Cisco ACI Virtual Edge Release Notes, Release 3.1(1h)

Cisco Application Centric Infrastructure (ACI) Virtual Edge is a hypervisor-independent distributed service virtual machine (VM) that is specifically designed for Cisco ACI. It leverages the native distributed virtual switch that belongs to the hypervisor. Cisco ACI Virtual Edge runs in the user space, operates as a virtual leaf, and is managed by Cisco APIC.

Cisco ACI Virtual Edge is supported as a vLeaf for Cisco APIC with the VMware ESXi hypervisor. It manages a data center defined by the VMware vCenter Server. If you use Cisco AVS, you can migrate to Cisco ACI Virtual Edge; if you use VMware VDS, you can run Cisco ACI Virtual Edge on top of it.

This document describes the features, bugs, and limitations for the Cisco Application Centric Infrastructure (ACI) Virtual Edge software. Use this document with the Cisco Application Policy Infrastructure Controller Release Notes, Release 5.1(1h).

For more information about this product, see *Related Content*.

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Date	Description
2021-04-15	Updated the Limitations and Restrictions section. Information was added for transient faults raised and cleared due to heart beat timeouts.
2020-10-22	Cisco ACI Virtual Edge Release 3.1(1h) became available.

Contents

- New Software Features
- Changes in Behavior
- Limitations and Restrictions
- Open Issues
- Resolved Issues
- Known Issues
- Compatibility Information
- Related Content
- Documentation Feedback
- Legal Information

New Software Features

There are no new software features in this release.

Changes in Behavior

There are no changes in behavior in this release.

Limitations and Restrictions

General

L3 Multicast is not supported on bridge domains with endpoints after AVE.

Hypervisor Availability

Cisco ACI Virtual Edge is available only on the VMware hypervisor.

VMware vSphere Support

Cisco ACI Virtual Edge is supported only on VMware vSphere 6.0 and later versions.

Cisco ACI Virtual Edge Deployment

The server where you install Cisco ACI Virtual Edge must have an Intel Nehalem CPU or later. You also must set the cluster Enhanced vMotion Compatibility (EVC) to a Nehalem CPU or later. See the knowledge base article Enhanced vMotion Compatibility (EVC) processor support (1003212) on the VMware web site.

Cisco Confidential

We recommend that you install only one Cisco ACI Virtual Edge virtual machine (VM) on each host.

Removing Cisco ACI Virtual Edge or the ESXi host from the VMware vCenter and then adding it back in is not supported. If you do that, Cisco ACI Virtual Edge loses password, infra VLAN, IP address, and other key configurations. You should instead delete the original Cisco ACI Virtual Edge and deploy a new one.

After you deploy Cisco ACI Virtual Edge, if the Cisco ACI Virtual Edge VM is moved across VMware vCenter, all the configurations that you made during deployment are lost.

Transient Fault, F3278, is raised and cleared due to Heart Beat (HB) timeouts that happen between AVE and leaf switches. The fault clears when the next HB is seen on AVE.

Management Interface IP Address

The Cisco ACI Virtual Edge management interface must have an IPv4 address. It can have an additional IPv6 address, but you cannot configure it with only an IPv6 address.

VMware vSphere vMotion Support

VMware vSphere vMotion is supported for endpoints but not supported for Cisco ACI Virtual Edge itself.

Note: After you migrate VMs using cross-data center VMware vMotion in the same VMware vCenter, you may find a stale VM entry under the source DVS. This stale entry can cause problems, such as host removal failure. The workaround for this problem is to enable "Start monitoring port state" on the vNetwork DVS. See the KB topic "Refreshing port state information for a vNetwork Distributed Virtual Switch" on the VMware Web site for instructions.

