Application Hosting on the Cisco Catalyst 9000 Series Switches

Introduction

Applications are used in enterprise networks for a variety of business-relevant use cases. Examples of enterprise applications include administrative tools such as protocol analyzers and security toolsets such as intrusion detection services. Traditionally, such applications would operate on an external physical or cloud-based virtual server.

Enterprise networks are now dealing with massive volumes of data, and there is a critical need to collect and analyze this data to respond faster and deliver insightful context. Traditional approaches, in which data is processed in remote servers, will no longer work. Data can burden the network unless some context is known. Edge computing can greatly reduce the data sent to the cloud or a remote server. Collecting and analyzing the data at the edge and making decisions locally rather than in centralized servers significantly reduces the latency and bandwidth of the network.

Powered by an x86 CPU, the application hosting solution on the Cisco® Catalyst® 9000 series switches provide the intelligence required at the edge. This gives administrators a platform for leveraging their own tools and utilities, such as a security agent, Internet of Things (IoT) sensor, and traffic monitoring agent.

Hardware resources for applications

To support application hosting capabilities on the Cisco Catalyst 9000 series switches, the switch provides hardware resources where applications can reside and execute. Cisco IOS XE running on the Cisco Catalyst 9000 series switches reserves dedicated memory and CPU resources for application hosting to provide a separate execution space for user applications without compromising the integrity and performance of the switch.

Moreover, applications must reside in one of the external Solid State Drive (SSD) storage options (USB 3.0 or M2 SATA), depending on the specific Cisco Catalyst 9000 platforms. Applications have no access to the internal device flash storage, which is reserved for Cisco IOS XE to protect its integrity.

Table 1 shows the available hardware resources for applications.

Note: Internal flash and front panel USB ports are not supported for application hosting purpose.

Table 1. Cisco Catalyst 9000 platforms' hardware resources for applications

Resource type	Cisco Catalyst 9300 Series	Cisco Catalyst 9400 Series	Cisco Catalyst 9500 Series	Cisco Catalyst 9500 Series High Performance	Cisco Catalyst 9600 Series
Memory(RAM)	2 GB	Up to 8 GB	Up to 8 GB	Up to 8 GB	Up to 8 GB
CPU	25% of total CPU	25% of total CPU	25% of total CPU	25% of total CPU	25% of total CPU
Storage	120 GB (USB 3.0 SSD)	240 to 960 GB (SATA)	120 GB (USB 3.0 SSD)	240 to 960 GB (SATA)	240 to 960 GB (SATA)

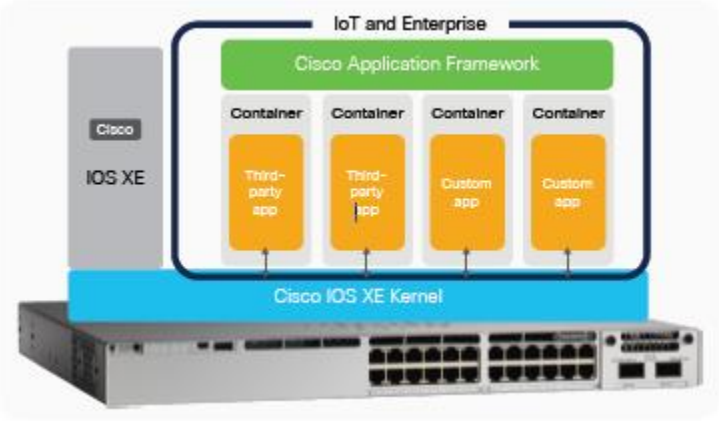
With Cisco IOS XE 16.12.1 release, application hosting capabilities are supported only on Catalyst 9300 series switches. The rest of the Catalyst 9000 platforms are on roadmap.

Note: The Cisco Catalyst 9200 Series do not support application hosting.

Hardware resource isolation and storage security

Application hosting on Cisco Catalyst 9000 family switches opens up new opportunities for innovation by converging network connectivity with a distributed application runtime environment, including hosting applications developed by partners and developers. For maximum flexibility and total isolation from the main operating system, the Cisco IOS XE kernel and Cisco Application Framework on the Cisco Catalyst 9000 series switches support containerized application by leveraging control groups (Cgroups) and user namespace.

