# Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 5.0(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) 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(2)*. For the features, issues, and limitations for the Cisco ACI Multi-Site Orchestrator, see the *Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.0(2)*.

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 |
|---|---|
| January 26, 2021 | Release 5.0(2j) became available. Added the resolved issues for this release. |
| September 25, 2020 | Release 5.0(2i) became available. This release adds the TCP MSS option; see the New Software Features section. |
| August 7, 2020 | Release 5.0(2h) became available. Added the resolved issues for this release. |
| July 3, 2020 | Release 5.0(2e) became available. |

# Contents



# New Software Features

| Feature | Description | Guidelines and Restrictions |
|---|---|---|
| TCP MSS option | Beginning with Release 5.0(2i), the TCP MSS option is available to configure the TCP maximum segment size (MSS). This value will be applied to all cloud router interfaces, including data Gigabit Ethernet interfaces, IPSec tunnel interfaces of cloud routers, and VPN tunnel interfaces toward cloud, on-premises, or other cloud sites. For VPN tunnels towards the cloud, if the cloud provider's MSS value is less than the value that you enter in this field, then the lower value is used; otherwise, the value that you enter in this field is used.<br><br>For more information, see the Cisco Cloud APIC for AWS Installation Guide, Release 5.0(x) and Cisco Cloud APIC for Azure Installation Guide, Release 5.0(x). | The MSS value affects only TCP traffic, and has no impact on other types of traffic, such as ping traffic. |
| Layer 4 to Layer 7 service redirect | With Layer 4 to Layer 7 service redirect, policies redirect traffic through specific service devices, where service devices can be deployed as a network load balancer or a third-party firewall. This traffic is not necessarily destined for the service device as part of the standard consumer-to-provider configuration; rather, you would configure the consumer-to-provider traffic as you normally would, and you would then configure service graphs to redirect that consumer-to-provider traffic to a specific service device.<br><br>For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.0(x). | See the Cisco Cloud APIC for Azure User Guide, Release 5.0(x) for a full list of guidelines and restrictions. |
| VNet peering for Azure cloud | You can now use Azure virtual network (VNet) peering with Cisco Cloud APIC to forward data between VNets. Azure VNet peering is a service that functions as an internal router to automate connectivity between VNets.<br><br>For more information, see the Configuring VNET Peering | ■ You cannot add, remove, or update a CIDR on the VNet if it has peering connections with other VNets. In this situation, you must re- |

| Feature | Description | Guidelines and Restrictions |
|---|---|---|
| | for Cloud APIC for Azure document. | move the VNet peerings, then make the necessary change to the CIDR (add, remove, or update the CIDR), then reestablish the VNet peerings again.<br>■ Resources in one virtual network can't communicate with the front-end IP address of a Basic Internal Load Balancer (ILB) in a globally-peered virtual network.<br>■ Some services that use a Basic load balancer don't work over global virtual network peering. For more information, see:<br>Constraints for peered virtual networks.<br>There is no support for traffic between two user VNets where one of the VNets has only VNet peering configured and the other VNet has only VPN gateway configured. |
| Support for multi-node service graphs with native and third-party Layer 4 to Layer 7 services | You can now deploy Azure load balancers (network load balancers) and third-party firewalls in Azure. You can deploy up to three service nodes in a service graph. The nodes can be non-redirect or redirect.<br>For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.0(x). | See the Cisco Cloud APIC for Azure User Guide, Release 5.0(x) for a full list of guidelines and restrictions. |
| Azure NLB automation with service chaining | You can now deploy an Azure load balancer (network load balancer) using a service graph.<br>For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.0(x). | See the Cisco Cloud APIC for Azure User Guide, Release 5.0(x) for a full list of guidelines and restrictions. |

