Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 25.0(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 appropriate Cisco Application Policy Infrastructure Controller Release Notes. For the features, issues, and limitations for the Cisco Multi-Site Orchestrator, see the appropriate Cisco Multi-Site Orchestrator Release Notes.

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	Added compatibility information with Nexus Dashboard Orchestrator (NDO).
September 21, 2021	Release 25.0(1c) became available. Beginning with release 25.0(1c), the release numbering has changed for Cisco Cloud APIC. The sequential order of releases for Cisco Cloud APIC is as follows: • 4.1(x) (support for AWS only) • 4.2(x) • 5.0(x) • 5.1(x) • 5.2(x) • 25.0(x)

New Software Features

Feature	Description
Support for Google Cloud with Cisco Cloud APIC	Support is available for Google Cloud with Cisco Cloud APIC. As part of the support for Google Cloud with Cisco Cloud APIC, the following are supported: • Support for external connectivity from Google Cloud to other external sites • Support for configuring routing and security policies separately For more information, see: • Cisco Cloud APIC for Google Cloud User Guide, Release 25.0(x) • Cisco Cloud APIC for Google Cloud Installation Guide, Release 25.0(x)
Support for external connectivity from AWS or Azure to other external sites	Support is available for external connectivity from AWS or Azure to other external sites. For more information, see: • Cisco Cloud APIC for AWS Installation Guide, Release 25.0(x) • Cisco Cloud APIC for Azure Installation Guide, Release 25.0(x) • Cisco Cloud APIC for AWS User Guide, Release 25.0(x) • Cisco Cloud APIC for Azure User Guide, Release 25.0(x)
Support for configuring routing policies separately for AWS or Azure when configuring for external connectivity	Support is available for configuring routing policies separately for AWS or Azure, independent of security policies, between internal and external VRFs when configuring for external connectivity. For more information, see: • Cisco Cloud APIC for AWS Installation Guide, Release 25.0(x) • Cisco Cloud APIC for Azure Installation Guide, Release 25.0(x) • Cisco Cloud APIC for AWS User Guide, Release 25.0(x) • Cisco Cloud APIC for Azure User Guide, Release 25.0(x)
Support for Prometheus Node Exporter on Cisco Cloud APIC	The Prometheus Node Exporter is supported on Cisco Cloud APIC. For more information, see: • Cisco Cloud APIC for AWS User Guide, Release 25.0(x) • Cisco Cloud APIC for Azure User Guide, Release 25.0(x) • Cisco Cloud APIC for Google Cloud User Guide, Release 25.0(x)

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 25.0(1) releases in which the bug exists. A bug might also exist in releases other than the 25.0(1) releases.

Bug ID	Description	Exists in
CSCvy07759	CSR upgrade banner is not updated after the upgrade is complete.	25.0(1c) and later
CSCvz31331	APIC REST APIs allows to create a cloudEPg that refers to an external VRF in the infra tenant. This is disabled when configuring through the GUI and should be blocked in the backend as well.	25.0(1c) and later
CSCvz62225	When you scale up the number of CSRs or routers per region, some of the configurations may be missing on the newly created CSR. This issue happens randomly on the newly created CSRs, in this case tunnels or BGP sessions on the new CSRs may be down due to missing configuration.	25.0(1c) and later
CSCvz66172	Unable to get public IP addresses assigned to non Gig1 Interfaces of CSR. Gig1 Interface gets a public IP addresses.	25.0(1c) and later
CSCvz47166	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
CSCvy97972	Cisco Cloud APIC in this release limits the number of regions where we can deploy the hubnetwork in order to establish external connectivity. When you attempt to deploy/configure hubnetwork in more than four regions, the configuration will be rejected with the following error: Invalid Configuration CT_INTNETWORK_REGION_MAXIMUM: At present, there can be at most 4 cloudRegionName in cloudtemplateIntNetwork uni/tn-infra/infranetwork-default/intnetwork-default; current count = <total-hubnetwork-regions-attempted>	25.0(1c) and later
CSCvz17160	Customers are restricted to shorter key value pairs than they need to be.	25.0(1c) and later
CSCvz21771	VPN tunnels may not come up when the Cisco Cloud APIC configuration is posted via XML interface. This problem won't be seen/encountered when we use the Cisco Cloud APIC UI.	25.0(1c) and later
CSCvz26752	The Cisco Cloud APIC UI may display empty entries when routes are leaked to or from non-existing VRFs. For example, this is seen when a VRF is deleted and another VRF leaked one or more routes to that deleted VRF. The UI may indicate an empty value under the VRF to which the routes are leaked.	25.0(1c) and later
CSCvz41009	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
CSCvz43324	The Cloud APIC REST APIs allow you to create a cloud EPG that refers to an External VRF in the infra tenant. This is disabled on the UI and should be disabled through the REST API as well.	25.0(1c) and later