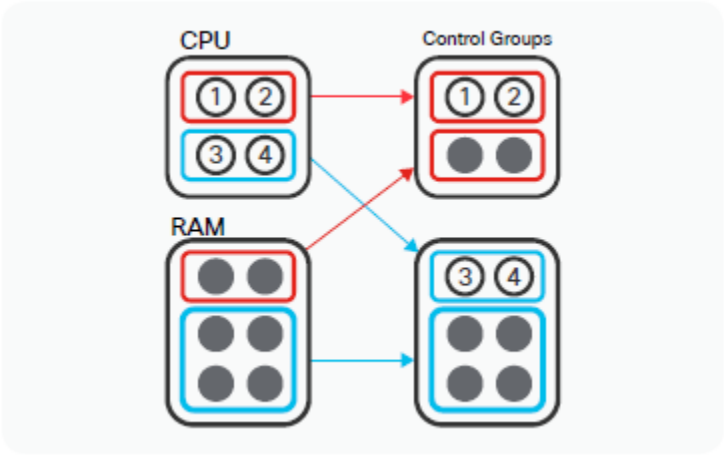
Figure 1. Cisco Application Framework on the Cisco Catalyst 9000 platform



Cgroups limit access to physical resources such as CPU and memory for applications, as shown in Figure 2. The Cisco Application Framework checks that there are sufficient resources to activate

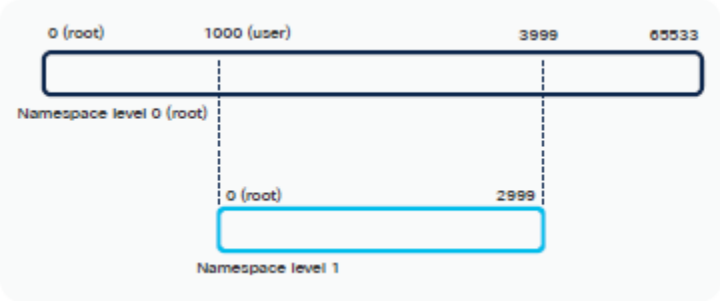
and install the application. If not enough resources are available for the application, then it will not be able to activate, and relevant messages will be given to the administrator.

Figure 2. Control groups



In addition to Cgroups, the user namespace feature provides additional isolation and security. This feature separates the user IDs and group IDs between the host operating system and containers, as shown in Figure 3. A privileged **user (root)** in the containers can't be mapped to a privileged **user (root)** on the host operating system.

Figure 3. User namespace



Moreover, SSD storage offers best-in-class security by providing AES-256 hardware encryption on SSD storage and passcode authentication on both SSD storage and the switch.

The AES-256 encryption is completely done in hardware. When using passcode authentication, the passcode has to set on both the SSD and the switch. When a SSD with passcode authentication pre-configured is inserted to the Catalyst 9000 switch that does not have the matching passcode configuration, then the authentication will be failed because the switch does not have the correct passcode configured. The passcode must match on both the SSD storage and on the switch for successful deauthentication as show on Figure 4.

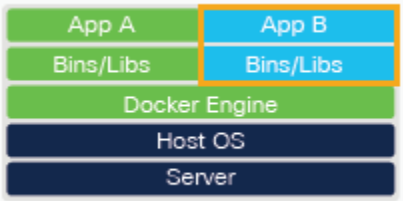
If the passcode configured SSD storage is removed from the Catalyst 9000 series switches and inserted into a non-Catalyst switch then the contents will be secured and not accessible. Any sensitive data is only accessible once unlocked in a Catalyst switch with the correct passcode.

Figure 4. Passcode authentication on SSD storage

Docker container

A Docker container is a lightweight, executable package of software that includes everything needed to run an application: code, dependencies, runtime, system libraries and system tools. Developers can easily create, deploy and move the applications across Docker hosts.

Figure 5. Docker container



Cisco IOS XE 16.12.1 introduces native Docker container support on Catalyst 9000 series switches. This enables users to build and bring their own applications without additional packaging. Developers don't have to reinvent the wheel by rewriting the applications every time there is an infrastructure change. Once packaged within Docker, the applications will work within any infrastructure that supports docker containers. Docker containers are lightweight and use very little CPU and memory overhead.

Once developers have built the docker application, running the standard "docker save" command can be used to export the application as ".tar" compressed file. The application can then be deployed on the Catalyst 9000 series switches. Cisco's ioxclient tool is no longer required to package the application. Ioxclient is an optional tool for developers who want to define additional parameters for the application.

Application developers can find more information about application hosting on the Cisco DevNet site at https://developer.cisco.com/app-hosting/ .Developer can also try the DevNet Sandbox to create a custom docker container in the developer environment and use the Catalyst 9000 switch to host the newly created application.

The DevNet Ecosystem also indicates the partners that have validated their applications for compatibility with Catalyst 9000 series switches. Cisco does not provide support for any third party or open-source applications, unless specifically called out.

