Overview

- Cisco ACI Fabric Overview, page 1
- Cisco AVS Overview, page 2
- About the Cisco AVS and the VMware vCenter, page 4
- Required Software, page 5

Cisco ACI Fabric Overview

The Cisco Application Centric Infrastructure (ACI) includes Cisco Nexus 9000 Series switches with the Application Policy Infrastructure Controller (APIC) to run in the leaf/spine ACI fabric mode. These switches form a "fat-tree" network by connecting each leaf node to each spine node; all other devices connect to the leaf nodes. The APIC manages the ACI fabric. The recommended minimum configuration for the APIC is a cluster of three replicated hosts. The APIC fabric management functions do not operate in the data path of the fabric. The following figure shows an overview of the leaf/spin ACI fabric.

Figure 1: ACI Fabric Overview

The ACI fabric provides consistent low-latency forwarding across high-bandwidth links (40 Gbps, with a 100-Gbps future capability). Traffic with the source and destination on the same leaf switch is handled locally, and all other traffic travels from the ingress leaf to the egress leaf through a spine switch. Although this architecture appears as two hops from a physical perspective, it is actually a single Layer 3 hop because the fabric operates as a single Layer 3 switch.

The ACI fabric object-oriented operating system (OS) runs on each Cisco Nexus 9000 Series node. It enables programming of objects for each configurable element of the system.
The ACI fabric OS renders policies from the APIC into a concrete model that runs in the physical infrastructure. The concrete model is analogous to compiled software; it is the form of the model that the switch operating system can execute. The figure below shows the relationship of the logical model to the concrete model and the switch OS.

**Figure 2: Logical Model Rendered into a Concrete Model**

All the switch nodes contain a complete copy of the concrete model. When an administrator creates a policy in the APIC that represents a configuration, the APIC updates the logical model. The APIC then performs the intermediate step of creating a fully elaborated policy that it pushes into all the switch nodes where the concrete model is updated.

**Note**

The Cisco Nexus 9000 Series switches can only execute the concrete model. Each switch has a copy of the concrete model. If the APIC goes off line, the fabric keeps functioning but modifications to the fabric policies are not possible.

The Cisco Nexus 9000 Series switches offer modular and fixed 1-, 10-, and 40-Gigabit Ethernet switch configurations that operate in either Cisco NX-OS stand-alone mode for compatibility and consistency with the current Cisco Nexus switches or in ACI mode to take full advantage of the APIC's application policy-driven services and infrastructure automation features.

**Cisco AVS Overview**

The Cisco Application Virtual Switch (AVS) is a key part of the Cisco Application Centric Infrastructure (ACI). It is a distributed virtual switch that offers different forwarding and encapsulation options and extends across many virtualized hosts and data centers defined by the VMware vCenter Server.

The Cisco AVS is integrated with the Cisco ACI architecture as a virtual leaf and is managed by the Cisco APIC. The Cisco AVS implements the OpFlex protocol for control plane communication.

This section provides an overview of the Cisco AVS.

The Cisco AVS supports two modes of traffic forwarding: Local Switching mode, formerly known as Fex disable mode; and No Local Switching mode, formerly known as Fex enable mode. You choose the forwarding mode during Cisco AVS installation.
Local Switching Mode

In Local Switching mode, all intra-EPG traffic is locally forwarded by the Cisco AVS, without the involvement of the leaf. All inter-EPG traffic is forwarded through the leaf. In this mode, the Cisco AVS can use either VLAN or VXLAN encapsulation for forwarding traffic to the leaf and back. You choose the encapsulation type during Cisco AVS installation.

If you choose VLAN encapsulation, a range of VLANs must be available for use by the Cisco AVS. These VLANs have local scope in that they have significance only within the Layer 2 network between the Cisco AVS and the leaf. If you choose VXLAN encapsulation, only the infra-VLAN needs to be available between the Cisco AVS and the leaf. This results in a simplified configuration and is the recommended encapsulation type if there are one or more switches between the Cisco AVS and the physical leaf.

Figure 3: The Cisco AVS in Local Switching Mode
No Local Switching Mode

In No Local Switching mode, all traffic is forwarded by the leaf. In this mode, VXLAN is the only allowed encapsulation type.

Figure 4: The Cisco AVS in No Local Switching Mode

About the Cisco AVS and the VMware vCenter

The Cisco Application Virtual Switch (AVS) is a distributed virtual switch that extends across many virtualized hosts. It manages a data center defined by the vCenter Server.

The Cisco AVS is compatible with any upstream physical access layer switch that complies with the Ethernet standard, including Cisco Nexus switches. The Cisco AVS is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL).

The Cisco AVS is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. This solution allows the network administrator to configure virtual switch and port groups in order to establish a consistent data center network policy.
The following figure shows a topology that includes the Cisco AVS with the Cisco Application Policy Infrastructure Controller (APIC) and VMware vCenter.

**Figure 5: Sample Cisco AVS Topology**

---

### Required Software

The following table shows the versions of software you need to install for Cisco Application Virtual Switch (AVS) to work with the Cisco Application Policy Infrastructure Controller (APIC), VMware vCenter, and VMware ESXi hypervisor:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AVS software</td>
<td>Cisco AVS is supported in Release 4.2(1)SV2(2.3) and later releases. However, Release 5.2(1)SV3(1.5) or later is required if you want to use Distributed Firewall and Microsegmentation with Cisco AVS.</td>
</tr>
<tr>
<td>Cisco APIC</td>
<td>See the Cisco AVS Release Notes for compatibility information. However, version 1.1(1j) or later is required with Cisco AVS 5.2(1)SV3(1.5) or later if you want to use Distributed Firewall and Microsegmentation with Cisco AVS.</td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>Cisco AVS is compatible with release 5.1, 5.5, or 6.0 of VMware vCenter Server.</td>
</tr>
<tr>
<td>VMware vSphere bare metal</td>
<td>Cisco AVS is supported as a vLeaf for the Cisco APIC with release 5.1 and later releases of the VMware ESXi hypervisor.</td>
</tr>
</tbody>
</table>

**Note**

When you choose a Cisco AVS VIB, you need to choose the one compatible with the version of VMware ESXi hypervisor that you use. ESXi 5.1 uses xxix.3.1.1.vib, ESXi 5.5 uses xxix.3.2.1.vib, and ESXi 6.0 uses xxxx.6.0.1.vib.
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Virtual Switch Update Manager (VSUM)</td>
<td>Cisco AVS is supported in VSUM Release 1.0 and later releases.</td>
</tr>
</tbody>
</table>