Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.2(1)

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, bugs, and limitations for the Cisco Cloud APIC.

Note: Use this document with the *Cisco Application Policy Infrastructure Controller Release Notes, Release 4.2(1)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.2(1),* which you can view at the following location:

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

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

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

The *Cisco Application Centric Infrastructure Fundamentals* guide provides complete details about the Cisco ACI, including a glossary of terms that are used in the Cisco ACI.

For the verified scalability limits, see the *Verified Scalability Guide* for this release.

You can access these documents from the following website:

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

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.

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description

Date	Description
September 8, 2019	4.2(1i): Release 4.2(1i) became available.

Contents

This document includes the following sections:

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- New Software Features

New Software Features

The following table lists the new software features in this release:

Table 2 New Software Features

Feature	Description	Guidelines and Restrictions
Cloud site-to-cloud site connectivity	Cloud APIC supports cloud site-to-cloud site connectivity: ■ Between Amazon AWS public cloud sites and Microsoft Azure public cloud sites ■ Between Amazon AWS public cloud sites (Amazon AWS public cloud site-to-Amazon AWS public cloud site) ■ Between Microsoft Azure public cloud sites (Microsoft Azure public cloud site-to-Microsoft Azure public cloud site) For information, see the *Cisco Cloud APIC for Azure Installation Guide, Release 4.2(x)*.	None.
Microsoft Azure support	Cloud APIC can now be installed in and manage Microsoft Azure cloud endpoints. For information, see the *Cisco Cloud APIC for Azure User Guide*.	For the guidelines and restrictions, see the *Cisco Cloud APIC for Azure User Guide*.

Feature	Description	Guidelines and Restrictions
Support for Certificate Signing Request version 16.12	This release now supports Certificate Signing Request (CSR) version 16.12.	None.

Bugs

This section contains lists of open and resolved bugs and known behaviors.

- Open Bugs
- Resolved Bugs
- Known Behaviors

Open Bugs

This section lists the open bugs. 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(1) releases in which the bug exists. A bug might also exist in releases other than the 4.2(1) releases.

Table 3 Open Bugs in This Release

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 cType equation here.ontract between the two EPGs themselves.	4.2(1i) and later
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	4.2(1i) and later
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(1i) 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(1i) and later
CSCvp71964	Cannot access the serial console of the CSR virtual machine in Azure.	4.2(1i) and later
CSCvp71964	The serial console of the CSR virtual machine cannot be accessed in Azure.	4.2(1i) and later

Bug ID	Description	Exists In
CSCvp92803	AWS EC2 or Azure virtual machines have been assigned secondary IP addresses, but are unreachable from other cloud sites.	4.2(1i) and later
CSCvp99474	No NSG is assigned when the cloud endpoint should be classified in the EPG.	4.2(1i) and later
CSCvq38474	Sometimes, endpoint information is not removed from the Cloud APIC and the endpoint IP address will be displayed in the Cloud APIC GUI and in the contract rules.	4.2(1i) and later
CSCvq57152	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(1i) and later
CSCvq73108	For Cloud APIC in Azure, when Cloud APIC is undeployed in the home region, then connectivity to Cloud APIC or the Cloud APIC itself may be lost.	4.2(1i) 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(1i) 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(1i) and later
CSCvq86855	The search icon in the toolbar is disabled.	4.2(1i) 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(1i) and later
CSCvq94072	Endpoints are discovered in Cloud APIC (AWS EC2 or Azure VM) and the security groups associated with the virtual machine are linked in Cloud APIC. The security group determines where the endpoints will be synced on the other cloud sites. EPSync listens to websockets for changes in endpoint's security group, and in normal circumstances almost immediately syncs on other sites. However, due this bug, endpoints might not be synced immediately after the hcloudSecurityGroup has been associated in Cloud APIC.	4.2(1i) and later
CSCvq95878	The Network Interface in Azure is not attached the expected Security Group.	4.2(1i) and later

Bug ID	Description	Exists In
CSCvq97517	Undeploying a template from a Cloud site throws an error to delete the contextprofiles before deleting the VRF instance, which is getting deleted as part of the template undeployment. Given that the cloudCtxprofile configuration changes/deletion may not work after an import (if the names given to cloudCtxProfiles on Cloud APIC are not of the VRF-region format), brownfield import from Cloud APIC is not supported completely in the 4.2(1) release.	4.2(1i) 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(1i) and later
CSCvr06406	An internet-facing application load balancer is not reachable from the internet due to an incorrect configuration that should be rejected by a validation.	4.2(1i) and later
CSCvr13711	Information regarding the Azure cloud resources can be visible in the Cloud APIC even if the Azure resource has been removed.	4.2(1i) and later
CSCvr18729	The dashboard of Cloud APIC running in Azure will fail to show the number of BGP sessions that are up or down. The count will always be 0 even if the sessions are up and exchanging routes.	4.2(1i) and later

Resolved Bugs

This section lists the resolved bugs. 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.

