Layer 4 to Layer 7 Services

Layer 4 to Layer 7 Services

Cisco Application Centric Infrastructure (ACI) treats services as a key part of an application. Any services that are required are treated as a service graph that is instantiated on the Cisco ACI fabric from the Cisco Application Policy Infrastructure Controller (APIC). You define the service for the application, while service graphs identify the set of network or service functions that the application requires.

Beginning with Cisco ACI Virtual Edge Release 1.2(1), Layer 4 to Layer 7 service graphs are supported for Cisco ACI Virtual Edge.

Beginning with the Cisco ACI Virtual Edge Release 2.2(1), support for Layer 4 to Layer 7 service graphs is extended to Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod.

For information about configuring Layer 4 to Layer 7 services on Cisco ACI Virtual Edge, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*. However, you first must follow the guidelines and understand the limitations in the next section of this chapter.

When you follow instructions in the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*, instead of configuring services on the VMware Distributed Virtual Switch (DVS) VMM domain, configure the services on the Cisco ACI Virtual Edge VMM domain with **AVE** as the switching mode.

Guidelines and Limitations for Layer 4 to Layer 7 Configuration

Follow the guidelines and note the limitations in this section when preparing to configure Layer 4 to Layer 7 service graphs for Cisco Application Centric Infrastructure (ACI) Virtual Edge.

Note The guidelines and limitations differ for Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod (vPod) and when it is not part of Cisco ACI vPod.

Guidelines and Limitations When Cisco ACI Virtual Edge Is Not Part of Cisco ACI vPod

Follow the guidelines in this section when preparing to configure Layer 4 to Layer 7 service graphs for Cisco Application Centric Infrastructure (ACI) Virtual Edge when it is not part of Cisco ACI Virtual Pod (vPod).

Note For information about Layer 4 to Layer 7 guidelines and limitations for Cisco ACI Virtual Edge when it is part of Cisco ACI Virtual Pod, see the section Guidelines and Limitations for Cisco ACI Virtual Edge When It Is Part of Cisco ACI vPod, on page 3 in this guide.

- Layer 4 to Layer 7 services is supported in routed mode with policy-based redirect (PBR); there is no support for transparent mode.
- Do not deploy both service VMs of an HA pair behind the same Cisco ACI Virtual Edge.

  To ensure that both service VMs of an HA pair do not end up behind the same Cisco ACI Virtual Edge after deployment, create a VM-host affinity rule. The rule ensures that each service VM of an HA pair runs on different hosts.

  When creating VM-host affinity rule, for **Type**, choose **Virtual Machines to Hosts** and in DRS groups, choose **Must run on hosts in group**. For more information about creating a VM-host-affinity rule, refer to VMware documentation for the corresponding vSphere version.
- Do not manually associate non-service VMs to a service EPG. At any point on a single host, only one endpoint for each service EPG is supported.
- Do not tag service VM interfaces deployed on Cisco ACI Virtual Edge; Cisco ACI Virtual Edge does not support trunk port groups.
- Virtual MAC-based service VM deployment is not supported for Cisco ACI Virtual Edge when it is not part of Cisco ACI Virtual Pod.
- The supported modes of service VM deployment on Cisco ACI Virtual Edge are standalone and HA mode (active/standby).

  If you use Citrix NetScaler LoadBalancer, 1-Arm mode is also supported.
- Cisco ACI Virtual Edge supports vMotion of service VMs.

  Note Refer to the corresponding vendor documentation for support of vMotion of service VMs on the VMware environment. The vMotion support is vendor-specific and may have certain guidelines and limitations.
- Only service-graph based deployments are supported on Cisco ACI Virtual Edge.
- Cisco ACI Virtual Edge does not support Route-Peering and Trunking Port.
- You cannot migrate Layer 4 to Layer 7 services deployed on a Cisco Application Virtual Switch (AVS) domain to Cisco ACI Virtual Edge.

  To proceed with migration, undeploy services on Cisco AVS. Also, while migrating from a VMware VDS Domain to Cisco ACI Virtual Edge, you can move the consumer and provider EPGs to Cisco ACI

Virtual Edge. However, Layers 4 to Layer 7 service EPGs still belong to the VMware VDS. For more information, see the chapter "Migration from VMware VDS to Cisco ACI Virtual Edge" of the *Cisco ACI Virtual Edge Installation Guide*.

- Ensure that the management and HA interfaces of service VMs are not connected to the Cisco ACI Virtual Edge port group.
- When you configure the Cisco ACI Virtual Edge VMM domain, it is mandatory to associate a VLAN pool with the domain.

  You must associate a VLAN pool with the domain because service VMs are deployed on the Cisco ACI Virtual Edge VMM domain with VLAN encapsulation mode. Configure both internal and external ranges for the VLAN pool. See the chapter Mixed-Mode Encapsulation in this guide for information.
- You can deploy compute VMs (providers and consumers) in the Cisco ACI Virtual Edge VMM domain with VXLAN or VLAN encapsulation mode.

  To support compute VMs in either mode, configure the Cisco ACI Virtual Edge VMM domain with mixed-mode encapsulation. See the chapter Mixed-Mode Encapsulation in this guide for information.

