Cisco Application Policy Infrastructure Controller, Release 1.2(2), Release Notes

This document describes the features, caveats, and limitations for the Cisco Application Policy Infrastructure Controller (APIC) software.

Note: Use this document in combination with the *Cisco NX-OS Release 11.2(2) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*, which you can view at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

Additional product documentation is listed in the "Related Documentation" section.

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Table 1 shows the online change history for this document.

Table 1 Online History Change

Date	Description
February 22, 2016	1.2(2g): Created the release notes for Release 1.2(2g).
February 23, 2016	1.2(2g): In the New Software Features section, for the Configuration Zones feature, added mention that triggered policy deployment is not supported. In the Open Caveats section, added bug CSCuy42763. In the New Software Features section, added "Static Route to nullo".
February 24, 2016	In the New Software Features section, added "Microsoft Integration Enhancements".
February 25, 2016	In the Compatibility Information section, updated the AVS version to 5.2(1)SV3(1.15).
February 27, 2016	1.2(2h): Release 1.2(2h) became available. Added the resolved caveats for this release.
February 29, 2016	In the Installation Notes section, added mention that you should back up your configuration before installing or upgrading to this release. In the Compatibility Information section, updated the supported ASA device package version to "1.2.5.5 or later". Added a link to the cisco.com page that has the Cisco ACI Virtualization Guide. Added a link to the AVS Release Notes. In the Downgrading the APIC Controller section, in the procedure, changed "eraseconfig" to "acidiag touch setup".

Date	Description
March 2, 2016	1.2(2g): In the Open Caveats section, added bug CSCuy50173.
March 4, 2016	In the Compatibility Information section, added mention of SCVMM UR 9 release and WAP UR 9.
March 16, 2016	In the Installation Notes section, added mention that ACI with SCVMM or Windows Azure Pack only supports ASCII characters.
March 28, 2016	In the New Software Features section, for the Interleak Enhancements feature, removed mention of EIGRP. EIGRP is not supported with this feature.
April 20, 2016	In the New Documentation section, added the Cisco APIC Layer 4 to Layer 7 Service Graph Deployment Guide, Release 1.2(2g) document.
June 24, 2016	1.2(2h): In the Resolved Caveats section, added bug CSCva04363.
August 8, 2016	In the New Software Features section, added the Ignore Acknowledged Faults feature.
August 11, 2016	In the Upgrading the APIC Controller section, added information about upgrading from an unlisted release.
September 24, 2016	1.2(2i): Release 1.2(2i) became available; there are no changes to this document for this release. See the *Cisco NX-OS Release 11.2(2i) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches* document for changes in this release.
December 6, 2016	In the Compatibility Information section, added information about a known issue when using the Safari browser to connect to the APIC.
February 28, 2017	In the Usage Guidelines section, added: If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.
April 17, 2017	Removed deprecated Knowledge Base articles.
November 20, 2017	In the Usage Guidelines section, changed a mention of "Virtual Private Cloud (VPC)" to "virtual port channel (vPC)."

Contents

This document includes the following sections:

Introduction

The Cisco Application Centric Infrastructure (ACI) is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates the entire application deployment life cycle.

The *Cisco Application Centric Infrastructure Fundamentals* guide provides complete details about the ACI, including a glossary of terms that are used in the ACI.

Installation Notes

- For installation instructions, see the *Cisco ACI Fabric Hardware Installation Guide*.
- Back up your APIC configuration prior to installing or upgrading to this release. Single APIC clusters, which should not be run in production, can lose their configuration if database corruption occurs during the installation or upgrade.
- For instructions on how to access the APIC for the first time, see the *Cisco APIC Getting Started Guide*.
- For the Cisco APIC Python SDK documentation, including installation instructions, see the *Cisco APIC Python SDK Documentation*.

  The SDK egg file needed for installation is included in the package:

  — acicobra-1.2_2<letter>-py2.7.egg

  Replace "<letter>" with the letter of the release. For example, for the 1.2(2g) release, the filename is "acicobra-1.2_2g-py2.7.egg".

  Note: Installation of the SDK with SSL support on Unix/Linux and Mac OS X requires a compiler. For a Windows installation, you can install the compiled shared objects for the SDK dependencies using wheel packages.

