon seeing the GNU GRUB menu to edit the boot commands.

Note In a VMware environment, you may need to press a different key to view the GNU GRUB menu. Refer to your VMware documentation for information about access to the GNU GRUB menu. Additionally, there may be different keys to press to enter the boot sequence depending upon the BIOS used for the host.

Step 3 Search for the line in the GNU GRUB menu output that begins with "linux" and change “ro” to “rw”, and append "init=/bin/bash" to that line.
For example, search for this line:

```
linux /vmlinuz-3.13.0-24-generic root=/dev/mapper/grapevine--vg-root ro cgroup_enable=memory
swapaccount=1 quiet sqlash $vt_handoff
```

And change it to this line:

```
linux /vmlinuz-3.13.0-24-generic root=/dev/mapper/grapevine--vg-root rw cgroup_enable=memory
swapaccount=1 quiet sqlash $vt_handoff init=/bin/bash
```

Step 4 Press **Ctrl-x** or the **F10** key to proceed with the boot process.
Note We recommend that you use the **F10** key to proceed with the boot process.

At this point, the host will boot up in root mode. You can now enter the Linux **passwd** command to reset the password for the Linux grapevine user.

Step 5 Enter the Linux **passwd** command to reset the password for the Linux grapevine user.

```
$  passwd grapevine
```

Caution This procedure permits you to change the Linux **grapevine** user password. Do not change the Linux **root** user password at any point in this procedure.

Step 6 When prompted, enter a new Linux grapevine password.

Step 7 When prompted, confirm the new Linux grapevine password by entering it a second time.

Step 8 Enter the following **reboot** command to reboot the system.

```
$ /sbin/reboot -f
```

The system reboots and will start up with new configuration and password.

At the end of the reboot process, you are presented with the GNU GRUB menu.

Step 9 Press **Enter** to boot up in the Ubuntu OS.

Step 10 After booting up in the Ubuntu OS, log back into the host by entering your Linux grapevine username and password.
Note Enter the Linux grapevine password created in step 6 above.

Step 11 Restart the configuration wizard using the following command.

```
$ config_wizard
```

Proceed through the configuration wizard process by clicking **next>>** and accepting the pre-configured values until you reach the **LINUX USER SETTINGS** step.

Step 12 When prompted to enter values for the **LINUX USER SETTINGS**, enter the new Linux grapevine password that you created earlier in step 6.
Note You need to start up the configuration wizard and run through the configuration process to synchronize the Linux grapevine user password to the controller itself.

Step 13 Click **next>>** and continue through the configuration wizard process, until the last step of this process.

Note When prompted to enter values for the **CONTROLLER CLEAN-UP** step, be sure to enter **no** for both **Harvest All Virtual Disks** and **Delete All Users**.

Step 14 At the end of the configuration wizard process, click **proceed>>** to have the configuration wizard save and apply your configuration changes to the Cisco APIC-EM.

Troubleshooting Commands

You can issue commands on both Grapevine root and clients to troubleshoot the Cisco APIC-EM.

Related Topics

Root Commands, on page 107
Client Commands, on page 109

Root Commands

The following table describes commands that you can issue on the Grapevine root to troubleshoot the Cisco APIC-EM.

Note Enter the **grape help** command on Grapevine root to view the available commands.

Table 6: Root Troubleshooting Commands

Root Command	Description
grape capacity_plugin display	Displays the current settings used by Grapevine.
grape client display	Displays the number of Grapevine clients that are currently running. This command also displays any clients that have faulted.
grape client status	Displays the status of the Grapevine clients.
grape host evacuate *host_id*	The **grape host evacuate** command harvests all of the services on the host where it is issued. If you issue this command on a host in a multi-host cluster, then the services are harvested and transferred to the remaining two hosts in the cluster. If you issue this command on a host in a single host configuration, all the services are harvested.
grape host status *host_id*	The **grape host status** command displays all of the services on the host where it is issued.

