Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 5.2(1)

Introduction

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 cloud provider 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. Cisco Cloud Application Policy Infrastructure Controller (APIC) can be used to solve the these problems by extending a Cisco 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 5.2(1). For the features, issues, and limitations for the Cisco Multi-Site Orchestrator, see the Cisco Multi-Site Orchestrator Release Notes, Release 3.3(1).

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
October 8, 2021	Removed mention of the supported Cisco ACI product releases. Cloud APIC does not depend on any specific Cisco ACI product releases.
August 13, 2021	Removed open issues CSCvy30852, CSCvy07759, and CSCvy41881. Moved open issues CSCvy12722, CSCvy28896, CSCvy28890, and CSCvw48190 to known issues.
August 6, 2021	Release 5.2(1h) became available. Added known issue CSCvz20282.
June 11, 2021	Added open issue CSCvy14025, CSCvy50245, and CSCvy42684.
June 7, 2021	Release 5.2(1g) became available.

New Software Features

Feature	Description
Support for importing existing Azure brownfield cloud VNets into Cisco Cloud APIC	This release provides support for importing existing brownfield Azure cloud VNets (VNets that were not configured through Cisco Cloud APIC) into Cisco Cloud APIC. For more information, see Importing Existing Brownfield Azure Cloud VNets Into Cisco Cloud APIC.

Feature	Description
Support for Amazon Web Services (AWS) Transit Gateway Connect in Cisco Cloud APIC	Support for Amazon Web Services (AWS) Transit Gateway Connect in Cisco Cloud APIC. By using the AWS Transit Gateway Connect feature: • Only one AWS Transit Gateway is deployed per hub network per region • Equal-cost multi-path (ECMP) routing is enabled to all the CSRs in a region For more information, see Cisco Cloud APIC for AWS Installation Guide, Release 5.2(x).
Support for manual upgrades for CSRs, independent from the Cisco Cloud APIC upgrades	You can manually trigger an upgrade of the CSRs, independent of the Cisco Cloud APIC upgrades. Prior to release 5.2(1), the CSRs were upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC. For more information, see: Cisco Cloud APIC for AWS Installation Guide, Release 5.2(x) Cisco Cloud APIC for Azure Installation Guide, Release 5.2(x)
Support for communication with an external site from regions without a CSR in AWS	You can have communication with an external site in regions without a CSR in AWS. For more information, see Cisco Cloud APIC for AWS User Guide, Release 5.2(x).
Support for private IP addresses for CSR interfaces and Cisco Cloud APIC in AWS	You can assign a private IP address to a Cisco Cloud Services Router (CSR) and Cisco Cloud APIC in AWS. For more information, see: Cisco Cloud APIC for AWS Installation Guide, Release 5.2(x) Cisco Cloud APIC for AWS User Guide, Release 5.2(x)
Support for VNet peering across Azure Active Dirtectories (ADs) to allow spoke VNets to be deployed in different subscriptions in different Azure ADs	Support is now available for VNet peering across Azure ADs, so spoke VNets can be deployed in different subscriptions in different Azure ADs. In releases prior to release 5.2(1), you must deploy the infra (hub) and spoke VNets in the same Azure AD, but you can deploy the infra and spoke VNets in different subscriptions within the same Azure AD. For more information, see Configuring VNet Peering for Cloud APIC for Azure.

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 5.2(1) releases in which the bug exists. A bug might also exist in releases other than the 5.2(1) releases.

Bug ID	Description	Exists in
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	5.2(1g) and later
CSCvu64277	Stats seen on Cisco Cloud APIC are sometimes not in sync with Azure stats.	5.2(1g) and later