Bug ID	Description	Exists in
CSCvz46464	There may be some traffic loss encountered when Cisco Cloud APIC is rebooted and a new configuration is imported. The new configuration takes time to deploy as we achieve eventual consistency.	25.0(1c) and later
CSCvz47232	When we delete any configuration, it takes time to reach eventual consistency and clean up all the resources on the cloud. This may not happen when Cisco Cloud APIC is rebooted while the delete/cleanup operation is underway. A few resources may remain on the cloud if Cisco Cloud APIC is rebooted while the cleanup is in progress.	25.0(1c) and later
CSCvy89617	Cloud routers may not get created if external network objects are not configured. External network configuration is required for configuring cloud routers.	25.0(1c) and later
CSCvy94328	overlay-1 VRF in tenant "infra" shows up as one of the VRFs with which an external network is associated. However, Cisco Cloud APIC does not allow overlay-1 VRF to be associated with any external network. In this release, overlay-1 VRF shows up alongside other VRFs to be associated with an external network. It has no functional impact, but it gives an incorrect impression that we have a external network associated with overlay-1 VRF. This external network name is set to default and there are no other objects/MOs for this external network configured.	25.0(1c) and later
CSCvz38067	Incorrect DNS server is configured on Cisco Cloud APIC with Google Cloud. Though this is not directly used when deploying Cisco Cloud APIC with Google Cloud, an incorrect IP address is configured.	25.0(1c) and later
CSCvz11574	The cloud VRF egress route table is missing the route for 0.0.0.0/0 via the Internet Gateway (IGW), which leads to issues with ssh for VMs in the cloud VRF.	25.0(1c) and later
CSCvz52773	When performing a Cisco Cloud APIC upgrade (but not also performing a CSR upgrade), before the upgrade is finished and when the Cisco Cloud APIC is reconciling the CSR configurations, if you delete certain configurations and add the same configurations back (for example, if you delete a VRF and add the VRF back), a traffic drop may happen. Eventually it should recover.	25.0(1c) and later
CSCvz39389	After a clean reboot of Cisco Cloud APIC and an import of the configuration, a CSR might take around 45 minutes to re-establish the datapath readiness.	25.0(1c) and later
CSCvz40326	Routes to and from overlay-2 VRF may not be configured in the cloud deployment.	25.0(1c) and later
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	25.0(1c) and later
CSCvu64277	Stats seen on Cisco Cloud APIC are sometimes not in sync with Azure stats.	25.0(1c) and later
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.	25.0(1c) and later
CSCvu72354	Adding an EPG endpoint selector fails with an error message saying the selector is already attached.	25.0(1c) and later
CSCvu78074	Route nextHop is not set to the redirect service node specified in the service graph.	25.0(1c) 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.	25.0(1c) and later

Bug ID	Description	Exists in
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.	25.0(1c) and later
CSCvy06610	The eventmgr crashes when handling a fault triggered by a new cloud account.	25.0(1c) and later
CSCvy42684	Importing a configuration into Cloud APIC 5.2 displays the following error: maximum buffer length exceeded.	25.0(1c) 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
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.	25.0(1c)
CSCvy50245	Tunnels are down on one of the CSRs after terminating the CSR instance from the AWS Portal.	25.0(1c)
CSCvx67107	Third party firewalls and load balancers are not shown in the topology view.	25.0(1c)

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 25.0(1) releases in which the bug exists. A bug might also exist in releases other than the 25.0(1) releases.

Bug ID	Description	Exists in
CSCvz49747	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
CSCvy77233	Routes for subnets that are not yet configured in Google Cloud may become visible on an external device. When you configure routes to be advertised to an external device, but don't actually configure subnets in the cloud that you intend to advertise the routes for, those routes are still advertised. Remote router may see routes that are advertised even when the subnets are not yet configured. The traffic will get dropped because the subnets are not actually configured.	25.0(1c) and later

Bug ID	Description	Exists in
CSCvx98260	When delete followed by add operations of tenant or other resources (such as VPCs and contracts) are done within a short span of time, it is possible that the resource deployment in Google Cloud may get out of sync with the configuration on Cisco Cloud APIC. The likelihood of this happening is directly proportionate to the scale of configuration and how quickly the operations are done. We may see resources either not created or not deleted on Google Cloud to match the user configuration on Cisco Cloud APIC.	25.0(1c) and later
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.	25.0(1c) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	25.0(1c) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) and later
CSCvu05329	The Ctx Oper managed object is not deleted after the attachment is deleted.	25.0(1c) and later
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.	25.0(1c) and later
CSCvu88006	On the Dashboard, fewer VNet peerings are shown than expected.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) 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	25.0(1c) and later
CSCvw07781	There is complete traffic loss for 180 seconds.	25.0(1c) and later

Bug ID	Description	Exists in
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.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) and later
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.	25.0(1c) and later
CSCvw51544	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	25.0(1c) and later
CSCvw55088	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	25.0(1c) and later
CSCvx91010	When TGW Connect is disabled, traffic loss is observed for about 8 minutes.	25.0(1c) 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.	25.0(1c) and later
CSCvy12722	Loss of traffic between a cloud and Cisco ACI On-Premises deployment.	25.0(1c) and later
CSCvy13369	After upgrading AWS, infra vPC peering does not get deleted.	25.0(1c) and later
CSCvy19286	There is traffic loss after downgrading from 5.2(1) to 5.1(2).	25.0(1c) and later

Bug ID	Description	Exists in
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.	25.0(1c) 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.	25.0(1c) 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.	25.0(1c) and later
CSCvy33435	There is intersite traffic loss when TGW Connect is enabled.	25.0(1c) and later
CSCvy34180	Cloud Intersite traffic is dropped due to the CSR in the cloud site not advertising the EVPN routes.	25.0(1c) 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.	25.0(1c) 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."	25.0(1c) 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 appropriate Cisco Application Policy Infrastructure Controller Release Notes and Cisco Multi-Site Orchestrator Release Notes for compatibility information for those products.

- Cloud APIC release 25.0(1) is compatible with Cisco Nexus Dashboard Orchestrator, release 3.(5).
- 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)
    - EU (Stockholm)
    - 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
    - Germanywestcentral
    - Japaneast
    - Japanwest
    - Koreacentral
    - Koreasouth
    - Northcentralus
    - Northeurope
    - Norwayeast
    - Southafricanorth
    - Southcentralus

    - Southeastasia
    - Southindia
    - Switzerlandnorth
    - Uaenorth
    - 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
- Cloud APIC supports all Google Cloud regions.

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