  Note: The model package depends on the SDK package; be sure to install the SDK package first.
- Cisco ACI with Microsoft System Center Virtual Machine Manager (SCVMM) or Microsoft Windows Azure Pack only supports ASCII characters. Non-ASCII characters are not supported. Ensure that English is set in the System Locale settings for Windows, otherwise ACI with SCVMM and Windows Azure Pack will not install. In addition, if the System Locale is later modified to a non-English Locale after the installation, the integration components might fail when communicating with the APIC and the ACI fabric.

You can find all of the indicated documentation at the following URL:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Upgrading the APIC Controller

The following table lists the supported APIC upgrades. If you are upgrading from a release that is not listed in the table, you must first upgrade to one of the listed "From" releases, and then upgrade to the desired release.

Note: Do not make any configuration changes until the APIC and switch upgrades are complete.

Table 2 Supported APIC Upgrades for the 1.2(2g) Release

From	To	Limitations	Recommended Procedure

From	To	Limitations	Recommended Procedure
1.2(1)	1.2(2)	None	1. Upgrade APICs 2. After the APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(4)	1.2(2)	Due to bug CSCux40954, which was resolved in the 1.2(1) release, the Cisco APIC firmware process using the **Upload** button from the GUI does not work. The upload appears to complete successfully, but the firmware is not updated in the repository. You must instead download the image using SCP or HTTP from a server to the APIC.	1. Upgrade APICs 2. After the APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(3f)	1.2(2)	None	1. Upgrade APICs 2. After the APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(2h)	1.2(2)	None	1. Upgrade APICs 2. After the APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.1(1)	1.2(2)	None	1. Upgrade APICs 2. After the APICs are upgraded successfully, upgrade the switches using two or more maintenance groups
1.0(4q) or a later patch	1.2(2)	None	1. Upgrade APICs 2. After the APICs are upgraded successfully, upgrade the switches using two or more maintenance groups

Downgrading the APIC Controller

This section provides information about downgrading the APIC controller.

Note: APIC Image downgrades will be blocked by default if the target image is not in a supported downgrade path.

The following table lists the supported APIC and switch downgrades.

Table 3 Supported APIC and Switch Downgrades

From	To	Limitations	Recommended Procedure
1.2(2)	1.1(10) and later	None	1. Downgrade APICs. 2. After the APICs are downgraded successfully, downgrade the switches using two or more maintenance groups.
1.2(1)	1.1(10) and later	None	1. Downgrade APICs. 2. After the APICs are downgraded successfully, downgrade the switches using two or more maintenance groups.
1.2(1)	1.0(4q) and earlier	None	You must perform a stateless downgrade. See the procedure below.

The following procedure performs a stateless downgrade:

Note: You must plan for a Fabric outage, as this procedure rebuilds the Fabric.

1. Export the Fabric configuration.
2. Run the "acidiag touch setup" command on the APIC controllers. This will reboot the controllers. Ensure that the controllers have been rebooted before moving on to step 3.
3. Run the "setup-clean-config.sh" script on the switch nodes and reload all of the switches. Steps 2 and 3 clear the configuration on the Fabric, making this a stateless downgrade.
4. Rediscover the Fabric.
5. Downgrade the Fabric to the desired release.
6. Run the "acidiag touch setup" command on the APIC controllers. This step is required so that the script can run additional commands that might be required for the version that is being used. The "acidiag touch setup" command will reload the APICs.
7. Run the "setup-clean-config.sh" script on the switch nodes and reload them.
8. Complete the initial setup script on the APIC controllers.
9. Import the Fabric configuration using the import "merge" mode.

Compatibility Information

- This release supports the hardware and software listed on the *ACI Ecosystem Compatibility List* document and the software listed as follows:
  - Cisco NX-OS Release 11.2(2)

  - Cisco AVS, Release 5.2(1)SV3(2.1)

    For more information about the supported AVS releases, see the AVS software compatibility information in the *Cisco Application Virtual Switch Release Notes* at the following URL:

    https://www.cisco.com/c/en/us/support/switches/application-virtual-switch/products-release-notes-list.html

  - Cisco UCS Manager software release 2.2(1c) or later is required for the Cisco UCS Fabric Interconnect and other components, including the BIOS, CIMC, and the adapter

  See the *ACI Ecosystem Compatibility List* document at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html