Features Not Supported for Cisco ACI Virtual Edge with Multipod

The following features are not supported for Cisco ACI Virtual Edge with multipod:

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

Features Not Supported for Cisco ACI Virtual Edge when It Is Part of Cisco ACI vPod

Cisco ACI Virtual Edge is not supported for the following features when it is part of Cisco ACI vPod:

- VMware vSphere Proactive HA
- SPAN and ERSPAN
- Subnets configured under endpoint group EPGs

Pre-provisioning Not Supported for EPG Resolution Immediacy

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

Cisco Confidential

VMware Fault Tolerance and Distributed Firewall

When VMware Fault Tolerance failover occurs, Cisco ACI Virtual Edge cannot transfer pods because no VMware vMotion is involved in the failover. When that occurs, you need to reestablish all TCP sessions. This issue occurs regardless of whether Cisco ACI Virtual Edge is part of a Cisco ACI Virtual Pod.

Unsupported Operations in VMware vCenter

Any manual modification and override of Cisco ACI Virtual Edge portgroups in VMWare vCenter or modification of the interface connection states in Cisco ACI Virtual Edge are not supported. Making these modifications might render the Cisco ACI Virtual Edge unstable.

MAC Pinning Not Supported with Direct Connection to VPC Leaf Pair

Do not use MAC pinning with a direct connection to a VPC leaf pair. Instead, use Link Aggregation Control Protocol (LACP) or enhanced LACP to provide redundancy and reliability. Using MAC pinning with a direct connection leads to traffic loss when peer leaf switches are rebooted. Use MAC Pinning only where virtual port channel (VPC) cannot be supported, such as for Cisco UCS Fabric Interconnects with southbound interfaces.

Open Issues

Click the bug ID in the following table to access the Bug Search Tool and see additional information about the bug. A bug might also exist in releases other than the Cisco ACI Virtual Edge 3.1(1h) releases.

Bug ID	Description
CSCvh06525	When doing a bulk vMotion of 50 or more ports, the ports take additional time to come up and start forwarding traffic. We see delays of about 30 seconds to two minutes for the very last port to come up when doing vMotion of 300 ports. Some ports forward traffic much earlier as they are in the front of the vMotion queue.
CSCvj58344	When control channel (OpFlex) from Cisco ACI Virtual Edge to the physical leaf is down, any port that attaches and then detaches before OpFlex comes back will remain in Cisco ACI Virtual Edge indefinitely. No functional impact since the actual port has already gone away.
CSCvj59097	If a bridge domain multicast is configured with optimized flood and is moved by vMotion, the subscriber to another policy group that is another VPC or other top-of-rack pair can cause loss of reception of up to the maximum configured querier interval time.
CSCvj74270	Traffic loss is seen on VMs when disconnecting and reconnecting Cisco ACI Virtual Edge VM NICs from VMware vCenter.

Cisco Confidential

Bug ID	Description

CSCvq63041	Cisco ACI Virtual Edge–when not part of Cisco ACI Virtual Pod–fails to come up. In the kernel logs, we see logs similar to the following one, showing that it was blocked for more than 2 minutes:
	
	`Jul 21 22:09:26 localhost kernel: INFO: task jbd2/dm-21-8:3051 blocked for more than 120 seconds.`
	
	Or you see logs similar to the following ones, in which the writes were blocked for more than 8 minutes:
	
	`Jul 21 22:01:47 localhost systemd[1]: Started Process Monitoring and Control Daemon.`
	`Jul 21 22:09:26 localhost systemd-journal[3700]: Permanent journal is using 16.0M (max allowed 594.7M, trying to leave 892.0M free of 5.4G available`

CSCvq87091	When moving a port with vMotion–and some external factors, such as network or storage failure occur–the port detaches on the source host. If the port is actively sending packets, it re-attaches immediately. For a silent host, the port remains detached until it sends some traffic.

Resolved Issues

Click the bug ID in the following table to access the Bug Search Tool and see additional information about the bug.

