Cisco Application Virtual Switch Release Notes, Release 5.2(1)SV3(2.6)

First Published: 2017-02-18
Last Updated: 2017-03-20

This document describes the features, bugs, and limitations for the Cisco Application Virtual Switch (AVS) software.

Contents

This document includes the following sections:

Cisco AVS

Cisco AVS is a hypervisor-resident distributed virtual switch that is specifically designed for Cisco Application Centric Infrastructure (ACI) and managed by the Application Policy Infrastructure Controller (APIC). Cisco AVS implements the OpFlex protocol for control plane communication.

Cisco Systems, Inc.
www.cisco.com

Cisco AVS supports two modes of traffic forwarding: local switching and no local switching. The forwarding mode is selected during Cisco AVS installation.

Cisco AVS is supported as a vLeaf for Cisco APIC with the VMware ESXi hypervisor. It manages a data center defined by the vCenter Server.

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

Cisco AVS Software Compatibility

Cisco AVS Release 5.2(1)SV3(2.6) is supported as a vLeaf for Cisco APIC with releases 5.1, 5.5, and 6.0 of the VMware ESXi hypervisor.

Note When you choose a Cisco AVS VIB, you must choose the one compatible with the version of VMware ESXi hypervisor that you use. ESXi 5.1 uses *xxxx*.3.1.1.vib, ESXi 5.5 uses *xxxx*.3.2.1.vib, and ESXi 6.0 uses *xxxx*.6.0.1.vib.

Compatibility and Upgrade/Downgrade Considerations

The following table lists the compatibility of Cisco AVS with Cisco APIC. Note the following:

- The “Recommended Cisco APIC Version” in the second column of the table is the version that has been thoroughly tested with the Cisco AVS version.
- The “Upgrade Compatible” versions in the third column of the table are versions that you can upgrade from to the recommended Cisco APIC version.

  For example, you cannot upgrade from Cisco APIC version 1.1(4l) to Cisco APIC version 2.1(1h); you can upgrade only from the versions in upgrade compatible list.
- The “Downgrade Compatible” versions in the third column are versions to which you can downgrade to from the recommended Cisco APIC version.

  For example, you cannot downgrade from APIC version 2.1(1h) to Cisco APIC version 1.1(4l); you can downgrade only to the versions in the downgrade compatible list.
- Although you can upgrade or downgrade Cisco APIC to a compatible version, you also should upgrade or downgrade Cisco AVS to a recommended version.

  For example, if you downgrade Cisco APIC from version 2.1(1h) to 2.0(2f), you also should downgrade Cisco AVS 5.2(1)SV3(2.5) to Cisco AVS 5.2(1)SV3(2.2). The Cisco AVS version in the first column is the recommended version for the Cisco APIC version in the second column.
- In the table, all Cisco APIC versions in the third column are upgrade and downgrade compatible unless otherwise stated.