- The breakout of 40G ports to 4x10G on the N9332PQ switch is not supported in ACI-Mode.
- To connect the N2348UPQ to ACI leaf switches, the following options are available:
  - Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the N9332PQ switch
  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the N9396PX or N9372PX switches
- Connecting the APIC (the controller cluster) to the ACI fabric requires a 10G interface on the ACI leaf. You cannot connect the APIC directly to the N9332PQ ACI Leaf.
- This release supports the following firmware:
  - 1.5(4e) CIMC HUU iso
  - 2.0(3i) CIMC HUU iso (recommended)
- Beginning with Cisco Application Virtual Switch (AVS) release 5.2(1)SV3(1.10), you can connect service virtual machines that are part of Layer 4 to Layer 7 service graphs to AVS. Layer 4 to Layer 7 service graphs for Cisco AVS can be configured for service virtual machines that are in VLAN mode. By using two AVS VMM domains (one with VLAN and one with VXLAN), you can have a virtual machine in VXLAN mode that is protected by service graphs that are using the service virtual machine in VLAN mode.
- This release supports VMM Integration and VMware Distributed Virtual Switch (DVS) 6.x. For more information about guidelines for upgrading VMware DVS from 5.x to 6.x and VMM integration, see the *Cisco ACI Virtualization Guide, Release 1.2(2)* at the following URL:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
- This release supports the Microsoft System Center Virtual Machine Manager (SCVMM) Update Rollup 9 and 10 releases, and the Microsoft Windows Azure Pack Update Rollup 9 and 10 releases.
- This release supports the partner packages specified in the *L4-L7 Compatibility List Solution Overview* document at the following URL:

  https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/solution-overview-listing.html
- This release supports Adaptive Security Appliance (ASA) device package version 1.2.5.5 or later.
- If you are running a Cisco Adaptive Security Virtual Appliance (ASAv) version that is prior to version 9.3(2), you must configure SSL encryption as follows:

  (config)# ssl encryption aes128-sha1
- A known issue exists with the Safari browser and unsigned certificates, which applies when connecting to the APIC GUI. For more information, see the *Cisco APIC Getting Started Guide*.

- For information about APIC compatibility with UCS Director, see the appropriate *Cisco UCS Director Compatibility Matrix* document at the following URL:

  https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-device-support-tables-list.html

Usage Guidelines

This section lists usage guidelines for the APIC software.

- The APIC GUI supports the following browsers:
  - Chrome version 35 (at minimum) on Mac and Windows
  - Firefox version 42 (at minimum) on Mac, Linux, and Windows
  - Internet Explorer version 11 (at minimum)
  - Safari 7.0.3 (at minimum)

  Note: Restart your browser after upgrading to this release.

  Caution: A known issue exists with the Safari browser and unsigned certificates. Read the information presented here before accepting an unsigned certificate for use with WebSockets.

  When you access the HTTPS site, the following message appears:

  "Safari can't verify the identity of the website APIC. The certificate for this website is invalid. You might be connecting to a website that is pretending to be an APIC, which could put your confidential information at risk. Would you like to connect to the website anyway?"

  To ensure that WebSockets can connect, you must do the following:

  1. Click Show Certificate.
  2. Select Always Trust in the three drop-down lists that appear.

  If you do not follow these steps above, WebSockets will not be able to connect.
- The APIC GUI includes an online version of the Quick Start guide that includes video demonstrations.
- The infrastructure IP address range must not overlap with other IP addresses used in the fabric for in-band and out-of-band networks.
- The APIC does not provide IPAM services for tenant workloads.
- To reach the APIC CLI from the GUI: select System > Controllers, highlight a controller, right-click and select "launch SSH". To get the list of commands, press the escape key twice.
- In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
- For the following services, use a DNS-based host name with out-of-band management connectivity. IP addresses can be used with both in-band and out-of-band management connectivity.
  - Syslog server
  - Call Home SMTP server
  - Tech support export server
  - Configuration export server

  - Statistics export server

- Both leaf and spine switches can be managed from any host that has IP connectivity to the fabric.
- When configuring an atomic counter policy between two endpoints, and an IP is learned on one of the two endpoints, it is recommended to use an IP-based policy and not a client endpoint-based policy.
- When configuring two Layer 3 external networks on the same node, the loopbacks need to be configured separately for both Layer 3 networks.
- All endpoint groups (EPGs), including application EPGs and Layer 3 external EPGs, require a domain. Interface policy groups must also be associated with an Attach Entity Profile (AEP), and the AEP must be associated with domains. Based on the association of EPGs to domains and of the interface policy groups to domains, the ports and VLANs that the EPG uses are validated. This applies to all EPGs including bridged Layer 2 outside and routed Layer 3 outside EPGs. For more information, see the *Cisco Fundamentals Guide* and the *KB: Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port* article.