| Feature | Description | Guidelines and Restrictions |
|---|---|---|
| Inter-VNET/VPC services | You can now deploy and automate the Inter-VNet services.<br><br>For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.0(x). | See the Cisco Cloud APIC for Azure User Guide, Release 5.0(x) for a full list of guidelines and restrictions. |
| Support for multiple CIDR and subnet blocks on the infra VNet | You can configure multiple CIDR and subnet blocks on the infra VNet in the Cisco Cloud APIC.<br><br>For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.0(x). | None. |
| Support for cloud EPGs and cloud external EPGs in the infra tenant. | You can create cloud EPGs and cloud external EPGs in the infra tenant in the Cisco Cloud APIC, where all the cloud EPGs and cloud external EPGs will be associated with the overlay-2 VRF in the infra tenant.<br><br>For more information, see the Cisco Cloud APIC for Azure User Guide, Release 5.0(x). | When creating an EPG in the infra tenant:<br><br>■ Choose the overlay-2 VRF.<br><br>We recommend that you do not use the existing "cloud-infra" application profiles because those application profiles are used by EPGs in the overlay-1 VRF. Choose a different application profile or click Create Application Profile to create a new one. |
| Configuration drifts information | Cloud APIC provides visibility into any security policy (contract) configuration discrepancy between what you deploy from the Cloud APIC and what is actually configured in the cloud site.<br><br>For more information, see the "Configuration Drifts" chapter in the *Cisco Cloud APIC for Azure User Guide, Release 5.0(x)*. | This is a beta feature in this release and is supported only for contracts. |
| Custom naming rules for cloud resources | You can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud.<br><br>For more information, see the "Cloud Resources Naming" topic in the *Cisco Cloud APIC for Azure User Guide, Release 5.0(x)*. | None. |
| Naming convention support for more than 32 characters for the tenant and VRF name combination | All VRFs are assigned a VrfEncoded value. If the tenant and VRF name combination has more than 32 characters, then a VRF name (which also contains the tenant name) is identified in the cloud router using the VrfEncoded value.<br><br>For more information, see the "Creating a VRF Using the Cisco Cloud APIC GUI" topic in the *Cisco Cloud APIC for* | None. |

| Feature | Description | Guidelines and Restrictions |
|---|---|---|
| | *Azure User Guide, Release 5.0(x)* and Cisco Cloud APIC for AWS User Guide, Release 5.0(x). | |
| Support for a static IP address for a load balancer | While creating a device, you can assign a static IP address for an application load balancer (ALB) or a network load balancer (NLB).<br><br>For more information, see the "Creating Service Devices Using the Cloud APIC GUI" topic in the *Cisco Cloud APIC for Azure User Guide, Release 5.0(x)*. | The assigned static IP address must be in the same subnet as the load balancer.<br><br>ALB SKU Standard supports static and dynamic IP addresses. ALB SKU Standard V2 support static IP addresses only. Cloud APIC creates standard SKU NLBs only. |
| Support for comma-separated filters for rule creation in contracts | After a contract is created, some of the rules defined in the contract can be consolidated based on certain criteria. You can combine multiple ports and multiple IP addresses and ranges into a single, easy-to-understand rule.<br><br>For more information, see the *Cisco Cloud APIC for Azure User Guide, Release 5.0(x)*. | None. |
| Tag-based search | While viewing the cloud resource details for endpoints, you can search based on the cloud tag attribute. You can filter the search results for a cloud tag by entering a key or value term.<br><br>For more information, see the "Viewing Cloud Resource Details" topic in the *Cisco Cloud APIC for Azure User Guide, Release 5.0(x)*. | None. |

# 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(2) releases in which the bug exists. A bug might also exist in releases other than the 5.0(2) releases.

| Bug ID | Description | Exists In |
|---|---|---|
| CSCvx16810 | After upgrading to release 5.0(2j), traffic is still working. After about 1 hour, the CSR may lose all VRF configurations such that traffic from the Cloud to an external destination is dropped. The "show vrf" command does not show any user VRF configuration. | 5.0(2j) and later |

| Bug ID | Description | Exists In |
|---|---|---|
| CSCvo30542 | TACACS monitoring of the destination group is not supported through the GUI. | 5.0(2e) and later |
| CSCvt52797 | Some cloud-to-cloud tunnels are operationally down in external-facing CSRs. | 5.0(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. | 5.0(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. | 5.0(2e) 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(2e) and later |
| 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. | 5.0(2e) and later |
| CSCvu17097 | Inter tenant shared services traffic is impacted after tenant delete and add. | 5.0(2e) and later |
| CSCvu52738 | A secure LDAP test user does not make use of secure LDAP for a test user liveness check. | 5.0(2e) and later |
| CSCvu63858 | The inner table view of a contract might have incomplete information for the consumer EPGs. | 5.0(2e) and later |
| CSCvu64277 | Stats seen on Cisco Cloud APIC are sometimes not in sync with Azure stats. | 5.0(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. | 5.0(2e) and later |
| CSCvu72020 | The GUI cannot properly display the service graph association in EPG communication, due to a mismatched tenant name. | 5.0(2e) and later |