Bug ID	Description
CSCvt45927	In some cases Kni0 derives a higher metric as compared to Kni2. Kni0 IP can be derived from OpflexOdev. Because it has higher metrics than Kni2, SSH and pings to Kni0 do not work. Kni2 is used for load balancing and should not respond to pings/ssh.
CSCvt58389	When you have a single VMM deployed in two different VMware vCenters, one of the vCenters may show that the existing Cisco ACI Virtual Edge is not installed. This issue occurs when you have two different VMware vCenters in the same SSO domain and you uninstall all of the Cisco ACI Virtual Edge virtual machines for the VMM domain on one of the VMware vCenters. This issue occurs because the cisco-ave and cisco-ave-*vmm-domain* tags are removed on the other VMware vCenter for the Cisco ACI Virtual Edge virtual machines.
CSCvu01818	Symptoms: ■ There is a message in the Cisco APIC GUI saying that vleaf_elem has restarted several times and may not have recovered. ■ There are core files of the vleaf_elem process.

Known Issues

Where applicable, click the Bug ID in the following table to access the Bug Search Tool and see additional information about the bug.

Bug ID	Description
N/A	The Process vemfwd Always runs at 100% of CPU: The Cisco ACI Virtual Edge process vemfwd always runs at 100% of CPU. This is by design; Cisco ACI Virtual Edge always runs at a high CPU on one core to accommodate the Data Plane Development Kit (DPDK).

Cisco Confidential

Bug ID	Description
N/A	False Memory Fault in VMware vCenter: The Cisco ACI Virtual Edge VM can trigger a false memory fault in VMware vCenter. This is a cosmetic issue. For performance reasons, the latency sensitivity of the Cisco ACI Virtual Edge VM is set to high. This setting is known to trigger false positives in VMware vCenter. See the following article on the VMware website: Memory usage alarm triggers for certain types of Virtual Machines in ESXi 6.x (2149787).

N/A	Permission Denied for some Files on vem-support with Admin Login: When you log in as an administrator, you may be denied some files when you enter a vem-support command. However, you can use one of two methods to get the files:
	
	■ Generate a log bundle by entering a command in the Cisco APIC GUI:
	
	— Go to Admin > Import/Export > Export Policies > AVE/AVS Tech Support.
	
	— Right-click AVE/AVS Tech Support and choose Create AVS Tech Support.
	
	— In the Create AVE/AVS Tech Support dialog box, create a tech support export policy, which creates an archive file containing configuration information, logs, and diagnostic data that will help Cisco Technical Assistance Center (TAC) with troubleshooting and resolving a technical issue.
	
	■ Enter sudo mode and run the vem-support all command, as shown in the following example:
	
	`cisco-ave_192.0.2.162_AVE-Lag:~$ su`
	`Password:`
	`cisco-ave_192.0.2.162_AVE-Lag:admin# vem-support all`

N/A	Brief Delay Possible When Switching EPG from Native to AVE Mode: Changing the switching mode from Native to AVE (Cisco ACI Virtual Edge) on an EPG requires changing the underlying switching platform from regular VMware DVS to Cisco ACI Virtual Edge. It also requires moving all the associated ports from DVS to Cisco ACI Virtual Edge. This operation requires reprogramming of the port group associated with that EPG. That in turn requires a VMware vCenter operation. This operation may take a few seconds to complete and for ports to show up in forwarding state on the Cisco ACI Virtual Edge switching platform. The length of time depends on the VMware vCenter load as well as the number of endpoints that reside on the EPG that is being moved from Native to AVE mode.
N/A	LACP Policy Not Applied on Port Channel: When a Link Aggregation Control Protocol (LACP) policy is applied as a vSwitch policy for the VMM domain, the LACP policy is applied only to the VMware vSphere Distributed Switch (VDS) uplinks. However, it is not applied to the Cisco ACI Virtual Edge port channel. This is expected behavior. Cisco ACI Virtual Edge does not support LACP on its uplinks because VDS does not support it for its virtual Ethernet (vEth) interfaces. So, the VMM port channel policy is applied only for the VDS uplinks.