  Note: In the 1.0(4x) and earlier releases, when creating static paths for application EPGs or Layer 2/Layer 3 outside EPGs, the physical domain was not required. In this release, it is required. Upgrading without the physical domain will raise a fault on the EPG stating "invalid path configuration."
- An EPG can only associate with a contract interface in its own tenant.
- User passwords must meet the following criteria:
  - Minimum length is 8 characters
  - Maximum length is 64 characters
  - Fewer than three consecutive repeated characters
  - At least three of the following character types: lowercase, uppercase, digit, symbol
  - Cannot be easily guessed
  - Cannot be the username or the reverse of the username
  - Cannot be any variation of "cisco", "isco", or any permutation of these characters or variants obtained by changing the capitalization of letters therein
- The power consumption statistics are not shown on leaf node slot 1.
- For Layer 3 external networks created through the API or Advanced GUI and updated through the CLI, protocols need to be enabled globally on the external network through the API or Advanced GUI, and the node profile for all the participating nodes needs to be added through the API or Advanced GUI before doing any further updates through the CLI.
- For Layer 3 external networks created through the CLI, you should not to update them through the API. These external networks are identified by names starting with "__ui_".
- The output from "show" commands issued in the NX-OS-style CLI are subject to change in future software releases. Cisco does not recommend using the output from the show commands for automation.
- In this software version, the CLI is supported only for users with administrative login privileges.
- Do not separate virtual port channel (vPC) member nodes into different configuration zones. If the nodes are in different configuration zones, then the vPCs' modes become mismatched if the interface policies are modified and deployed to only one of the vPC member nodes.
- If you defined multiple login domains, you can choose the login domain that you want to use when logging in to an APIC. By default, the domain drop-down list is empty, and if you do not choose a domain, the DefaultAuth domain is used for authentication. This can result in login failure if the username is not in the DefaultAuth login domain. As such, you must enter the credentials based on the chosen login domain.

- A firmware maintenance group should contain max of 80 nodes.
- When contracts are not associated with an endpoint group, DSCP marking is not supported for a VRF with a vzAny contract. DSCP is sent to a leaf along with the actrl rule, but a vzAny contract does not have an actrl rule. Therefore, the DSCP value cannot be sent.
- If the communication between the APIC and vCenter is impaired, some functionality is adversely affected. The APIC relies on the pulling of inventory information, updating vDS configuration, and receiving event notifications from the vCenter for performing certain operations.

Verified Scalability Limits

The following table shows the CLI scalability limits.

Table 4 CLI Scalability Limits

Configurable Option	Scale
Number of tenants	500
Number of Layer 3 (L3) contexts	300
Number of endpoint groups (EPGs)	3,500
Number of endpoints (EPs)	20,000
Number of bridge domains (BDs)	3,500
Number of BGP + number of OSPF sessions + EIGRP (for external connection)	300
Maximum number of vPCs	48
Maximum number of PCs, access ports	48
Maximum number of encaps per access port	1,750
Number of multicast groups	8,000
Maximum number of vzAny provided contracts	16
Maximum number of vzAny consumed contracts	16
Maximum amount of encaps per endpoint group	2 static, 1 dynamic
Security TCAM size	4,000
Number of VRFs	500
Separate-Config-Set	
Tenants	100
Endpoint groups	1,000
Bridge domains	500
VRFs	100
SPAN destinations	3

Configurable Option	Scale
NTP servers	2
Contracts	100
DNS servers	2
Syslog servers	1

For additional verified scalability limits, see the *Verified Scalability Guide* for this release:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

New Software Features

The following table lists the new software features in this release:

