



Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.2(4)

If you have a private cloud, you might run part of your workload on a public cloud. However, migrating workload to the public cloud requires working with a different interface and learning different ways to set up connectivity and define security policies. Meeting these challenges can result in increased operational cost and loss of consistency.

To alleviate this issue, you can use the Cisco Cloud Application Policy Infrastructure Controller (APIC) to extend a Cisco Application Centric Infrastructure (ACI) Multi-Site fabric to Amazon Web Services (AWS) or Microsoft Azure public clouds. You can also mix AWS and Azure in your deployment.

This document describes the features, issues, and limitations for the Cisco Cloud APIC software. For the features, issues, and limitations for the Cisco APIC, see the [Cisco Application Policy Infrastructure Controller Release Notes, Release 4.2\(4\)](#). For the features, issues, and limitations for the Cisco ACI Multi-Site Orchestrator, see the [Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.2\(4\)](#).

For more information about this product, see [Related Documentation](#).

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
September 4, 2020	Release 4.2(4q) became available. This release adds the TCP MSS option; see the New Software Features section.
April 23, 2020	Release 4.2(4i) became available.

Contents

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

New Software Features

Feature	Description	Guidelines and Restrictions
TCP MSS option	<p>Beginning with release 4.2(4q), the TCP MSS option is available to configure the TCP maximum segment size (MSS). This value will be applied to all cloud router tunnel interfaces, including VPN tunnels toward the cloud and external tunnels toward the on-premises site or other cloud sites. For VPN tunnels toward the cloud, if the cloud provider's MSS value is less than the value that you enter in this field, then the lower value is used; otherwise, the value that you enter in this field is used.</p> <p>For more information, see the Cisco Cloud APIC for AWS Installation Guide, Release 4.2(x) and Cisco Cloud APIC for Azure Installation Guide, Release 4.2(x).</p>	None.

Changes in Behavior

There are no changes in behavior in this release.

Open Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 4.2(4) releases in which the bug exists. A bug might also exist in releases other than the 4.2(4) releases.

Bug ID	Description	Exists In
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	4.2(4i) and later

Open Issues

Bug ID	Description	Exists In
CSCvo93761	Changing an ExtEPG subnet prefix's mark from A to B will end up messing up BGP's prefixes in the CSR and will cause traffic loss.	4.2(4i) and later
CSCvp12535	With a larger number of Cloud APIC tenant EPGs and if the VRF configuration is pushed through the API in a single transaction, sometimes duplicate AWS resources are created.	4.2(4i) and later
CSCvp71964	Cannot access the serial console of the CSR virtual machine in Azure.	4.2(4i) and later
CSCvp92803	AWS EC2 or Azure virtual machines have been assigned secondary IP addresses, but are unreachable from other cloud sites.	4.2(4i) and later
CSCvp99474	No NSG is assigned when the cloud endpoint should be classified in the EPG.	4.2(4i) and later
CSCvq73867	A network interface in a Cloud APIC managed region in AWS or Azure matches the EP Selector in a cloud EPG, but the Security Group of that cloud EPG does not get attached to the network interface. Instead, the Security Group of another cloud EPG gets attached to the network interface.	4.2(4i) and later
CSCvq87116	A network interface in a Cloud APIC-managed AWS region matches the endpoint selector in a cloud EPG, but the security group for the cloud EPG does not get attached to the network interface.	4.2(4i) and later
CSCvr03104	If you try to deploy Cloud APIC to an unsupported region, then the Azure portal will allow you to select the region and will fail during deployment.	4.2(4i) and later
CSCvr48636	BGP Peer States on the Cloud APIC dashboard will show the peer states as "up" even while the actual BGP sessions are down, and control or data plane traffic is dropped.	4.2(4i) and later
CSCvs07094	A blank summary pane is shown after clicking on a filter name.	4.2(4i) and later
CSCvs20068	Selected filters are not added to the contract after saving.	4.2(4i) and later
CSCvs97247	Tenant admins do not have access to the EPG Communications screen.	4.2(4i) and later
CSCvt70799	A storage account created by Cisco Cloud APIC in Azure allows HTTP access.	4.2(4i) and later

Resolved Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCvs24183	Cloud CSRs are unreachable for some reason, but there is no indication in the Cloud APIC UI Dashboard to indicate unreachability.	4.2(4i)

Known Issues

Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 4.2(4) releases in which the bug exists. A bug might also exist in releases other than the 4.2(4) releases.