Cisco Confidential

Bug ID	Description
N/A	Fault Raised After Process Crash Regardless of When Crash Occurred: A fault for an invalid port group is raised on Cisco ACI Virtual Edge downgrades earlier than 2.0(1a). In Cisco ACI Virtual Edge Release 2.0(1a), a new port group, outside-cloud, is created for the Cisco ACI Virtual Edge VMM. When Cisco ACI Virtual Edge is downgraded to pre-2.0(1a) releases, the port group is removed from Cisco APIC but not from VMware vCenter. To avoid this fault, manually delete the port group outside-cloud from the VMware vCenter if you have an existing Cisco ACI Virtual Edge domain and you are downgrading from Cisco APIC 4.0(1h) or later.

Compatibility Information

Product	Supported Release	Information Location
VMware ESXI hypervisor	6.0 and later versions.	N/A
Cisco APIC	5.1(1h)	Cisco APIC and ACI Virtual Edge Support Matrix
Virtualization interoperability	5.1(1h)	Cisco ACI Virtualization Compatibility Matrix

Compatibility and Upgrade and Downgrade Considerations

Support Matrix

The *Cisco APIC and ACI Virtual Edge Support Matrix* is an interactive tool that enables you to choose an APIC version and view the compatible Cisco ACI Virtual Edge, vSphere, and compatible Cisco APIC versions.

Cisco ACI Virtual Edge Upgrade Method

You must use the Cisco ACI vCenter plug-in to upgrade Cisco ACI Virtual Edge. See the chapter “Cisco ACI Virtual Edge Upgrade” in the *Cisco ACI Virtual Edge Installation Guide, Release 3.0(x)* on Cisco.com for upgrade instructions.

Number of IP Addresses when Upgrading Cisco ACI Virtual Edge

If you use static or DHCP IP pools and want to upgrade Cisco ACI Virtual Edge, ensure that you have enough IP addresses. There must be more IP addresses in the static or DHCP pools than there are in the Cisco ACI Virtual Edge service VMs in the data center in VMware vCenter. Otherwise, the upgrade of the new Cisco ACI Virtual Edge will fail.

Scalability

Scalability information about Cisco ACI Virtual Edge is available in *Verified Scalability Guide for Cisco APIC.*

Cisco Confidential

Related Content

Cisco ACI Virtual Edge documentation includes release notes, an installation guide, and a configuration guide. The documents are available on the Cisco Application Policy Infrastructure Controller (APIC) website. Links to specific documents are in the following table:

Document	Description
Cisco ACI Virtual Edge Installation Guide, Release 3.0(x)	Provides installation, upgrade, and migration information for Cisco ACI Virtual Edge.
Cisco ACI Virtual Edge Configuration Guide, Release 3.0(x)	Provides configuration information for Cisco ACI Virtual Edge.
Cisco ACI Virtual Edge Health Status	Provides information for monitoring health of Cisco ACI Virtual Edge, including viewing and troubleshooting faults.

The Cisco Application Policy Infrastructure Controller (APIC) website also includes documentation for Cisco ACI and Cisco APIC. Documents include installation, upgrade, configuration, programming, scalability, and troubleshooting guides, technical references, release notes, and knowledge base (KB) articles, as well as other documentation. KB articles provide information about a specific use case or a specific topic.

You can watch videos that demonstrate how to perform specific tasks in the Cisco APIC on the Cisco ACI YouTube channel.

By using the "Choose a topic" and "Choose a document type" fields of the Cisco APIC documentation website, you can narrow down the displayed documentation list to make it easier to find the desired document.

Temporary licenses with an expiry date are available for evaluation and lab use purposes. They are strictly not allowed to be used in production. Use a permanent or subscription license that has been purchased through Cisco for production purposes. For more information, go to Cisco Data Center Networking Software Subscriptions.

Documentation Feedback

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

Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2020 Cisco Systems, Inc. All rights reserved.

Cisco Confidential