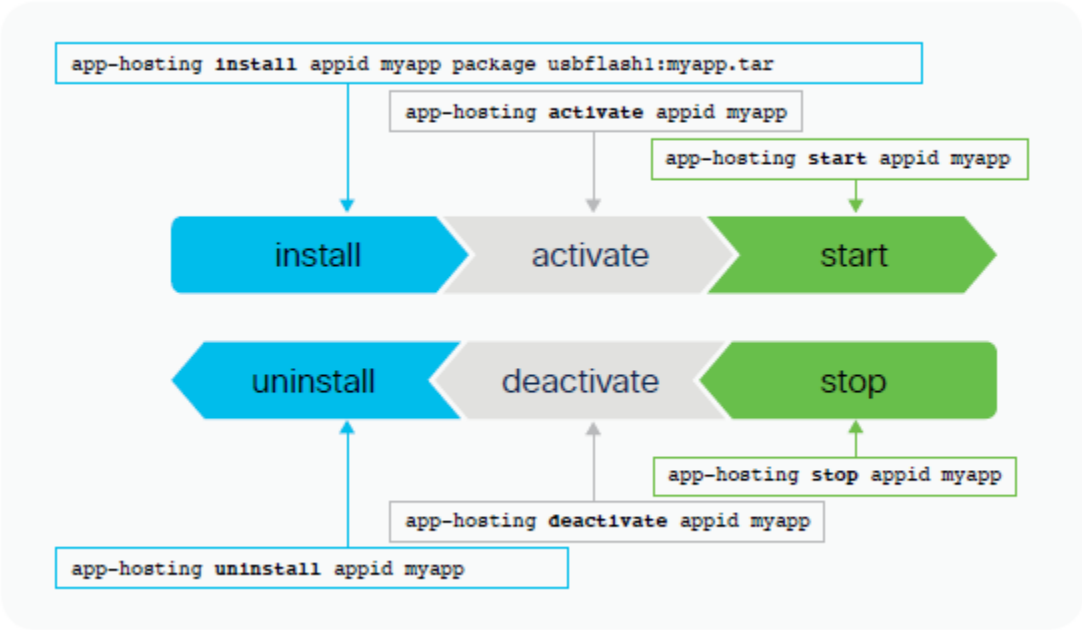
Application lifecycle management

The application lifecycle on the Cisco Catalyst 9000 series switches consists of three stages (Figure 6):

1. Install: Installing application on the device. Resources needed by the application are not yet committed to it.
2. Activate: Committing the HW resources required by the application.
3. Start: Putting the application is now running state.

Note: A Cisco DNA Advantage license is required for application hosting on the Cisco Catalyst 9000 series switches.

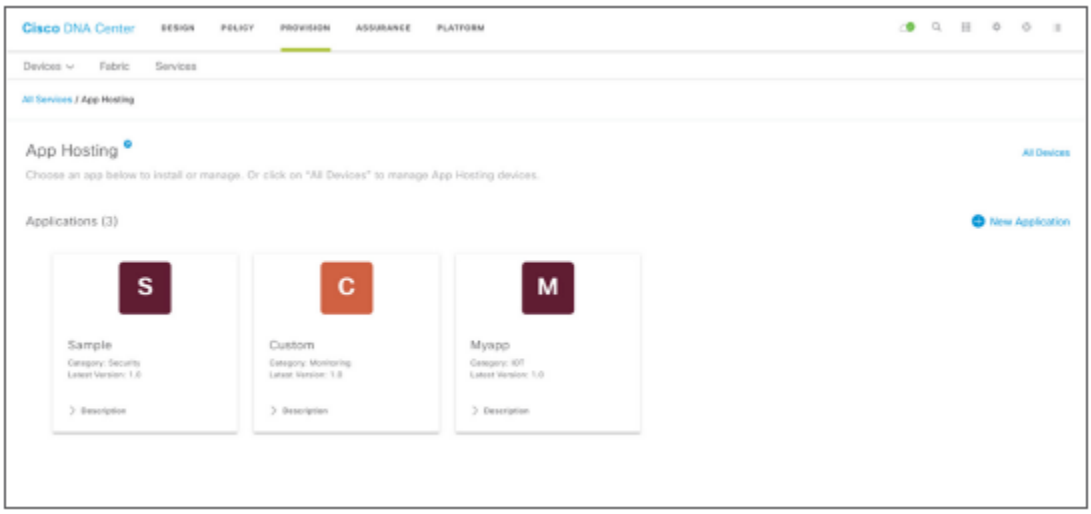
Figure 6. Application lifecycle management



Hosted applications can be managed through the command-line interface (CLI) until Cisco IOS XE 16.11.1 is released. Starting Cisco IOS XE 16.12.1 and an upcoming Cisco DNA Center release, Cisco will provide a centralized user interface to deploy and manage the entire lifecycle of the applications, in addition to the CLI management.

