# Cisco Application Virtual Switch Release Notes, Release 5.2(1)SV3(3.20)

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

**Note:** Use this document in combination with the Cisco Application Policy Infrastructure Controller (APIC) Release Notes, which you can view at the following location:

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

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/products-release-notes-list.html

Table 1 shows the online change history for this document.

**Table 1 Online History Change**

| Date | Description |
|---|---|
| 2017-12-22 | Created release notes for the Cisco AVS 5.2(1)SV3(3.20) release. |
| 2018-03-30 | Restored information about Cisco AVS 5.2(1)SV3(3.3) to Table 2. |
| 2018-04-13 | Added Cisco AVS 5.2(1)SV3(3.4) to Table 2. |

# Contents

This document includes the following sections:

# Introduction: 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 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 Guide*.

# Cisco AVS Software Compatibility

Cisco AVS Release 5.2(1)SV3(3.20) is supported as a vLeaf for Cisco APIC with releases 5.5, 6.0, and 6.5 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 5.5 uses xxxx.3.2.1.vib, ESXi 6.0 uses xxxx.6.0.1.vib, and ESXi 6.5 uses xxxx.6.5.1.vib.

## Compatibility and Upgrade/Downgrade Considerations

Table 2 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 2 – Cisco AVS and Cisco APIC compatibility**

| Cisco AVS Version | Recommended Cisco APIC Version | Upgrade/Downgrade Compatible Cisco APIC Version |
|---|---|---|
| 5.2(1)SV3(3.20) | 3.1(1i) | • Upgrade compatible versions: 2.2(2q), 2.3(1i), 3.0(1k), 3.0(2h)<br>• Downgrade compatible versions: 2.2(2q), 2.3(1i), 3.0(1k), 3.0(2h) |

| Cisco AVS Version | Recommended Cisco APIC Version | Upgrade/Downgrade Compatible Cisco APIC Version |
|---|---|---|
| 5.2(1)SV3(3.10) | 3.0(1k) | • Upgrade compatible versions: 2.3(1f), 2.2(2k), 2.2(1o)<br>• Downgrade compatible versions: 2.3(1f), 2.2(2k), 2.2(1o) |
| 5.2(1)SV3(3.5a) | 2.3(1l) | • Upgrade compatible versions: 2.2(2i), 2.2(1o), 2.1(2g), 2.1(1i)<br>• Downgrade compatible versions: 2.2(2i), 2.2(1o), 2.1(2g), 2.1(1i) |
| 5.2(1)SV3(3.5) | 2.3(1e) | • Upgrade compatible versions: 2.2(2i), 2.2(1o), 2.1(2g), 2.1(1i)<br>• Downgrade compatible versions: 2.2(2i), 2.2(1o), 2.1(2g), 2.1(1i) |
| 5.2(1)SV3(3.4) | 2.2(4f) | • Upgrade compatible versions: 2.2(3t), 2.2(2q), 2.2(1o), 2.1(4a), 2.1(3j), 2.1(2k), 2.1(1i), 2.0(2o)<br>• Downgrade compatible versions: 2.2(3t), 2.2(2q), 2.2(1o), 2.1(4a), 2.1(3j), 2.1(2k), 2.1(1i), 2.0(2o) |
| 5.2(1)SV3(3.3) | 2.2(3j) | • Upgrade compatible versions: 2.2(2q), 2.2(1o), 2.1(3h), 2.1(2e), 2.1(1i), 2.0(2n)<br>• Downgrade compatible versions: 2.2(2q), 2.2(1o), 2.1(3h), 2.1(2e), 2.1(1i), 2.0(2n) |
| 5.2(1)SV3(3.2) | 2.2(2j) | • Upgrade compatible versions: 2.2(1o), 2.1(2e), 2.1(1i), 2.0(2n)<br>• Downgrade compatible versions: 2.2(1o), 2.1(2e), 2.1(1i), 2.0(2n) |
| 5.2(1)SV3(2.14) | 2.2(1n) | • Upgrade compatible versions: 2.1(1h), 2.0(2h), 2.0(1r)<br>• Downgrade compatible versions: 2.1(1h), 2.0(2h), 2.0(1r) |
| 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)<br>• 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)<br>• Downgrade compatible versions: 2.0(2f), 2.0(1q), 1.3(2i), 1.3(1i) |
| 5.2(1)SV3(2.2a) | 2.0(2n) | • Upgrade compatible versions: 2.0(2m), 2.0(1p), 1.3(2h), 1.3(1i), 1.2(3h), 1.2(2h), 1.2(1m)<br>• Downgrade compatible versions: 2.0(2m), 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(2.2) | 2.0(2f) | • Upgrade compatible versions: 2.0(1p), 1.3(2h), 1.3(1i), 1.2(3h),<br>• 1.2(2h), 1.2(1m)<br>• Downgrade compatible versions: 2.0(1p), 1.3(2h), 1.3(1i), 1.2(3h),<br>• 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)<br>• 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)<br>• 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[1] |

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

| Cisco AVS Version | Recommended Cisco APIC Version | Upgrade/Downgrade Compatible Cisco APIC Version |
|---|---|---|
| 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) |

For compatibility and other information about Cisco AVS releases earlier than 5.2(1)SV3(1.5), see the Cisco AVS Release Notes for the specific release on Cisco.com.