Bug ID	Description	Exists in
CSCvu66521	In the "Cloud Resources" section of the GUI, the names displayed in the "Name" column are not the same as the name of resources on the cloud. These are showing the Cloud APIC object names.	5.2(1g) and later
CSCvu72354	Adding an EPG endpoint selector fails with an error message saying the selector is already attached.	5.2(1g) and later
CSCvu78074	Route nextHop is not set to the redirect service node specified in the service graph.	5.2(1g) and later
CSCvv32664	When the CSR bandwidth needs to be increased, the user needs to undeploy all the CSRs in all the regions and redeploy with the desired bandwidth, which can cause traffic loss.	5.2(1g) and later
CSCvx16601	When the "AllowAll" flag is enabled on a service device such as a native load balancer or on the logical interface of a third party device, it is possible that to see some specific rules apart form a rule that allows all traffic from any source to any destination.	5.2(1g) and later
CSCvx67107	Third party firewalls and load balancers are not shown in the topology view.	5.2(1g) and later
CSCvy06610	The eventmgr crashes when handling a fault triggered by a new cloud account.	5.2(1g) and later
CSCvy14025	The Next Hop Routing entry missing in the ER gateway route table for redirecting the traffic going from the consumer to the provider EPG to a service device.	5.2(1g) and later
CSCvy42684	Importing a configuration into Cloud APIC 5.2 displays the following error: maximum buffer length exceeded.	5.2(1g) and later
CSCvy50245	Tunnels are down on one of the CSRs after terminating the CSR instance from the AWS Portal.	5.2(1g) 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
CSCvt52797	Some cloud-to-cloud tunnels are operationally down in external-facing CSRs.	5.2(1g)
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.	5.2(1g)
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.	5.2(1g)
CSCvu72020	The GUI cannot properly display the service graph association in EPG communication, due to a mismatched tenant name.	5.2(1g)
CSCvw21595	When deploying a service graph on Cisco Cloud APIC, faults F3764 and F3763 appear. The ALB is deployed on AWS, but the security group is not.	5.2(1g)

Bug ID	Description	Fixed in
CSCvw27056	A CSR's management Interface is down or inaccessible through SSH.	5.2(1g)
CSCvw36844	No UDR entries will be present if extEPG is consumer on a graph on which REDIRECT is enabled.	5.2(1g)
CSCvw57813	After a Cisco Cloud APIC upgrade, all of the Cloud Service Routers will be upgraded in two batches, even and odd. State of the cuurent batch of CSRs that are upgraded are persisted in the Cisco Cloud APIC. When the Cisco Cloud APIC is rebooted mid-upgrade of the CSRs, the state information of the upgrade will be lost. This results in the halt of the CSR upgrade process.	5.2(1g)
CSCvw58899	After a configuration import, an fvCtx managed object may have a different vrfIndex value. This would cause the configuration in the CSRs to be modified, thereby leading to traffic drops.	5.2(1g)
CSCvw60314	After upgrading one of the Cloud APIC sites to the 5.2(1) release, intersite traffic loss occurs. This is due to intersite IPSec tunnels being deleted and recreated by MSO. Traffic recovers in about 30 to 40 minutes after the tunnels are recreated.	5.2(1g)
CSCvx06278	Rules in the firewall may be missing for traffic that has a cloud site-external EPG as the consumer/source to a provider EPG/destination when redirect is enabled in the cloud graph.	5.2(1g)

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 5.2(1) releases in which the bug exists. A bug might also exist in releases other than the 5.2(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.	5.2(1g) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	5.2(1g) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	5.2(1g) 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.	5.2(1g) 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.	5.2(1g) 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.	5.2(1g) and later
CSCvu05329	The Ctx Oper managed object is not deleted after the attachment is deleted.	5.2(1g) and later

Bug ID	Description	Exists in
CSCvu81355	Traffic gets dropped after downgrading to the 5.0(1) release. Cloud Services Router has incompatible configurations due to an issue with reading configurations using SSH.	5.2(1g) and later
CSCvu88006	On the Dashboard, fewer VNet peerings are shown than expected.	5.2(1g) and later
CSCvv81647	When an invalid Cloud Services Router license token is configured after initially configuring a valid token, the Cloud Services Router fails the license registration and keeps using the old valid token. This failure can only be found from the CSR event log.	5.2(1g) and later
CSCvw05821	Redirection and UDR does not take effect when traffic coming through an express route and destined to a service end point is redirected to a native load balancer or firewall.	5.2(1g) and later
CSCvw07392	Inter-site VxLAN traffic drops for a given VRF table when it is deleted and re-added. Packet capture on the CSR shows "Incomplete Adjacency" as follows: Punt 1 Count Code Cause 1 10 Incomplete adjacency <<<<<<< Drop 1 Count Code Cause 1 94 Ipv4NoAdj	5.2(1g) and later
CSCvw07781	There is complete traffic loss for 180 seconds.	5.2(1g) and later
CSCvw24376	Inter region traffic is black-holed after the delete trigger for contracts/filter. It was observed that the TGW entry pointing to the remote region TGW is missing for the destination routes. On further debugging it was found that post delete trigger as part of re-add flow, when a describe call is sent to AWS got a reply with the state of this entry as "active" because of which a new create request is not being sent.	5.2(1g) and later
CSCvw39814	Infra VPC subnet route table entry for 0.0.0.0/0 route with TGW attachment as nh, is left as a stale entry upon being undeployed. There is no functional impact. Upon being redeployed, this entry is updated with the correct TGW attachment ID as nh.	5.2(1g) and later
CSCvw40737	SSH to a virtual machine's public IP address fails, despite the NSG allowing the traffic inbound. SSH to the private IP address of the virtual machine from within the VNet works.	5.2(1g) and later
CSCvw40818	After upgrading Cloud APIC, the Cloud Services Routers will be upgraded in two batches. The even set of CSRs are triggered for upgrade first. AFTER their upgrade is complete and all of the even CSRs are datapathReady, only then the odd set of CSRs will be triggered for upgrade. When even one of the upgrade of the even CSRs fail and they don't become datapathReady, the odd set of CSRs will not be triggered for upgrade. This is the behavior followed to avoid any traffic loss.	5.2(1g) and later
CSCvw48190	When Cloud APIC is restart, the VPN connection from a tenant's VNets will get deleted and re-created, one by one. This can be seen in the Azure activity logs. It should not impact traffic, as all connections are not deleted at the same time.	5.2(1g) and later
CSCvw49898	When the downgrading from the 5.2(1) release to the 5.0(2) release, traffic loss is expected until all of the CSRs are downgraded back to the 17.1 release. The traffic loss occurs because when the CSRs are getting downgraded to the 17.1 release, the CSR NIC1s will be in the backendPools and traffic from the spokes will still be forwarded to the native load balancer. The traffic gets blackholed until the CSRs get fully programmed with all the configurations in the 17.1 release.	5.2(1g) and later