Table 1 Cisco AVS and Cisco APIC Compatibility

Cisco AVS Version	Recommended Cisco APIC Version	Upgrade/Downgrade Compatible Cisco APIC Version
5.2(1)SV3(2.6)	2.1(2d)	• Upgrade compatible versions: 2.1(1i), 2.0(2m), 2.0(1r), 1.3(2j), 1.3(1j), 1.2(3m) • Downgrade compatible versions: 2.1(1i), 2.0(2m), 2.0(1r), 1.3(2j), 1.3(1j)
5.2(1)SV3(2.5)	2.1(1h)	• Upgrade compatible versions: 2.0(2f), 2.0(1q), 1.3(2i), 1.3(1i), 1.2(3h) • Downgrade compatible versions: 2.0(2f), 2.0(1q), 1.3(2i), 1.3(1i)
5.2(1)SV3(2.2)	2.0(2f)	• Upgrade compatible versions: 2.0(1p), 1.3(2h), 1.3(1i), 1.2(3h), 1.2(2h), 1.2(1m) • Downgrade compatible versions: 2.0(1p), 1.3(2h), 1.3(1i), 1.2(3h), 1.2(2h), 1.2(1m), 1.1(4l)
5.2(1)SV3(2.1a)	2.0(1p)	• Upgrade compatible versions: 1.3(2f), 1.3(1g), 1.3(1i), 1.2(3d), 1.2(2h), 1.2(1m), 1.1(4l) • Downgrade compatible versions: 1.3(2f), 1.3(1g), 1.3(1i), 1.2(3d), 1.2(2h), 1.2(1m)
5.2(1)SV3(2.1)	2.0(1m)	• Upgrade compatible versions: 1.3(2f), 1.3(1g), 1.3(1i), 1.2(3d), 1.2(2h), 1.2(1m), 1.1(4l) • Downgrade compatible versions: 1.3(2f), 1.3(1g), 1.3(1i), 1.2(3d), 1.2(2h), 1.2(1m)
5.2(1)SV3(1.25)	1.3(2f)	1.3(1g), 1.3(1i), 1.2(3d), 1.2(2h), 1.2(1m), 1.1(4k), 1.1(3f), 1.1(2i), 1.1(1s)[1]
5.2(1)SV3(1.20a)	1.3(1g), 1.3(1i)	1.2(3c), 1.2(2g), 1.2(1m), 1.1(4i), 1.1(3f), 1.1(2h)
5.2(1)SV3(1.20)	1.3(1g)	1.2(3c), 1.2(2g), 1.2(1m), 1.1(4i), 1.1(3f), 1.1(2h)
5.2(1)SV3(1.16b)	1.2(3g)	1.2(2h),1.2(2g), 1.2(1m), 1.1(4i), 1.1(3f), 1.1(2h), 1.1(1s), 1.0(4q)
5.2(1)SV3(1.16a)	1.2(3e)	1.2(2h),1.2(2g), 1.2(1m), 1.1(4i), 1.1(3f), 1.1(2h), 1.1(1s), 1.0(4q)
5.2(1)SV3(1.16)	1.2(3c)	1.2(2g), 1.2(1m), 1.1(4i), 1.1(3f), 1.1(2h), 1.1(1s), 1.0(4q)
5.2(1)SV3(1.15)	1.2(2g), 1.2(2h)	1.2(1m), 1.1(4g), 1.1(4i), 1.1(4e) 1.1(3f), 1.1(2i), 1.1(1s), 1.0(4q)
5.2(1)SV3(1.10a)	1.2(1m)	1.1(4i), 1.1(4e), 1.1(3f), 1.1(2h), 1.1(1s), 1.0(4q)
5.2(1)SV3(1.10)	1.2(1i)[1]	1.1(4i), 1.1(4e), 1.1(3f), 1.1(2h), 1.1(1s), 1.0(4q)
5.2(1)SV3(1.7)	1.1(4i), 1.1(4g), 1.1(4f), 1.1(4e)	1.1(3f), 1.1(2h), 1.1(1s)
5.2(1)SV3(1.6)	1.1(3f)	1.1(2h), 1.1(1s), 1.1(1r), 1.0(4q)
5.2(1)SV3(1.5i)	1.1(2h)	1.1(1s), 1.1(1o), 1.0(4q)
5.2(1)SV3(1.5c)	1.1(1s)	1.1(1o), 1.1(1j), 1.0(4q)
5.2(1)SV3(1.5b)	1.1(3f)	1.1(2h), 1.1(1r), 1.0(4q)
5.2(1)SV3(1.5a)	1.1(2h)	1.1(1o), 1.0(4q)
5.2(1)SV3(1.5)	1.1(1o)	1.1(1j), 1.0(4q), 1.0(4o), 1.0(4h)

Table 1 Cisco AVS and Cisco APIC Compatibility (continued)

