Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 5.1(2)

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 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 5.1(2). For the features, issues, and limitations for the Cisco ACI Multi-Site Orchestrator, see the Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.1(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
February 12, 2021	Release 5.1(2g) became available. Added the open and known issues and new software features for this release. From the Open Issues section, removed bug CSCvw51219. This bug was erroneously included. Moved bug CSCvw49898 from the Open Issues table to the Known Issues table.
January 20, 2021	In the Open Issues section, added bug CSCvx06278.
November 27, 2020	Release 5.1(2e) became available.

New Software Features

Feature	Description
Allow All Traffic option is available for third-party firewalls and Azure network load balancers	Beginning with release 5.1(2g), the **Allow All Traffic** option is available for third-party firewalls and Azure network load balancers deployed as pass-through devices on a redirect-enabled service graph.
IP-based rules for inter-VRF contracts in the same VNet	Beginning with release 5.1(2g), if two EPGs have a contract and are in the same VNet but belong to different VRFs, IP-based rules are now used to enable communication between those hosted VRFs in that VNet. Prior to release 5.1(2g), if two EPGs had a contract and were in the same VNet, but belonged to different VRFs, ASG-based rules were used to enable communication between those hosted VRFs in that VNet.
Ability to map network security groups (NSGs) to	NSGs are now mapped to subnets instead of EPGs. Prior to release 5.1(2), NSGs were

Feature	Description
subnets	mapped to EPGs. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Support for non-Cisco ACI on-premises destinations over express route	Support is now available to represent non-Cisco ACI on-premises destinations that are reachable over an Azure express route as site-ext EPGs. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Support for 40G throughput with Cisco Cloud Services Routers by increasing the maximum number of supported CSRs to 8	Up to 40G throughput is supported by version 17.3 Cisco cloud services routers. The maximum throughput for a CSR depends on the instance type. 40G throughput can be achieved because the maximum number of CSRs supported per region has been increased from 4 to 8. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x) the Cisco Cloud APIC for Azure Installation Guide, Release 5.1(x).
Cloud services support using cloud service EPGs	You can now automate network segmentation and security policies for cloud native services and third-party services using the new cloud service EPG. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Support for assigning only a private IP address to access a Cisco Cloud Services Router	Assigning a public IP address to the Cloud APIC and Cisco Cloud Services Router (CSR) is now optional. Cloud APIC and Cisco CSRs can now operate with only a private IP address. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Restricting access using restricted security domains	Security has been enhanced for a user by restricting access using restricted security domains. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Support for third-party load balancers	A third party load-balancer is a non-cloud native Layer 4 to Layer 7 services load balancer. You can now use third-party load balancers for Azure deployments. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Layer 4 to Layer 7 services redirect support for cloud native and third-party services	The Layer 4 to Layer 7 service redirect feature for Cisco Cloud APIC now supports cloud native and third-party services. For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.1(x).
Support for Layer 4 to Layer 7 services redirect and non-redirect service graphs for site-ext EPGs over an express route	You can now use Layer 4 to Layer 7 services redirect and non-redirect service graphs for site-ext EPGs over an express route.
Support for segmentation using multiple VRF tables per VNet	Segmentation is now supported using multiple VRF tables per Azure virtual network (VNet).
Support for custom naming for Layer 4 to Layer 7 service deployments	You can now provide custom names to cloud resources, such as network load balancers, application load balancers, and device application security groups.

Changes in Behavior

- Beginning with release 5.1(2), VNet peering is enabled by default at the global level and cannot be disabled. Prior to release 5.1(2), you could enable and disable VNet peering at the global level through the First Time Setup window.

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 5.1(2) releases in which the bug exists. A bug might also exist in releases other than the 5.1(2) releases.