Table 4 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvo77459	Instances in Cloud APIC-created VPCs with public IP addresses will not get public DNS host names.	4.2(1i)
CSCvo86768	IPSec tunnels between the cloud router and on-premises router is down.	4.2(1i)
CSCvo88454	CSRs are unreachable and no configurations get pushed to them.	4.2(1i)
CSCvo95354	When a CSR is terminated, the elastic the IP address for primary network interface is not released.	4.2(1i)
CSCvo96809	The GUI redirect banner message is not displayed on GUI on this release.	4.2(1i)
CSCvp07389	Cloud APIC GUI shows IPSec tunnels and BGP sessions to be down in the dashboard when some of the cloud CSR router IPSec tunnels toward the AWS virtual gateway are down.	4.2(1i)

Bug ID	Description	Fixed in
CSCvp10651	When a configuration export is done from a Cloud APIC and the configuration is imported with an atom replace into another Cloud APIC and an instance that is launched from a different AWS cloud formation template stack, the security rules for cloud APIC to Cloud Router (CSR 1Kv) communication may not be programmed correctly.	4.2(1i)
CSCvp11518	Inter-site communication between an on-premises VRF instance and a cloud VRF instance will stop in all CSRs when external connectivity is removed only from a few CSRs.	4.2(1i)
CSCvp80204	After creating a contract with no filters, the "Apply Filters Both Directions" setting may not have the value that was originally configured.	4.2(1i)
CSCvp96162	EndPoints stop syncing across sites and Cloud Endpoints will be unreachable from On-Prem. EPSync debug info from Swagger will show stale sites information instead of reflecting of the latest info.	4.2(1i)
CSCvq13212	If the user selected CSR throughput as 2.5/5/10G. The user would only get 2G throughput. (1G for internal/eth-1 interface and 1G for external/eth-2 interface)	4.2(1i)
CSCvp33535	AWS objects, such as S3 Buckets, Security Groups, and EC2 instances, do not include any relative tagging to identify that they were created by the Cloud APIC.	4.2(1i)

Known Behaviors

This section lists bugs that describe known behaviors. 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(1) releases in which the bug exists. A bug might also exist in releases other than the 4.2(1) releases.

Table 5 Known Behaviors in This Release

Bug ID	Description	Exists In
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	4.2(1i) 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(1i) 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(1i) and later

Supported Cisco ACI Releases

This section lists which releases of other Cisco ACI products are supported in this release of Cloud APIC.

Table 6 Supported Cisco ACI Releases

Product	Release
ACI Multi-Site Orchestrator	2.2(1)
APIC	4.2(1)
NX-OS	14.2(1)

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(1)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.2(1)* for compatibility information for those products, which you can view at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

- 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:
  - US East (Ohio)
  - US East (N. Virginia)
  - US West (N. California)
  - US West (Oregon)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Osaka- Local)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Canada (Central)
  - EU (Frankfurt)
  - EU (Ireland)
  - EU (London)
  - South America (São Paulo)
  - AWS GovCloud (US-West)
- 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
- Ukwest
- Westcentralus
- Westeurope
- Westindia
- Westus
- Westus2

Usage Guidelines

This section lists the usage guidelines for the Cisco Cloud APIC software. In addition to the information here, see the *Cisco Application Policy Infrastructure Controller Release Notes, Release 4.2(1)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.2(1)* for usage guidelines for those products, which you can view at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

- User passwords must meet the following criteria:
  - Minimum length is 8 characters
  - Maximum length is 64 characters
  - Fewer than three consecutive repeated characters
  - At least three of the following character types: lowercase, uppercase, digit, symbol
  - Cannot be easily guessed
  - Cannot be the username or the reverse of the username
  - Cannot be any variation of "cisco", "isco", or any permutation of these characters or variants obtained by changing the capitalization of letters therein

Related Documentation

For additional Cisco Cloud APIC documentation, go to the following website:

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

For information about the verified scability, Cisco Application Policy Infrastructure Controller (APIC), and Cisco ACI Multi-Site Orchestrator (MSO) documentation, go to the following website:

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

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.

New Documentation

This section lists the new product documents for this release.

- *Cisco Cloud APIC for Azure Installation Guide, Release 4.2(x)*

You can find these documents on the following website:

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

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.