Table 5 New Software Features, Guidelines, and Restrictions

Feature	Description	Guidelines and Restrictions
BGP Dynamic Neighbors, Route Dampening, Weight Attribute, Remove-Private-As	Rather than providing a specific neighbor address, a dynamic neighbor dynamic range of addresses can be provided. BGP dampening minimizes propagation into the fabric of flapping eBGP routes received from external routers connected to border leaf switches (BLs). Use the BGP weight attribute to select a best path. Private Autonomous numbers (AS) are from 64512-65535; they cannot be leaked to a global BGP table. Private AS numbers can be removed from the AS path on a per peer basis and can only be used for eBGP peers.	None
BGP Route Policy Enhancements	The route control profile now enables specifying not only what is allowed, but what to match (community) and what to set (such as preference, next hop, community, and so forth). Route control profiles can be combinable with match and set options, or global (for all subnets within a tenant). Route control profiles provide enhanced default import and default export route control. The protocol interleak/redistribute policy controls externally learned route leaking into the ACI BGP routes, and includes support for set attributes.	None
Bidirectional Forwarding Detection	Use Bidirectional Forwarding Detection (BFD) to provide sub-second failure detection times in the forwarding path between ACI fabric border leaf switches configured to support peering router connections.	None
Configuration Zones	Configuration zones divide the ACI fabric into different zones that can be updated with configuration changes at different times. This limits the risk of deploying a faulty fabric-wide configuration that might disrupt traffic or even bring the fabric down. An administrator can deploy a configuration to a non-critical zone, and then deploy it to critical zones when satisfied that it is suitable. **Note:** Do not upgrade or downgrade nodes that are part of a disabled configuration zone.	Supported for infra policies. Triggered policy deployment ("Deploy Now" in GUI) is not supported in this release. Only setting the deployment mode to Enabled or Disabled is supported.
Data Plane Policing	Data plane policing (DPP) is used to manage bandwidth consumption on ACI fabric access interfaces. DPP policies can apply to egress traffic, ingress traffic, or both. DPP monitors the	None.

Feature	Description	Guidelines and Restrictions
	data rates for a particular interface.	
Device Managers and Chassis Managers	Device managers and chassis managers serve as a single point of configuration for a set of clusters in a Cisco Application Centric Infrastructure (ACI) fabric. The chassis manager also adds support for a chassis, which can support a number of virtual service devices that are represented as CDev objects. For more information, see the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.	None
DSCP Marking	Previously, DSCP marking could only be set on an L3Out, but now it can be set at the filter level on the following with the precedence order from the innermost to the outermost: contract, subject, in term, out term.	None
EIGRP and IPv6	IPv6 is now supported with EIGRP.	None
Ignore Acknowledged Faults	In the Health Score Evaluation Policy, you can enable the **Ignore Acknowledged Faults** feature, which allows faults to be ignored in health score calculations if the faults have been acknowledged. Prior to this release or with the **Ignore Acknowledged Faults** feature disabled, all faults affect the health score and subsequently lower its total value even if the faults are acknowledged. For more information about how health scores are calculated, see the *Cisco Application Centric Infrastructure Fundamentals* document. This feature is not on by default. To enable the feature, in the GUI on the menu bar, choose **Fabric > Fabric Policies > Monitoring Policies**. In the Navigation pane, choose **Health Score Evaluation Policies > Health Score Evaluation Policy**. In the Work pane, put a check in the **Ignore Acknowledge Faults** check box.	None
Interleak Enhancements	Interleak from OSPF now enables the user to set attributes such as "community", "preference", and "metric" for route leaking from OSPF to BGP. For more information about Interleak Enhancements, see the *Cisco APIC Layer 3 Networking Configuration Guide*.	None
Intra-EPG Deny Isolation	Intra-EPG deny policies provide full isolation for virtual or physical endpoints; no communication is allowed between endpoints in an EPG that is operating in full isolation mode. Intra-EPG deny isolation can be applied to bare metal server deployments and to VMware Distributed Virtual Switch (DVS) deployments (based on PVLAN tags).	None
IPv6 on ACI Fabric and APIC Management Interfaces	Now, there are no restrictions on which ACI interfaces support IPv6; IPv4 only, IPv6 only, or dual stack configuration is supported for in-band and out-of-band interfaces.	None