Cisco DNA Center provides consistent workflows to manage multiple Catalyst 9000 series switches through the “App Hosting” dashboard (Figure 7).

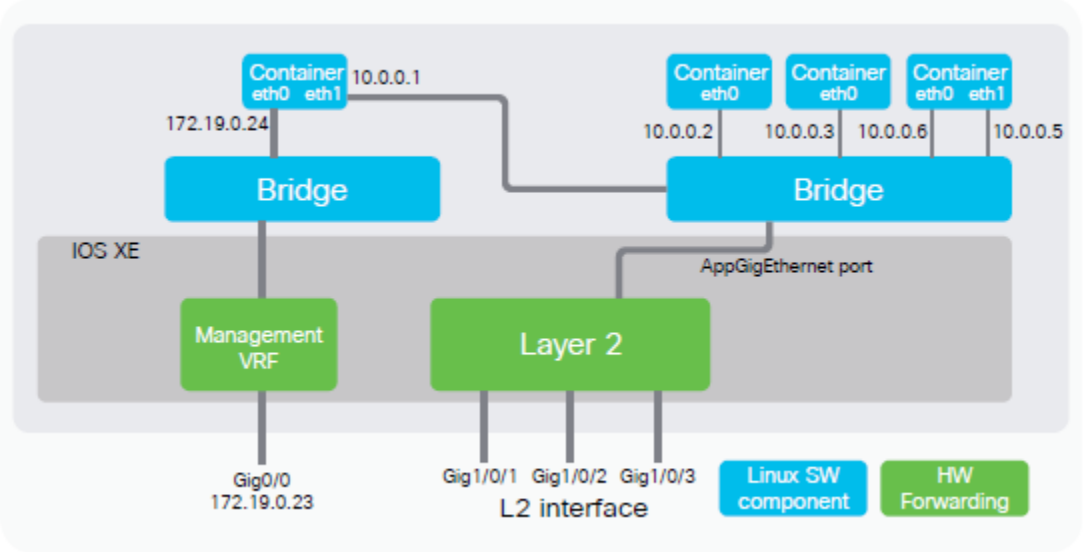
Figure 7. Cisco DNA Center App Hosting dashboard



Container networking

Containers can be connected via the management interface and front panel data ports (Figure 8) . The management interface connects to the container interface via the management bridge, and the IP address of the container will be on the same subnet as the management interface. Virtual network interface cards (vNICs) inside containers are seen as standard Ethernet interfaces (“eth0,eth1, etc.”).

Figure 8. Container network diagram



A new AppGigabitEthernet interface was introduced on Cisco Catalyst 9300 Series Switches with Cisco IOS XE Release 16.11.1. It is an internal hardware data port that is hardware-switched to the front panel data ports. The AppGigabitEthernet interface can be configured as a trunk or VLAN specific interface. For a trunk interface, it is extended to work as a Layer 2 trunk port, and all traffic

received by the port is available to the application. For a VLAN interface, the application is connected to a specific VLAN network by specifying the VLAN ID number.

The “AppGigabitEthernet” interface is only available on the Cisco Catalyst 9300 series switches and other Cisco Catalyst 9000 platforms are expected to be supported in future software releases.

Three options are available for assigning an IP address to the container:

4. Linux CLI: Logging directly into the container and configuring it using Linux commands.
5. Dynamic Host Configuration Protocol (DHCP): Using the DHCP client in the container and configuring a DHCP server or relay.
6. Cisco IOS XE CLI : Statically assigned via the Cisco IOS XE CLI.

The Cisco DNA Center workflow supports both the DHCP and static options.

Conclusion

Customers can now reduce their TCO and also eliminate the need to procure new hardware in order to monitor their networks. Key business outcomes are now made possible with the help of application hosting on the Cisco Catalyst 9000 switching platforms. A network operator in a large enterprise can host a network monitoring application on the Cisco Catalyst access platforms to know clearly where in the network the issues are and take action accordingly, due to the real-time insights being received. With Cisco DNA Center, all of this can be done remotely without having to send someone to multiple sites for troubleshooting or spending hours using the CLI. As the business needs grow, manual provisioning of the network will not scale. With a simple click of a button, network operators can now accommodate the growth of the organization and drive business agility.

C87-742415-00 06/19