Cisco AVS Version	Recommended Cisco APIC Version	Upgrade/Downgrade Compatible Cisco APIC Version
5.2(1)SV3(1.3c)	1.0(4q)	1.0(4o), 1.0(4h), 1.0(3f), 1.0(2m), 1.0(2j), 1.0(1n), 1.0(1k), 1.0(1h), 1.0(1e)
5.2(1)SV3(1.3b)	1.0(4h)	1.0(3f), 1.0(2m), 1.0(2j), 1.0(1n), 1.0(1k), 1.0(1h), 1.0(1e)
5.2(1)SV3(1.3)	1.0(3o)	1.0(3f), 1.0(2m), 1.0(2j), 1.0(1n), 1.0(1k), 1.0(1h), 1.0(1e)
5.2(1)SV3(1.2)	1.0(2m)	1.0(2j), 1.0(1n), 1.0(1k), 1.0(1h), 1.0(1e)
5.2(1)SV3(1.1)	1.0(1n)	1.0(1k), 1.0(1h), 1.0(1e)
4.2(1)SV2(2.3)	1.0(1n)	1.0(1k), 1.0(1h), 1.0(1e)

1. Cisco APIC Release 1.2(1i) is deferred. See the Cisco APIC Release Notes for Release 1.2(1i) for more information.

New and Changed Information

Cisco AVS Release 5.2(1)SV3(2.6) supports all of the features that were introduced in 5.2(1)SV3(1.10), 5.2(1)SV3(1.10a), 5.2(1)SV3(1.15), 5.2(1)SV3(1.16), 5.2(1)SV3(1.16a), 5.2(1)SV3(1.16b), 5.2(1)SV3(1.20), 5.2(1)SV3(1.20a), 5.2(1)SV3(1.25), 5.2(1)SV3(2.1), 2(1)SV3(2.1a), 5.2(1)SV3(2.2), and 5.2(1)SV3(2.5). For details, see the *Cisco Application Virtual Switch Release Notes* for these releases.

VLAN/VXLAN Mixed-Mode Encapsulation

Beginning with Cisco AVS Release 5.2(1)SV3(2.5), you can configure a single VMM domain to use VLAN and VXLAN encapsulation. Previously, you needed to configure two separate VMM domains, one for VLAN EPG encapsulation and one for VXLAN EPG encapsulation. Consequently, a domain's encapsulation mode now specifies its preferred encapsulation, not its sole encapsulation. When you associate an EPG to a domain using auto encapsulation, the EPG uses the domain's preferred encapsulation.

Note that Cisco APIC and Cisco AVS might show different encapsulation modes. This is expected: The Cisco APIC GUI shows the preferred encapsulation mode, while the Cisco AVS CLI shows the effective encapsulation mode. The latter is used internally by VXLAN load balancing and health status and doesn't affect actual EPG encapsulation.

For details, see the *Cisco Application Virtual Switch Configuration Guide*.

Support for `vemcmd show` Commands in Cisco APIC

Beginning with Cisco AVS Release 5.2(1)SV3(2.5), you can execute `vemcmd show` commands to troubleshoot Cisco AVS remotely through Cisco APIC NX-OS style CLI. Previously, the only method you could use to execute `vemcmd show` commands was directly on the Cisco AVS host.

For details, see the *Cisco Application Virtual Switch Troubleshooting Guide*.

Additional Parameters for LACP Load Balancing

Beginning with Cisco AVS Release 5.2(1)SV3(2.5), you can configure LACP load balancing for Cisco AVS using one of more than a dozen different parameters. Previously, LACP load balancing was automatically configured, using the source MAC address. However, now you configure LACP load balancing by issuing a `vemcmd` command through the ESXi CLI.

For details, see the *Cisco Application Virtual Switch Configuration Guide*.

FirePOWER NGIPS for Vulnerability Detection

You can now use the FirePOWER Next-Generation Intrusion Prevention System (NGIPS) for vulnerability detection, which then performs automatic microsegmentation of rogue endpoints in the ACI fabric for Cisco AVS, VMware vSphere Distributed Switch (VDS), and Bare-Metal workloads.