Bug ID	Description	Exists in
CSCvw50918	Upon downgrading Cloud APIC, VPN connections between Cloud APIC and the cloud (AWS/Azure VPN gateway) will be deleted and re-created, causing traffic loss. Traffic loss is based on how quickly the VPN connections are deleted and re-created in AWS due to AWS throttling.	5.2(1g) and later
CSCvw51544	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	5.2(1g) and later
CSCvw55088	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	5.2(1g) and later
CSCvx91010	When TGW Connect is disabled, traffic loss is observed for about 8 minutes.	5.2(1g) and later
CSCvy10936	Downgrading Cisco Cloud APIC from release 5.2(1) to 5.1(2) may cause CSRs to not be downgraded. The CSR release for 5.2(1) is 17.3.2, and the CSR version for release 5.1(2) is 17.3.1. After the Cisco Cloud APIC downgrade, the CSR version should be downgraded to 17.3.1, but it will not happen due to this bug.	5.2(1g) and later
CSCvy12722	Loss of traffic between a cloud and Cisco ACI On-Premises deployment.	5.2(1g) and later
CSCvy13369	After upgrading AWS, infra vPC peering does not get deleted.	5.2(1g) and later
CSCvy19286	There is traffic loss after downgrading from 5.2(1) to 5.1(2).	5.2(1g) and later
CSCvy28890	There is a loss in SSH connectivity to the Cisco Cloud APIC across reboots. But, after a few minutes, the connection should come back and users will be able to SSH in to the Cisco Cloud APIC again.	5.2(1g) and later
CSCvy28896	There is an increase in the connector's memory utilization. All of the CSR workflows rerunning might happen even after the setup is in the steady state.	5.2(1g) and later
CSCvy30314	After upgrading the Cisco Cloud APIC, on the TGW route tables, the default route (0.0.0.0/0) does not point to infra VPC attachment or is missing. In this case, traffic intended to get forwarded to the CSR will be dropped or forwarded to an invalid next-hop.	5.2(1g) and later
CSCvy33435	There is intersite traffic loss when TGW Connect is enabled.	5.2(1g) and later
CSCvy34180	Cloud Intersite traffic is dropped due to the CSR in the cloud site not advertising the EVPN routes.	5.2(1g) and later
CSCvy45517	The Cisco Cloud APIC GUI shows the total allowed count for CtxProfile, VRF (fvCtx), EPGs, and contracts. These numbers have been validated only for Azure-based deployments. For AWS deployments, the numbers supported are much lower.	5.2(1g) and later
CSCvz20282	An upgrade to or downgrade from the Cloud APIC 5.2(1g) release to any release while using " Ignore Compatibility Check: no" will fail. The following fault is raised: " The upgrade has an upgrade status of Failed Due to Incompatible Desired Version."	5.2(1g) 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 5.2(1) and Cisco Multi-Site Orchestrator Release Notes, Release 3.3(1) for compatibility information for those products.

- Cloud APIC release 5.2(1) is compatible with Multi-Site Orchestrator, release 3.3(1) or above.
- 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 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