Feature	Description	Guidelines and Restrictions
Microsoft Integration Enhancements	This release includes the following Microsoft integration enhancements: • IPAM for Windows Azure Pack and SCVMM • Windows Azure Pack multi-bridge domain for the same VRF • Windows Azure Pack L3Out for BYOA tenant For more information, see the *Cisco ACI Virtualization Guide*.	None
OSPF Name Lookup	OSPF can be configured to enable name lookup for router IDs and perform prefix suppression.	None
Outbound and Inbound Prefix-List and Route Map-Based Filtering	Introduced support for specifying constraints on the subnets that can be created through OpenStack. These constraints enable you to disallow the creation of certain subnets, or to make them public or private in the APIC. See the *Cisco ACI with OpenStack OpFlex Deployment Guide for Red Hat* and *Cisco ACI with OpenStack OpFlex Deployment Guide for Ubuntu*.	None
Port Tracking Policy for Uplink Failure Detection	Uplink failure detection can be enabled in the fabric access global port tracking policy. The port tracking policy monitors the status of links between leaf switches and spine switches. When an enabled port tracking policy is triggered, the leaf switches take down all access interfaces on the switch that have EPGs deployed on them. Depending on the model of leaf switch, each leaf switch can have 6, 8, or 12 uplink connections to each spine switch. The port tracking policy specifies the number of uplink connections that trigger the policy, and a delay timer for bringing the leaf switch access ports back up after the number of specified uplinks is exceeded.	None
Route Summarization	Route summarization simplifies route tables by replacing many specific addresses with a single address. For example, 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 is replaced with 10.1.0.0/16. Route summarization policies enable routes to be shared efficiently among border leaf switches and their neighbor leaf switches. BGP, OSPF, or EIGRP route summarization policies are applied to a bridge domain or transit subnet. For OSPF, inter-area and external route summarization are supported.	None
SNMP Trap Destinations Over IPv6	Adds support for SNMP trap destinations over IPv6.	None
Static Route to nullo	Configuring static route to the nullo interface is now supported.	None
Stretched Fabric with Three Sites	Increases the number of supported stretched fabric sites from two to three, and adds the ability of having more than two route reflectors per site.	None

Feature	Description	Guidelines and Restrictions
vRealize VPC	In a VPC Plan: • A load balancer and DHCP is supported for the private address space. • A firewall and load balancer are supported.	None

New Hardware Features

For new hardware features, see the *Cisco NX-OS Release 11.2(2) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches* at the following location:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

Changes in Behavior

This section lists changes in behavior in this release.

- Both leaf and spine switches can now be managed from any host that has IP connectivity to the fabric. In previous releases, a spine could not be accessed by hosts that were behind a router.
- When upgrading to the 1.2(2) release, a non-default out-of-band contract applied to the out-of-band node management endpoint group can cause unexpected connectivity issues to the APICs. This is because prior to the 1.2(2) release, the default out-of-band that was contract associated with the out-of-band endpoint group would allow all default port access from any address. In 1.2(2), when a contract is provided on the out-of-band node management endpoint group, the default APIC out-of-band contract source address changes from any source address to only the local subnet that is configured on the out-of-band node management address. Thus, if an incorrectly configured out-of-band contract is present that had no impact in 1.2(1) and prior releases, upgrading to the 1.2(2) release can cause a loss of access to the APICs from the non-local subnets.

Caveats

This section contains lists of open and resolved caveats and known behaviors.

- Open Caveats
- Resolved Caveats
- Known Behaviors

Open Caveats

This section lists the open caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug. If a caveat is fixed in a patch of this release, the "Fixed In" column of the tables specifies the release.

Open Caveats in the 1.2(2g) Release

The following table lists the open caveats in the 1.2(2g) release.