Root Command	Description
grape instance display	Displays the Cisco APIC-EM services that are currently running.
grape instance status	Displays the status of the Cisco APIC-EM services.
grape network display	Displays the current external network configuration used by both Grapevine and the Cisco APIC-EM including: • IP addresses • Netmask • DNS servers
grape release display current	Displays the versions of the Cisco APIC-EM services that are currently running.
grape release display latest	Displays the latest available versions of the Cisco APIC-EM services.
grape release update force	Updates a service for Cisco APIC-EM. Use this command to force a service update.
grape root display	Displays the Grapevine root properties, including: hostname, interfaces, root ID, and version.
grape service display	Displays the Cisco APIC-EM services that are currently installed.
grape update_service display	Displays the current automatic services update configuration. Additional fields in the command output indicate the last time the Cisco cloud was polled for updates (`last_connect_time`), as well as the Cisco cloud status(`last_connect_status`). For example, whether the Cisco cloud is reachable, unreachable, etc.
grape version	Displays the version of Grapevine that the Grapevine root is running.
rca	The **rca** command runs a root cause analysis script that creates a tar file that contains log files, configuration files, and the command output. After running this command and creating the tar file, you can send the file to Cisco support for assistance in resolving an issue.

Root Command	Description
reset_grapevine	The **reset_grapevine** command returns the configuration settings back to values that you configured when running the configuration wizard for the first time. The configuration settings are saved to a .JSON file. This .JSON file is located at: `$ /etc/grapevine/controller-config.json`.
reset_grapevine backup_restore	The **reset_grapevine backup_restore** command returns the configuration settings back to values that you configured when running the configuration wizard for the first time. The configuration settings are saved to a .JSON file. This .JSON file is located at: `$ /etc/grapevine/controller-config.json`. Additionally, this command also retains task information, release information, update history, and backup information during a Grapevine reset. This retained information is needed for any future backup/restore process.
reset_grapevine factory	The **reset_grapevine factory** command returns the configuration settings back to their factory defaults. **Caution** This command shuts down both Cisco APIC-EM and the host (physical or virtual) where the controller resides. After running this command, you will need to access the host and reboot it.
reset_grapevine local	The **reset_grapevine local** command returns the configuration settings on the local host where it is run back to values that you configured when running the configuration wizard for the first time. This command removes the local host from the multi-host cluster.
securityutil openport	Displays the open ports on the Grapevine root and clients. An open port is any TCP or UDP port, for which a listener exists on one or more IP addresses.
sudo service grapevine status	Determines the status of the Grapevine root core services and whether all of the root core services are running.

Related Topics

Troubleshooting Commands, on page 107

Client Commands

The following table describes commands that you can issue on the Grapevine client to troubleshoot the Cisco APIC-EM.

Table 7: Client Troubleshooting Commands

Client Command	Description
grape version	Displays the version of Grapevine that the Grapevine client is running.
sudo service grapevine status	Determines the status of the Grapevine client core services and whether all of the client core services are running.

Related Topics

Troubleshooting Commands, on page 107

Troubleshooting Log Files

You can use log files to troubleshoot the Cisco APIC-EM. Log files are stored on both the Grapevine root and clients.

Note Logging files are persistent across any system failures and software updates for change management.

Related Topics

Root Log Files, on page 110
Client Log Files, on page 112

Root Log Files

The following table lists log files located on the Grapevine root that can be used to troubleshoot the Cisco APIC-EM.

Table 8: Root Log Files

Directory	Filename	Description
/var/log/	boot.log	This log file provides you with the details of the boot process and any errors that may occur during this process. Use this log file to troubleshoot any of the following problems: • Why did the Grapevine client fail to communicate with the Grapevine root? • Why did the Grapevine client fail to upgrade?
/var/log/	config_wizard.log	Use this log file to determine if there were any errors during the initial Grapevine configuration and deployment.
/var/log/	grapevine_manager.log	Use this log file to determine if there were any errors during a manual file update using the **Update Settings** fields in the controller's UI.
/var/log/grapevine	supervisord.log	Use this log file to determine whether any of the Grapevine root core services unexpectedly expired.
/var/log/grapevine	cassandra.log	Use this log file to determine whether the Grapevine database is healthy.
/var/log/grapevine	grapevine_root.log	Use this log file to troubleshoot any of the following problems: • Why did Grapevine fail to grow or harvest a service instance? • Why did an automatic service update fail? • Why did Grapevine fail to communicate with a Grapevine client?

