Overview

About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's Software Defined Networking (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	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.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP application is one of the components in the Cisco Network PnP solution. The Cisco Network PnP solution 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. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links.
Cisco Active Advisor	The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on: • End-of-life milestones for hardware and software • Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices • Warranty and service contract status
Cisco SD-Bonjour	The Cisco SD-Bonjour application provides controller functions in the network. It enables discovery and distribution of policy-based Cisco SD-Bonjour services, independent of network boundaries.
Cisco Integrity Verification	The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release.

Feature	Description
Cisco Remote Troubleshooter	The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel. As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management.
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.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

Cisco APIC-EM Components and Architecture

The Cisco APIC-EM consists of the components and architecture discussed in this section. To better troubleshoot any issues with the Cisco APIC-EM, you should review the topics in this section.

Appliances

The Cisco APIC-EM can be deployed on either a physical or virtual appliance.

- For physical appliance support, the Cisco APIC-EM can be installed on the following Cisco UCS servers:
    - Cisco APIC-EM has been tested and qualified to run on these servers.
        - Cisco UCS C220 M4S Server

    - ◦ Cisco UCS C220 M3S Server
    - ◦ Cisco UCS C22 M3S Server

  - ◦ Any Cisco UCS server that meets the minimum system requirements as listed in the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.
  - ◦ A physical appliance can also be a *dedicated* Cisco UCS server. The following two physical appliances are currently available:
    - ◦ Cisco APIC-EM Controller Appliance 10C-64G-2T (APIC-EM-APL-R-K9)
    - ◦ Cisco APIC-EM Controller Appliance 20C-128G-4T (APIC-EM-APL-G-K9)

Note Contact Cisco support for additional information about the above appliances and for ordering information.

- For virtual appliance support, the Cisco APIC-EM can also be installed and deployed in a virtual machine that meets the minimum system requirements on VMware vSphere. For information about these requirements, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*

Hosts

You can set up either a single host or multi-host deployment for your network. A host is defined as an appliance, physical server, or virtual machine running instances of the Grapevine clients. The Grapevine root itself runs directly on the host's operating system. 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 For additional information about a multi-host deployment, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

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.

Root and Clients

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

For a list of the supported services for this release, see the About Cisco APIC-EM Services.

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.

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.

For a list of the supported services for this release, see the About Cisco APIC-EM Services.

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.

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.

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.