# New and Changed Information

Cisco AVS Release 5.2(1)SV3(3.20) 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), 5.2(1)SV3(2.5), 5.2(1)SV3(2.14), 5.2(1)SV3(3.2), 5.2(1)SV3(3.5), 5.2(1)SV3(3.8), 5.2(1)SV3(3.10), and 5.2(1)SV3(3.20). For details, see the *Cisco Application Virtual Switch Release Notes* for these releases.

## First Hop Security

Starting with Cisco AVS Release 5.2(1)SV3(3.20), First-Hop Security (FHS) feature is supported. The FHS feature set provides improved management and IPv4 link security over the layer 2 links. In a service provider environment, these features closely control address assignment and derived operations, such as Duplicate Address Detection (DAD) and Address Resolution (AR). For information about the new feature, see the section "First Hop Security" in the *Cisco Application Virtual Switch Configuration Guide*.

# Limitations and Restrictions

For Cisco AVS scalability information, see the *Verified Scalability Guide for Cisco ACI* for the relevant Cisco APIC release.

## Changing the MTU VTEP Interface while Decommissioning Cisco APIC

If you are decommissioning a Cisco APIC, do not change the maximum transmission unit (MTU) Virtual Tunnel Endpoint (VTEP) at the same time. If you do so, when you recommission the Cisco APIC, the lease does not appear available although the leaf still has the VTEP entry.

## 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.

## 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.

## Number of Cisco AVS Instances on ESX or ESXi Host

You can connect a single ESX or ESXi host to only one Cisco AVS at a time. You cannot add multiple Cisco AVS to a single ESX or ESXi host.

# Bugs (Caveats)

## 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.

1. Go to http://tools.cisco.com/bugsearch.
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.
3. To search for a specific bug, enter the bug ID in the **Search For** field and press **Return**.
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.
5. To export the results to a spreadsheet, click the **Export Results to Excel** link.

## Open Bugs

Table 3 lists the open bugs in Cisco AVS Release 5.2(1)SV3(3.20):

**Table 3 – Open Cisco AVS 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. |
| CSCva15371 | MC traffic floods due to IGMP support limitation on Cisco AVS. |
| CSCvc02318 | New port attach on same ltl retains old dfw syslog flows of old port. |
| CSCvc77434 | Cisco AVS traffic not sent on uplinks after ESXi host vmnic down and up commands. |
| CSCvd39664 | VPC LACP down on UCS C-series with VIC on ESXi 6.5 due to enic driver that comes with ESX installer. |
| CSCvd60582 | vRealize: Add support for DVS version 6.5 in vRealize workflow for VMM creation. |
| CSCvd95133 | VSUM 2.1: Observed exception while uploading 5.2(1)SV3(3.2) latest patch bundle. |

## Resolved Bugs

Table 4 lists the resolved bugs in Cisco AVS Release 5.2(1)SV3(3.20):

**Table 4 – Resolved Cisco AVS bugs**

| Bug ID | Headline |
|---|---|
| CSCuv50632 | VEM does not send an IGMP join and therefore cannot resolve ARP. |
| CSCuz32676 | Distributed Firewall: Flows in Last_ACK even after closing the connection. |
| 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 | Cisco AVS: Migration of ports across base and VM attributes may not work. |
| CSCva85030 | Newer Cisco AVS doesn't report stats to older TOR. |
| CSCva94195 | Configuration for vSwitch policy moved to VMM domain since Cisco APIC version 1.2x. |
| CSCvb00780 | Cisco AVS doesn't apply IP or MAC microsegment EPG to VM port. |
| CSCvb04299 | Error when adding host to AVS through vCenter Web Client. |
| CSCvb48774 | Traffic drops when Useg EPG is deleted and source and destination endpoints are in two different TORs. |
| CSCvc74777 | UCS topology: On VEM restart, pinning keeps change on some of hosts. |

The compatible Cisco APIC version contains bug fixes; see the Cisco APIC *Release Notes*.

# Documentation

## Related Documentation for Cisco AVS

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

For information about guides and videos for Cisco AVS, see the *Cisco Application Virtual Switch Documentation Overview*.

## Related Documentation for Cisco APIC

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.