Table 6 Open Caveats in the 1.2(2g) Release

Bug ID	Description	Fixed In
CSCux25207	After upgrading TORs from the 1.1(4e) release to the 1.2(1k) release, when the maint-grp-1 set of the TORs are rebooted, there is traffic loss on the virtual machines.	
CSCuy20938	The AVS host to leaf OpFlex handshake could be delayed after a VIB upgrade when there is a large number of vMotions happening in short time. OpFlex will auto-establish for the newly upgraded host once the vMotion events processing load subside.	
CSCuy22066	Upgrading or downgrading the APIC intermittently fails. The upgrade logs (/root/insieme_installer.log) show that the TCSD service is unable to run, as it is failing to communicate with TPM hardware. The problem happens when the TCSD daemon is unable to communicate with TPM hardware through the TIS module that is compiled into kernel.	
CSCuy25817	Downgrading an APIC configured with Intra-EPG deny configuration from the 1.2(2) release to an earlier release is not supported. You must manually clean up the Intra-EPG deny configuration before downgrading.	
CSCuy39911	A configuration failed fault gets raised on the in-band management EPG. This can happen if the EPG is not modifed in the same transaction where the relation from mgmt:InBZone to the EPG becomes formed. This is a falsely-raised fault and does not have any operational impact.	
CSCuy39924	Eraseconfig does not bring up IFC in the factory setting mode.	
CSCuy40276	Public subnets in a bridge domain can be advertised out through a routing protcol using a "match bridge-domain <bridge_domain_name>" in the route-map associated with the protcol. Route control properties such as "set tag"or "set metric" can be set for these public subnets through "inherit route-profile <profile name>" under the "match bridge-domain" command. If the route-profile name is not equal to "default-export", then the route control properties are not set correctly on the exported BD subnets.	

Bug ID	Description	Fixed In
CSCuy40279	Match statements on a route-map, such as match bridge-domain, community, or prefix-list, that do not have specific route-profiles defined under the match statement use the default-export route-profiles when the route-map is applied in the export direction and default-import route-profile when the route-map is applied in the import direction. The route-profile set action that is associated with the "default-export" or "default-import" route-profiles does not take effect on the route-map under certain conditions.	
CSCuy40280	The "match community" statement under the route-map <name> does not take effect.	
CSCuy41710	The Layer 3 sub-interface MTU value is reset to the inherited fabric policy value when l3extInstP is deleted.	
CSCuy42763	If a configuration zone is set to the triggered state (in the GUI, this is when the Deployment Mode is Disabled and the user selects Deploy Now), multiple policymgr shards will dump a core.	1.2(2h)
CSCuy50173	After installing the 1.2(2) release and using PXE boot to bring up the APICs, the admin login does not work.	

Open Caveats in the 1.2(2h) Release

There are no new open caveats in the 1.2(2h) release.

Open Caveats in the 1.2(2i) Release

There are no new open caveats in the 1.2(2i) release.

Resolved Caveats

This section lists the resolved caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Resolved Caveats in the 1.2(2g) Release

The following table lists the resolved caveats in the 1.2(2g) release.

Table 7 Resolved Caveats in the 1.2(2g) Release

Bug ID	Description
CSCuw61081	Live migration of a virtual machine initiated from SCVMM might fail if there is a compliance check failure on the virtual machine network. You must deploy the Microsoft UR9 release for this feature to work.
CSCuw61304	After a clean reboot and import of the configuration, a fault is raised for mgmt node connection groups.
CSCuw93034	Using the browser upload button to upload an image to the APIC from a local machine and canceling the upload midway, a stale image file remains in the /firmware/fwrepos/fwrepo.Uploads/ directory.
CSCux00422	Deny contract rule by taboo contract remains on the leaf even after the taboo contract was removed from the EPG.
CSCux09127	If the Troubleshooting wizard is configured with the Layer 4 to Layer 7 service provider as the source and the Layer 4 to Layer 7 service consumer as the destination, it might not work.
CSCux21853	The VMM policy shows the vCenter as being online, but the inventory is not synchronized and the DVS disappeared.
CSCux37088	After an upgrade, some interfaces are out of service.

Bug ID	Description
CSCux39365	Port channel association to external connectivity using the CLI or Basic GUI might fail if the name is large.
CSCux40946	In some configuration sequences, the public subnets of some of the bridge domains might not be advertised to external networks, even though the protocols (BGP, OSPF, EIGRP) are configured with the 'default' route-map in the 'out' direction.
CSCux43024	Configuring a VRF or context filter for SPAN-ing fabric ports by using the CLI does not succeed.

Resolved Caveats in the 1.2(2h) Release

The following table lists the resolved caveats in the 1.2(2h) release.