| Bug ID | Description | Exists In |
|---|---|---|
| CSCvu72354 | Adding an EPG endpoint selector fails with an error message saying the selector is already attached. | 5.0(2e) and later |
| 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. | 5.0(2e) and later |
| CSCvu78074 | Route nextHop is not set to the redirect service node specified in the service graph. | 5.0(2e) and later |
| CSCvu80939 | The route table entry to the provider subnet is not created in the consumer's route table. | 5.0(2e) and later |
| CSCvu81750 | Inter-site BGP sessions are down after a policy-based upgrade of Cloud APIC from the 5.0(1) release to the 5.0(2) release. | 5.0(2e) and later |
| CSCvu84182 | Faults containing the following keywords are observed and VGW does not get deleted in Azure:<br>- InUseSubnetCannotBeDeleted<br>- NetCfgInvalidSubnet<br>- VirtualNetworkGatewayCannotBeDeleted | 5.0(2e) and later |
| 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.<br>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. | 5.0(2e) and later |
| CSCvv91481 | The Cloud APIC cannot SSH to the CSRs on their OOB intfs (Gi1) public IP addresses. Repeated connection attempts are seen in the Cloud APIC csrdriver logs (/var/sysmgr/tmp_logs/csrdriver.log). Cloud APIC-to-CSR SSH/tcp22 connections are stuck in SYN_SENT as shown by netstat, which is also confirmed in a tcpdump. No return traffic is observed from the CSR. | 5.0(2e) and 5.0(2h) |

# 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 |
|---|---|---|

| Bug ID | Description | Fixed in |
|---|---|---|
| CSCvv91481 | The Cloud APIC cannot SSH to the CSRs on their OOB intfs (Gi1) public IP addresses. Repeated connection attempts are seen in the Cloud APIC csrdriver logs (/var/sysmgr/tmp_logs/csrdriver.log). Cloud APIC-to-CSR SSH/tcp22 connections are stuck in SYN_SENT as shown by netstat, which is also confirmed in a tcpdump. No return traffic is observed from the CSR. | 5.0(2j) |
| CSCvu89372 | Custom cloud resource names can be configured through a global policy on Cisco Cloud APIC. The global policy can be customized by using the GUI or REST API. The GUI limits the customization option for the Virtual network name. | 5.0(2h) |
| 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(2e) |
| CSCvt77579 | CSRs with unknown status are listed in the Inter-Site Connectivity screen. | 5.0(2e) |
| CSCvt82672 | A BGP faults show up in the Cloud APIC dashboard for multiple CSR BGP sessions. | 5.0(2e) |
| 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.<br><br>There will be fault raised for route table entries that failed to get programed in the cloud. | 5.0(2e) |
| 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(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 5.0(2) releases in which the bug exists. A bug might also exist in releases other than the 5.0(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. | 5.0(2e) and later |
| CSCvo55112 | Logs are lost upon stopping the Cloud APIC instance. | 5.0(2e) and later |
| CSCvo95998 | There is traffic loss after a Cloud APIC upgrade. Traffic will eventually converge, but this could take a few minutes. | 5.0(2e) and later |

| Bug ID | Description | Exists In |
|---|---|---|
| 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(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. | 5.0(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. | 5.0(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. | 5.0(2e) and later |
| CSCvu88006 | On the Dashboard, fewer VNet peerings are shown than expected. | 5.0(2e) and later |
| CSCvw85050 | The CSR is not downgraded to 16.12 when the Cloud APIC is downgraded to the 5.0(1) release. | 5.0(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 5.0(2)* and *Cisco ACI Multi-Site Orchestrator Release Notes, Release 3.0(2)* for compatibility information for those products.

- Cloud APIC release 5.0(2) supports the following Cisco ACI product releases:
  - Cisco ACI Multi-Site Orchestrator, release 3.0(2)
  - Cisco APIC, release 5.0(2)
  - Cisco NX-OS for ACI-mode switches, release 15.0(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