Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.1(2)

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) public clouds.

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 4.1(2)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.1(2),* 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
June 11, 2019	4.1(2g): Release 4.1(2g) became available.

Date	Description
June 15, 2019	4.1(2g): In the Open Bugs section, added bug CSCvq13212.
June 27, 2019	In the Compatibility Information section, added the list of supported AWS regions.
August 29, 2019	4.1(2g): Moved bug CSCvo93492 from the Open Bugs section to the Resolved Bugs section.

Contents

This document includes the following sections:

- New and Changed Information
- Upgrade and Downgrade Information
- Bugs
- Supported Cisco ACI Releases
- Compatibility Information
- Usage Guidelines
- Related Documentation

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
AWS GovCloud support	Cisco Cloud APIC supports AWS GovCloud only for the us-gov-west region. For more information, see the *Cisco Cloud APIC Installation Guide, Release 4.1(x)*.	The us-gov-east region is not supported at this time.
Cloud APIC UI performance improvements	Cloud APIC UI performance improvements.	None.
Supported use cases	This release supports the following use cases: ■ Configuring a cloud-local L3Out for Cisco Cloud APIC ■ Configuring an L3Out for Cisco Cloud APIC through an on-premises fabric ■ Configuring shared services in Cisco Cloud APIC ■ Stretching a VRF in a Cisco Cloud APIC	See the specific use case documentation for the guidelines and restrictions for that use case.

Feature	Description	Guidelines and Restrictions
	■ Stretching an EPG in a Cisco Cloud APIC For more information, see the relevant use case documentation.	

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 4.1(2) releases in which the bug exists. A bug might also exist in releases other than the 4.1(2) 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 contract between the two EPGs themselves.	4.1(2g) and later
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	4.1(2g) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	4.1(2g) and later
CSCvo77459	Instances in Cloud APIC-created VPCs with public IP addresses will not get public DNS host names.	4.1(2g) and later
CSCvo86768	IPSec tunnels between the cloud router and on-premises router is down.	4.1(2g) and later
CSCvo88454	CSRs are unreachable and no configurations get pushed to them.	4.1(2g) and later

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.	4.1(2g) and later
CSCvo95354	When a CSR is terminated, the elastic the IP address for primary network interface is not released.	4.1(2g) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	4.1(2g) and later
CSCvo96809	The GUI redirect banner message is not displayed on GUI on this release.	4.1(2g) and later
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.	4.1(2g) and later
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.	4.1(2g) and later
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.	4.1(2g) 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.	4.1(2g) and later
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.	4.1(2g) and later
CSCvp80204	After creating a contract with no filters, the "Apply Filters Both Directions" setting may not have the value that was originally configured.	4.1(2g) and later
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.	4.1(2g) and later
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)	4.1(2g) 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
CSCvo14126	When the user switches the login domain type, the providers are not deleted.	4.1(2g)
CSCvo63243	There are timing issues with the fetchers.	4.1(2g)
CSCvo75384	When querying for some oper objects, the GUI or API might return duplicate objects.	4.1(2g)
CSCvo89150	Selecting Cloud APIC to manage more than 4 regions may not work properly. Deployments might have indeterministic issues.	4.1(2g)
CSCvo93492	CSRs in an infra VPC or user VPC creation in GovCloud regions may fail or may not work as expected. Note: Starting with Release 4.1(2), Cisco Cloud APIC supports AWS GovCloud only for the us-gov-west region. The us-gov-east region is not supported at this time.	4.1(2g)
CSCvo97314	The Cloud APIC dashboard shows that the BGP session between the cloud router and AWS virtual private gateway is down even though the IPSec tunnels are up.	4.1(2g)
CSCvp10859	Under scale conditions and with API failures due to underlying cloud throttling issues, multiple faults are generated to reflect the API failures, but some of them do not get cleared when the underlying faulty conditions are cleared.	4.1(2g)

Known Behaviors

This section lists bugs that describe known behaviors. There are no known behaviors for this release.

Supported Cisco ACI Releases

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

Table 5 Supported Cisco ACI Releases

Product	Release
ACI Multi-Site Orchestrator	2.1(2)
APIC	4.1(2)
NX-OS	14.1(2)

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 4.1(2)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.1(2)* 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)

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 4.1(2)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 2.1(2)* 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

There is no new documentation for this release.