Guidelines and Limitations for Cisco ACI Virtual Edge When It Is Part of Cisco ACI vPod

Follow the guidelines in this section when configuring Layer 4 to Layer 7 service graphs for Cisco Application Centric Infrastructure Virtual Edge when it is part of Cisco ACI Virtual Pod (vPod).

- Layer 4 to Layer 7 services are supported using only Layer 3 policy-based redirect (PBR) is supported.

  For information about PBR, see the chapter "Configuring Policy-based Redirect" in the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.
- Do not deploy both service VMs of an HA pair behind the same Cisco ACI Virtual Edge.

  Create a VM-host affinity rule. The rule ensures that both service VMs of an HA pair do not end up behind the same Cisco ACI Virtual Edge after deployment. The rule also ensures that each service VM of an HA pair runs on different hosts.

  When creating VM-host affinity rule, for **Type**, choose **Virtual Machines to Hosts** and in DRS groups, choose **Must run on hosts in group**. For more information about creating a VM-host-affinity rule, refer to VMware documentation for the corresponding vSphere version.
- Do not manually associate non-service VMs to a service EPG. At any point on a single host, only one endpoint for each service EPG is supported.
- Do not tag service VM interfaces deployed on Cisco ACI Virtual Edge; Cisco ACI Virtual Edge does not support trunk port groups.
- Virtual MAC-based service VM deployment is supported for Cisco ACI Virtual Edge when it is deployed inside Cisco ACI Virtual Pod.

  When creating a device policy for Citrix NetScaler Load Balancer in HA mode on the Cisco Application Policy Infrastructure Controller (APIC), enable Promiscuous Mode. The virtual MAC configuration on the service device requires that Promiscuous Mode be enabled.
- The supported modes of service VM deployment on Cisco ACI Virtual Edge are standalone, HA mode (active/standby), and 1-arm mode (in case of Citrix Netscaler LoadBalancer).

- Cisco ACI Virtual Edge supports VMware vMotion of service VMs.
- Only service-graph based deployments are supported on Cisco ACI Virtual Edge.
- Cisco ACI Virtual Edge does not support Route-Peering or Trunking Port.
- For Cisco ACI Virtual Edge used in the cloud, equal-cost multipath routing (ECMP) and health group features are not supported. This is the case although you may be able to configure those features using service graphs.
- You cannot migrate service VMs from Cisco ACI vPod to a physical pod or service VMs from a physical pod to a Cisco ACI vPod.
- Layer 4-Layer 7 PBR policy does not have pod awareness.
- When Citrix NetScaler service is deployed e in HA mode, VMware vMotion is not supported between Cisco ACI vPod and the physical pod.
- If you use Citrix NetScaler Load Balancer in HA mode, non-vMAC switchover cannot be done, because listing multiple redirect entries in the redirect policy is not supported.
- VMware vMotion of ASAv devices is not supported after one switchover. VMware vMotion of ASAv devices is supported only when operational ACTIVE is same as configured ACTIVE device.

Qualified Service Devices

Service graph deployments for Cisco Application Centric Infrastructure (ACI) Virtual Edge are qualified for the following service devices:

- Cisco Adaptive Security Virtual Appliance (ASAv) firewall Version 9.9(1)

Note Before you deploy ASAv on the Cisco ACI Virtual Edge VMM domain, enable monitoring of `externalIf` and `internalIf`. To enable monitoring through the CLI, you can use the commands **monitor-interface externalIf** and **monitor-interface internalIf** on ASAv.

- INDUS: Revised at Pooja's request. Originally: "Citrix NetScaler VPX (Unmanaged mode) Version 11.0 build 70.16." ~ catortiz 8/16/19. Citrix NetScaler VPX Version 11.1 build 48.10nc.

Supported Deployments

The Cisco Application Centric Infrastructure (ACI) Virtual Edge supports the following deployments:

- ASAv in Routed Mode
- F5 Networks BIG-IP load balancer (Unmanaged mode), Cisco ACI Virtual Edge when not used with Cisco ACI Virtual Pod (vPod)
  - One-arm mode
  - Two-arm mode

- Citrix NetScaler VPX Version 11.1 build 48.10nc for Cisco ACI Virtual Edge when used with Cisco ACI vPod
- Standalone and HA mode (active/standby)
- One-arm and two-arm deployment modes

Bridge Domain Configuration for Cisco ASAV, Citrix NetScaler, or F5 BIG-IP ADC

When you configure the bridge domains for Cisco ASAv, Citrix NetScaler, or F5 BIG-IP ADC, configure the bridge domains as you do for a generic configuration, except as follows:

Configuration	Action
L2 Unknown Unicast	Choose **Flood**.
ARP Flooding check box	Check the check box.
Unicast Routing check box	This configuration depends on deployment. For example, put a check in the **Unicast Routing** check box if you want the Cisco ACI fabric to route the traffic. Also, when configuring the inside bridge domain, enable **Unicast Routing** if you plan to use endpoint attach.

References

For more information on configuring Bridge domains on Cisco ACI, see the Cisco APIC Layer 2 Networking Configuration Guide.

For general information about bridge domain setting that is related to service graph design, see Service Graph Design with Cisco Application Centric Infrastructure White Paper.