Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 5.0(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, 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 5.0(1)*. For the features, issues, and limitations for the Cisco ACI Multi-Site Orchestrator, see the *Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.0(1)*.

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
May 14, 2020	Release 5.0(1k) became available.

Contents

New Software Features

Feature	Description	Guidelines and Restrictions
Support for AWS transit gateways on Cisco Cloud APIC	You can use an Amazon Web Services (AWS) transit gateway with Cisco Cloud APIC to automate connectivity between virtual private clouds. For more information, see *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway*.	See the section "AWS Transit Gateway Limitations and Restrictions" in *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway*.
Support for using filters to see specific information from AWS flow logs	You can use filters to see specific information derived by processing AWS flow logs. You can filter for a combination of source or destination IP address, port and protocol. For more information, see the section "Cisco Cloud APIC Statistics" in the *Cisco Cloud APIC for AWS User Guide 5.0(x)*.	■ You can define up to eight filters for a given AWS log group at the same time. ■ We recommend that you configure statistics filters using the Cisco Cloud APIC GUI.
Support for statistics collection for AWS transit gateway traffic	You can collect statistics for traffic to and from AWS transit gateways in Cisco Cloud APIC. For more information, see *Increasing Bandwidth Between VPCs by Using AWS Transit Gateway* and the statistics chapter of the *Cisco Cloud APIC for AWS User Guide 5.0(x)*.	You must enable collection when you set up Cloud APIC for AWS transit gateway, and you must create flow logs.

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 5.0(1) releases in which the bug exists. A bug might also exist in releases other than the 5.0(1) releases.

Bug ID	Description	Exists In
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	5.0(1k) and later
CSCvt52797	Some cloud-to-cloud tunnels are operationally down in external-facing CSRs.	5.0(1k) and later
CSCvt62217	A fault is seen in Cisco Cloud APIC after a config import, indicating that the CreateOrUpdate Virtual Network operation is failing with error code 'ReferencedResourceNotProvisioned'.	5.0(1k) and later
CSCvt72525	Upon increasing the scale of Certificate Signing Requests (CSRs), a create subnet request fails and a fault is raised in the Cisco Cloud APIC.	5.0(1k) and later
CSCvt77579	CSRs with unknown status are listed in the Inter-Site Connectivity screen.	5.0(1k) and later
CSCvt82672	A BGP faults show up in the Cloud APIC dashboard for multiple CSR BGP sessions.	5.0(1k) and later
CSCvt88137	Some of the TGW attachments to non-infra tenant VPCs might be deleted and not get recreated in the case of quickly enabling, disabling, and re-enabling the hub network to the CloudCtxProfile.	5.0(1k) and later
CSCvu02115	If CSRs are undeployed and redeployed in a non-Cloud APIC home region, this results in a delete and re-add of the infra VPC. If there are other CloudContextProfiles (user tenant VRF tables) pointing to the hub network (transit gateway), then when the CSRs are redeployed, traffic from the transit gateway to a CSR may be dropped. In this case, the transit gateway will remain undeleted because the user tenant VPC is still using the transit gateway. The traffic drop might occur because when the infra VPC is redeployed, it might get a different set of CIDRs allocated to it.	5.0(1k) and later
CSCvu06450	In the Cloud APIC home region, if CSRs are undeployed and redeployed, there will be stale entries in the CSR route tables. If you reach the maximum route table entries limit because of these stale entries, any new route table entries will fail to get programmed in the cloud, and a VPN connection related to those entries will remain down. There will be fault raised for route table entries that failed to get programed in the cloud.	5.0(1k) and later
CSCvu15350	When using shared services with Cisco Intersite, after deleting the remote site VPC's secondary CIDR contract, the contract's entry is retained in the routing table. No change in traffic behavior is expected. The policy will prevent the traffic from flowing.	5.0(1k) and later

Bug ID	Description	Exists In
CSCvu17097	Inter tenant shared services traffic is impacted after tenant delete and add.	5.0(1k) 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
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.	5.0(1k)
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.	5.0(1k)
CSCvp71964	Cannot access the serial console of the CSR virtual machine in Azure.	5.0(1k)
CSCvp92803	AWS EC2 or Azure virtual machines have been assigned secondary IP addresses, but are unreachable from other cloud sites.	5.0(1k)
CSCvp99474	No NSG is assigned when the cloud endpoint should be classified in the EPG.	5.0(1k)
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.	5.0(1k)
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.	5.0(1k)
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.	5.0(1k)
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.	5.0(1k)
CSCvs07094	A blank summary pane is shown after clicking on a filter name.	5.0(1k)
CSCvs20068	Selected filters are not added to the contract after saving.	5.0(1k)
CSCvs49001	The AWS security group rule's description field is empty. This is a cosmetic bug.	5.0(1k)
CSCvt70799	A storage account created by Cisco Cloud APIC in Azure allows HTTP access.	5.0(1k)

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 5.0(1) releases in which the bug exists. A bug might also exist in releases other than the 5.0(1) 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.	5.0(1k) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	5.0(1k) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	5.0(1k) 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.	5.0(1k) 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.	5.0(1k) 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.	5.0(1k) 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 5.0(1)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.0(1)* for compatibility information for those products.

- Cloud APIC release 5.0(1) supports the following Cisco ACI product releases:
  - Cisco ACI Multi-Site Orchestrator, release 3.0(1)
  - Cisco APIC, release 5.0(1)
  - Cisco NX-OS for ACI-mode switches, release 15.0(1)
- 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
  - 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