Table 8 Resolved Caveats in Cisco APIC Release 1.2(2h)

Bug ID	Description
CSCuy39945	Compatibility checks are turned off when you create a switch firmware group. As a result, when you downgrade to older versions such as 1.1(2m) that do not support Sapporo+ switches, the downgrade is not blocked as incompatible. This leads to Sapporo+ switches not working correctly.
CSCuy42763	If a configuration zone is set to the triggered state (in the GUI, this is when the Deployment Mode is Disabled and the user selects Deploy Now), multiple policymgr shards will dump a core.
CSCuy43049	A cluster with 1 APIC-SERVER-M2 and 2 APIC-SERVER-L2 failed to upgrade from 1.2(1m) to 1.2(2g) because of the following error: "The upgrade has an upgrade status of Failed Due to Incompatible Desired Version - Version is not compatible with hardware. The failure occured at the Controller Image Extraction stage of the install"
CSCva04363	Restarting the ACI kernel extension causes a BSOD. The resolution requires a new Microsoft package for version 1.2.2i.

Resolved Caveats in the 1.2(2i) Release

There are no new resolved caveats in the 1.2(2i) release.

Known Behaviors

This section lists caveats that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Known Behaviors in the 1.2(2g) Release

The following table lists caveats that describe known behaviors in the 1.2(2g) release.

Table 9 Known Behaviors in the 1.2(2g) Release

Bug ID	Description
CSCu052668	The APIC does not validate duplicate IPs assigned to two device clusters. The communication to devices or the configuration of service devices might be affected.
CSCu079243	In some of the 5-minute statistics data, the count of ten-second samples is 29 instead of 30.
CSCu079250	The node ID policy can be replicated from an old appliance that is decommissioned when it joins a cluster.

Bug ID	Description
CSCup47703	The DSCP value specified on an external endpoint group does not take effect on filter rules on the leaf switch.
CSCup79002	The hostname resolution of the syslog server fails on leaf and spine switches over in-band connectivity.
CSCup94070	After importing an exported configuration, graph instances are not created and Layer 4 to Layer 7 packages are missing in the system.
CSCuq21360	Following a FEX or switch reload, configured interface tags are no longer configured correctly.
CSCur39124	Switches could get downgraded to a 1.0(1x) version if the imported configuration consists of a firmware policy with a desired version set to 1.0(1x).
CSCur48950	Some reported client endpoints are not present on the APIC during an upgrade.
CSCur71082	The APIC is rebooted using the CIMC power reboot. On reboot, the system enters into fsck due to a corrupted disk.
CSCus15627	The Cisco APIC Service (ApicVMMService) shows as stopped in the Microsoft Service Manager (services.msc in control panel > admin tools > services) after valid domain credentials are entered during installation or configuration of the service.
CSCut51929	The traffic destined to a shared service provider endpoint group picks an incorrect class Id (PcTag) and gets dropped.
CSCuu09236	Traffic from an external Layer 3 network is allowed when configured as part of a vzAny (a collection of endpoint groups within a context) consumer.
CSCuu61998	The microsegment endpoint group is in the incorrect state after downgrading.
CSCuu64219	Downgrading the fabric starting with the leaf will cause faults such as policy-deployment-failed with fault code F1371.
CSCuw09389	For direct server return operations, if the client is behind the Layer 3 out, the server-to-client response will not be forwarded through the fabric.
CSCuw81638	The OpenStack metadata feature cannot be used with ACI integration with the Juno release (or earlier) of OpenStack due to limitations with both OpenStack and Cisco's ML2 driver.

Resolved Caveats in the 1.2(2h) Release

The following table lists the resolved caveats in the 1.2(2h) release.

Resolved Caveats in the 1.2(2i) Release

The following table lists the resolved caveats in the 1.2(2i) release.

Related Documentation

The Cisco Application Policy Infrastructure Controller (APIC) documentation can be accessed from the following website:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

New Documentation

This section lists the new Cisco APIC product documents for this release.

- *Cisco ACI with OpenStack OpFlex Architectural Overview*
- *Cisco ACI with OpenStack OpFlex Deployment Guide for Red Hat*
- *Cisco ACI with OpenStack OpFlex Deployment Guide for Ubuntu*
- *Cisco APIC Layer 4 to Layer 7 Service Graph Deployment Guide, Release 1.2(2g)*
- *KB: Configuring Data Plane Policing with Cisco APIC*