Directory	Filename	Description
/var/log/grapevine	grapevine_capacity_manager.log	Use this log file to determine why Grapevine failed to grow or harvest a Grapevine client.

Related Topics

Troubleshooting Log Files, on page 110

Client Log Files

The following table lists log files located on the Grapevine client that can be used to troubleshoot the Cisco APIC-EM.

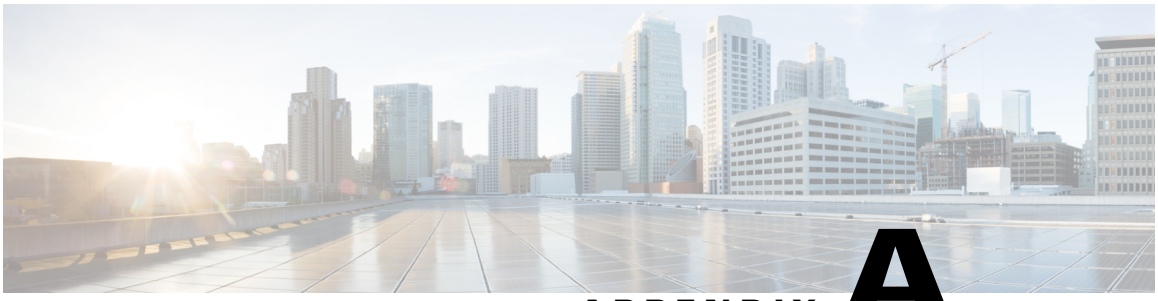
Table 9: Client Log Files

Directory	Filename	Description
/var/log	boot.log	Use this log file to determine the following: • Why did this Grapevine client fail to communicate with the root? • Why did this Grapevine client fail to upgrade?
/var/log/grapevine	supervisord.log	Use this log file to determine if any of the Grapevine client core services unexpectedly died?
/var/log/grapevine	grapevine_client.log	This log file provides you with the details of the Grapevine client daemon bootstrap process and any errors that may occur during this process. Use this log file to determine the following: • Why did this Grapevine client fail to grow or harvest a service instance? • Why did this Grapevine client fail to communicate to the Grapevine root?

Directory	Filename	Description
/var/log/grapevine/services	service-name/version/service-name.log	Use this log file to determine why did a service fail to perform some operation?

Related Topics

Troubleshooting Log Files, on page 110



APPENDIX A

Cisco APIC-EM Multi-Host Support

Multi-Host Support

A host is defined as an appliance, host or virtual machine with Linux containers running instances of the Grapevine clients. The Grapevine root itself runs directly on the host's operating system and not in the Linux containers. You can set up either a single host or multi-host deployment. A multi-host deployment with three hosts is best practice for both high availability and scale. Each Grapevine root in a multi-host configuration maintains an Active/Active status with the other Grapevine roots and is therefore able to coordinate with the other Grapevine roots the overall management of the cluster.

Note Active/Active is defined as all Grapevine roots being operational and active.

Each host must be running the same controller software in the multi-host configuration. You are able to mix and match physical and virtual appliances in the multi-host configuration.

The multi-host configuration has the following requirements and features:

- Each host requires a minimum of 32GB of memory.
- This multi-host cluster is able to tolerate the loss of one of the hosts and supports a single fail-over.

Note If the second host fails, the remaining host in the cluster will still be active and operable, but will exist in an unstable state. In the event of the loss of one of the hosts, we recommend that you remove this host from the cluster using the configuration wizard and then either repair and rejoin this host to the cluster or join a new host to the cluster.

- As each host is configured with 32GB of memory, if a host failure occurs then the remaining hosts would have a total 64GB of memory which is sufficient to run the controller.
- All three hosts must reside in the same subnet.

Clustering and Database Replication

The clustering feature of the Cisco APIC-EM provides a mechanism for distributing processing and database replication among multiple hosts that run the exact same version of the controller. Clustering provides a sharing of resources and features and enables system high availability and scalability.