Limitations and Restrictions

Upgrades of Cisco APIC, Leaf Switches, and the Cisco AVS to Cisco APIC 1.2(2g) or Later

Starting with the Cisco APIC 1.2(2g) release, the Cisco AVS uses site-specific certifications; previously, the Cisco AVS used image-based certifications. So when you upgrade from an earlier release to Cisco APIC 1.2(2g) or later, you need to follow a particular sequence when upgrading Cisco APIC, leaf switches, and the Cisco AVS. See the section “Upgrading from a Previous Release to Cisco APIC Release 1.2(2g) or Later” in the *Cisco AVS Installation Guide*.

Distributed Firewall when Using Direct Service Return with Load Balancing

You should disable Distributed Firewall if you are using direct service return with load balancing. If Distributed Firewall is enabled, an HTTP session will not be established.

Features not Supported for Cisco AVS with Multipod

The following features are not supported for Cisco AVS with multipod in the Cisco APIC 2.0(1.x) release:

- L3 Multicast
- Storage vMotion with two separate NFS in two separate PODs
- ERSPAN destination in different PODs
- Distributed Firewall syslog server in different PODs

Pre-provisioning not Supported for EPG Resolution Immediacy

When you set EPG resolution immediacy, Cisco AVS does not support pre-provisioning, which downloads a policy to a switch before the switch is installed.

Intra-EPG Isolation of Microsegment EPGs not Supported

Using intra-EPG isolation on a Cisco AVS microsegment (uSeg) EPG is not currently supported. Communication will be possible between two endpoints that reside in separate uSeg EPGs if either has intra-EPG isolation enforced, regardless of any contract that exists between the two EPGs.

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter a problem, feature, or a product name and press **Return**. (Leave the other fields empty.)

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

To export the results to a spreadsheet, click the **Export Results to Excel** link.

Open Bugs

The following table lists the open bugs in Cisco AVS Release 5.2(1)SV3(2.6):

Table 2 Open Bugs

Bug ID	Headline
CSCut61064	An IP-based microsegment breaks for a quiet VM moved to a guest OS-based microsegment in another bridge domain.
CSCux27711	ASAv ping stops at protected VMs after VEM restarts.

Table 2 Open Bugs (continued)

Bug ID	Headline
CSCva01452	Cisco AVS doesn't initiate OpFlex connection from other VTEP VMKs of VXLAN load balancing.
CSCva15371	Multicast traffic floods due to IGMP support limitation on Cisco AVS.

Resolved Bugs

The following table lists the resolved bugs in Cisco AVS Release 5.2(1)SV3(2.6).

Table 3 Resolved Bugs

Bug ID	Headline
CSCuz52137	AVS shows invalid output for the command "vemcmd show dfw globals."
CSCva21169	Traffic between enforced and unenforced EPGs will not work with Cisco N9000 as IPN.
CSCva39464	Kernel panic when putting a host into maintenance mode.
CSCva49536	AVS: Migration of ports across base and VM attributes may not work.
CSCva85030	Newer AVS doesn't report stats to older TOR.
CSCva94195	Configuration for vSwitch policy moved to VMM domain since Cisco APIC version 1.2x.
CSCvb04299	Error when adding host to AVS through vCenter Web Client.
CSCvb42595	On FI flap, multicast packets being dropped for 30 - 180 sec.
CSCvc29111	Vtep pinning incorrect on toggling PC mode.
CSCvc61634	PSOD on ESXi 5.5 in sf_apply_config_change.

The compatible Cisco APIC version contains bug fixes; see the Cisco APIC release notes.

Related Documentation for Cisco AVS

The Cisco AVS documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

Related Documentation for Cisco APIC

The Cisco APIC documentation is available at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Cisco APIC documentation includes the *Cisco ACI Virtualization Guide*, which provides detailed information about Distributed Firewall and Microsegmentation with Cisco AVS.

Documentation Feedback

To provide technical feedback on this document or report an error or omission, please send your comments to avs-docfeedback@cisco.com. We appreciate your feedback.

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/en/US/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 deliver content directly to your desktop using a reader application. The RSS feeds are a free service.