Bug ID	Description	Exists In
CSCvo06626	When a cloudExtEpg matches on a 0/0 network and has a bi-directional contract with two cloud EPGs, such as cloudEpg1 and CloudEpg2, this can result in inadvertent communication between endpoints in cloudEpg1 and cloudEpg2 without a contract between the two EPGs themselves.	4.2(4i) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	4.2(4i) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	4.2(4i) and later
CSCvq11780	Creating VPN connections fail with the "invalidCidr" error in AWS or the "More than one connection having the same BGP setting is not allowed" error in Azure.	4.2(4i) and later
CSCvq76039	When a fault is raised in the Cloud APIC, the fault message will be truncated and will not include the entire cloud message description.	4.2(4i) and later
CSCvr01341	REST API access to the Cloud APIC becomes delayed after deleting a tenant with scaled EPGs and endpoints. The client needs to retry after receiving the error.	4.2(4i) and later

Compatibility Information

This section lists the compatibility information for the Cisco Cloud APIC software. In addition to the information in this section, see the [Cisco Application Policy Infrastructure Controller Release Notes, Release 4.2\(4\)](#) and [Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.2\(4\)](#) for compatibility information for those products.

Compatibility Information

- Cloud APIC release 4.2(4) supports the following Cisco ACI product releases:
 - Cisco ACI Multi-Site Orchestrator, release 2.2(4)
 - Cisco APIC, release 4.2(4)
 - Cisco NX-OS for ACI-mode switches, release 14.2(4)
- Cloud APIC does not support IPv6.
- AWS does not support using iBGP between a virtual gateway and a customer gateway.
- Cloud APIC supports the following AWS regions:
 - **Asia Pacific (Mumbai)**
 - **Asia Pacific (Osaka- Local)**
 - **Asia Pacific (Seoul)**
 - **Asia Pacific (Singapore)**
 - **Asia Pacific (Sydney)**
 - **Asia Pacific (Tokyo)**
 - AWS GovCloud (US-Gov-West)
 - Canada (Central)
 - EU (Frankfurt)
 - EU (Ireland)
 - EU (London)
 - South America (São Paulo)
 - US East (N. Virginia)
 - US East (Ohio)
 - US West (N. California)
 - US West (Oregon)
- Cloud APIC supports the following Azure regions:
 - Australiacentral
 - Australiacentral2
 - Australiaeast
 - Australiasoutheast
 - Brazilsouth
 - Canadacentral
 - Canadaeast
 - Centralindia
 - Centralus
 - Eastasia
 - Eastus
 - Eastus2
 - Francecentral
 - Japaneast
 - Japanwest
 - Koreacentral
 - Koreasouth
 - Northcentralus
 - Northeurope
 - Southcentralus
 - Southeastasia
 - Southindia
 - Uksouth

Related Content

- Ukwest
- Westcentralus
- Westeurope
- Westindia
- Westus
- Westus2
- Cloud APIC supports the following Azure Government cloud regions:
 - US DoD Central
 - US DoD East
 - US Gov Arizona
 - US Gov Texas
 - US Gov Virginia

Related Content

See the [Cisco Cloud Application Policy Infrastructure Controller](#) page for the documentation.

See the [Cisco Application Policy Infrastructure Controller \(APIC\)](#) page for the verified scability, Cisco Application Policy Infrastructure Controller (APIC), and Cisco ACI Multi-Site Orchestrator (MSO) documentation.

The documentation includes installation, upgrade, configuration, programming, 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.

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

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.