Bug ID	Description	Exists in
CSCvo30542	TACACS monitoring of the destination group is not supported through the GUI.	5.1(2e) and later
CSCvt52797	Some cloud-to-cloud tunnels are operationally down in external-facing CSRs.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) and later
CSCvu64277	Stats seen on Cisco Cloud APIC are sometimes not in sync with Azure stats.	5.1(2e) 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.	5.1(2e) and later
CSCvu72020	The GUI cannot properly display the service graph association in EPG communication, due to a mismatched tenant name.	5.1(2e) and later
CSCvu72354	Adding an EPG endpoint selector fails with an error message saying the selector is already attached.	5.1(2e) and later
CSCvu78074	Route nextHop is not set to the redirect service node specified in the service graph.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) 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	5.1(2e) and later

Bug ID	Description	Exists in
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.	5.1(2e) 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.	5.1(2e) and later
CSCvw27056	A CSR's management Interface is down or inaccessible through SSH.	5.1(2e) and later
CSCvw36844	No UDR entries will be present if extEPG is consumer on a graph on which REDIRECT is enabled.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) and later
CSCvw48256	The primary CIDR of CtxProfile defines the VPC/VNet and hence cannot be changed/modified without deleting the vPC. For example, in the AWS console, you cannot simply modify or delete the primary CIDR. You must delete the entire vPC. However, in the Cisco ACI policy, a configuration post that modifies the primary CIDR will lead to an incorrect state of creating a new vPC while not deleting the old one. Because the GUI does not allow the primary CIDR change operation (that is, deselecting the primary option from one CIDR and selecting the primary CIDR box for the other CIDR), this problem will not happen if the operation is performed using GUI. If the operation is done using the REST API, a fault is raised for the new primary CIDR and the related subnet is not deployed in the cloud. The old CIDR is not cleaned up as well.	5.1(2e) and later
CSCvw55088	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	5.1(2e) and later
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.	5.1(2e) and later
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.	5.1(2e) and later
CSCvw60314	After upgrading one of the Cloud APIC sites to the 5.1(2) 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.	5.1(2e) and later
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.	5.1(2e) 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.	5.1(2g) 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
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.	5.1(2e)
CSCvu03950	An operational fault related to SSH connectivity to the Cloud Services Router is seen in the GUI. This fault indicates that Cloud Services Router connectivity has been lost and that configurations can no longer go to that Cloud Services Router.	5.1(2e)
CSCvu17097	Inter tenant shared services traffic is impacted after tenant delete and add.	5.1(2e)
CSCvu52738	A secure LDAP test user does not make use of secure LDAP for a test user liveness check.	5.1(2e)
CSCvu63858	The inner table view of a contract might have incomplete information for the consumer EPGs.	5.1(2e)
CSCvu76275	Duplicate rules can be seen in the Azure on the Network Security Group of an EPG providing a contract with an ALB or NLB attached. There is no functional impact. The duplicate rule seen will be an inbound rule that allows the ALB/NLB subnet to talk to the provider EPG application security group.	5.1(2e)
CSCvu80939	The route table entry to the provider subnet is not created in the consumer's route table.	5.1(2e)
CSCvu81750	Inter-site BGP sessions are down after a policy-based upgrade of Cloud APIC from the 5.0(1) release to the 5.1(2) release.	5.1(2e)
CSCvu84182	Faults containing the following keywords are observed and VGW does not get deleted in Azure: • InUseSubnetCannotBeDeleted • NetCfgInvalidSubnet • VirtualNetworkGatewayCannotBeDeleted	5.1(2e)
CSCvv19470	A rule to allow traffic from a consumer cloudEPg to a firewall's untrust interface will be missing if the firewall's untrust connector uses a tag-based selector. This symptom will be seen only if an NLB is the first node of the service chain and if the graph is not performing any redirect.	5.1(2e)

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 5.1(2) releases in which the bug exists. A bug might also exist in releases other than the 5.1(2) 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.	5.1(2e) and later
CSCvo55112	Logs are lost upon stopping the Cloud APIC instance.	5.1(2e) and later
CSCvo95998	There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) and later
CSCvu88006	On the Dashboard, fewer VNet peerings are shown than expected.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) 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.	5.1(2e) and later
CSCvw49898	When the downgrading from the 5.1(2) 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.	5.1(2e) 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.	5.1(2e) and later
CSCvw51544	A user who is assigned a large number of security domains may not be able to create other Cisco ACI policies.	5.1(2e) and later
CSCvw97632	There is traffic loss when Cloud APIC is being downgraded from release 5.1(2e) to 5.0(2i).	5.1(2e) 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 5.1(2) and Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.1(1) for compatibility information for those products.

- Cloud APIC release 5.1(2) supports the following Cisco ACI product releases:
    - Cisco ACI Multi-Site Orchestrator, release 3.1(1)
    - Cisco APIC, release 5.1(2)
    - Cisco NX-OS for ACI-mode switches, release 15.1(2)
- 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