Security Replication

In a multi-host environment, the security features of a single host are replicated among the other two hosts, including any X.509 certificates or trustpools. Once you join a host to another host or to a cluster, the Cisco APIC-EM credentials are shared and become the same as that of the host you are joining or the pre-existing cluster. The Cisco APIC-EM credentials are cluster-wide (across hosts) and not per-host.

Note We strongly suggest that any multi-host cluster that you set up be located within a secure network environment. For this release, privacy is not enabled for all of the communications between the hosts.

Service Redundancy

The Cisco APIC-EM provides high availability (HA) support using service redundancy. A Cisco APIC-EM cluster can be set up across multiple Linux containers within multiple hosts. On each host, the Grapevine root is an application running on the host and the Grapevine clients are created and reside in the containers. Both the Cisco APIC-EM services and database are then instantiated across the clients within the Linux containers:

- Cisco APIC-EM Services:
  - For service high availability, if a service fails then Grapevine (the Elastics Service Platform) spins up a new instance to replace it. If Grapevine is unable to spin up the new instance on the same container after a sole instance fails, then it spins up a new container and then spins up the new instance on this container.
  - Cisco APIC-EM supports a replacement service instance model. For example, assume that one of the roots on a single host spins up an instance. If that host and its root goes down, then another host on another root spins up an instance to ensure continuity of that service.
- Cisco APIC-EM Database:
  - The Cisco APIC-EM services use a PostgreSQL database management system. PostgreSQL has a built-in master-slave model for synchronizing data across replicated databases to respond to any failover situation.
  - The master and slave postgres instances are grown across different Linux containers and across different hosts. The data of these postgresSql instances are synchronized using PostgresSQL's built-in data streaming replication mechanism. With three hosts, there is one master (with a master postgres instances) and two slaves (each with a slave postgres instance).
  - If the master fails, then the slave seamlessly takes over.

- In the event of a failure by the master, an election process occurs among the remaining hosts to determine which becomes the new master. This election process can also be triggered by resetting the controller using the CLI or rebooting the host.

If the Cisco APIC-EM (roots and clients) are all deployed on a single host, then there is no HA support for any hardware failure (physical or virtual appliance failure, power cycle that shuts down the appliance, etc.). To protect against any hardware failure, you need to deploy the Cisco APIC-EM on a cluster with multiple hosts.

Multi-Host Synchronization

Whenever there is a configuration change on one of the hosts, Grapevine synchronizes the change with the other two hosts. The supported types of synchronization include:

- Database—Synchronization includes any database updates related to the configuration, performance, and monitoring data.
- File—Synchronization includes any changes to the configuration files.

Multi-Host Monitor Process

Grapevine is the main component that manages HA operations in a cluster. To ensure proper cluster HA operation, Grapevine uses both health checks and heart beats.

Health checks are used to monitor processes that are low performing and not running properly. Services that run on Grapevine have health checks that are periodically invoked. If there is any indication of an unhealthy service, Grapevine will harvest and regrow that service.

In addition to the health checks, Grapevine also uses heart beats between the services, clients, and roots to monitor the status of the cluster. Grapevine monitors these heart beats for any processes that may have failed. If there is no heart beat, then this indicates that a process has failed and to correct for this situation, Grapevine regrows the service.

Grapevine also uses a heart beat to monitor for adequate memory and storage capability for the cluster. If a heart beat indicates that the cluster's memory or storage fails below an appropriate level necessary for successful operations, then Grapevine will not grow any new services.

Split Brain and Network Partition

Split brain refers to a state in which each host does not know the HA role of its peers, and cannot determine which host currently has the primary HA role. In split brain mode, data modifications may have been made by either host, and those changes may not be replicated to the peer. Also, neither or none of the hosts may be functioning in the primary HA role.

The Cisco APIC-EM cluster uses a private network connection, where each host monitors each the other's health and status. Split brain mode occurs when there is a temporary failure of the network connections between the hosts, for example, due to one of the following occurrences:

- Physical disconnection of the network connection from a host.
- Loss of power to one or both hosts.

- Host appliance failure

INDEX

U