Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x

First Published: 2020-04-15

Last Modified: 2021-03-30

Release notes for Cisco IOS XE SD-WAN Release 17-2-x

•

Release Notes for Cisco IOS XE Catalyst SD-WAN Device, Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release Amsterdam 17.2.x, which provides Cisco SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager, as applicable to Cisco IOS XE Catalyst SD-WAN devices.

For release information about Cisco vEdge routers, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.1.x

What's New for Cisco IOS XE Release 17

This section applies to Cisco IOS XE Catalyst SD-WAN devices.

Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco IOS XE Release Amsterdam 17.2.1r

Feature	Description
Cisco SD-WAN Getting Started	
Install and Upgrade	This feature supports the use of a single "universalk9" image to deploy Cisco IOS XE SD-WAN and Cisco IOS XE functionality on all the supported devices. This universalk9 image supports two modes - Autonomous mode (for Cisco IOS XE features) and Controller mode (for Cisco SD-WAN features) .
Systems and Interfaces	
Configure Global Parameters	This feature lets you configure HTTP and Telnet server settings, and several other device settings, from Cisco vManage.
CLI Add-On Feature Templates	This feature adds a new feature template called the CLI add-on feature template. You can use this feature template to attach specific CLI configurations to a device. If a configuration cannot be specified using Cisco vManage but can be configured using the CLI on the device, then you can use this feature template to specify such configurations. You can also use CLI add-on feature templates to add small pieces of CLI configuration, instead of an entire running configuration. This feature is not intended to replace existing feature templates but instead to enhance their functionality. Note that not all CLIs are supported. For more information, see Supported and Qualified CLIs for CLI Add-On Feature Templates.
Ability to Send Syslog Messages over TLS	This feature allows you to transport syslog messages to external configured hosts by establishing a Transport Layer Security (TLS) connection. Using the TLS protocol enables the content of syslog messages to remain confidential, secure, and untampered or unaltered during each hop.
802.1X Support for SD-WAN	This feature lets you enable the IEEE 802.1X authentication on Cisco IOS XE SD-WAN devices. To be able to configure this feature using Cisco vManage, ensure that Cisco vManage is running Cisco SD-WAN Release 20.1.1.
Default Device Templates	A default device template provides basic information that you can use to bring up devices in a deployment quickly. This feature is supported on the Cisco Cloud Services Router 1000V Series, Cisco C1111-8PLTELA Integrated Services Routers, and Cisco 4331 Integrated Services Routers.
Integration with Cisco Unified Communications	This feature lets you use feature templates and voice policies to enable Cisco Unified Communications (UC) voice services for supported routers. When Cisco UC voice services are enabled, routers can process calls for various endpoints, including voice ports, POTS dial peers, SIP dial peers, and phone profiles in SRST mode. Configuring UC voice services for Cisco Unified Communications requires that Cisco vManage be running Cisco SD-WAN Release 20.1.1. This feature is supported on Cisco 4000 Series Integrated Services Routers.
Support for NAT Pool, Static NAT, and NAT as a Loopback Interface	This feature supports NAT configuration for loopback interface addresses, NAT Pool support for DIA, and Static NAT on Cisco IOS XE SD-WAN devices.

Feature	Description
Support for Configuring Secondary IP Address	You can configure up to four secondary IPv4 or IPv6 addresses, and up to four DHCP helpers. Secondary IP addresses can be useful for forcing unequal load sharing between different interfaces, for increasing the number of IP addresses in a LAN when no more IPs are available from the subnet, and for resolving issues with discontinuous subnets and classful routing protocol.
Low-bandwidth Link Optimization	This feature extends the low-bandwidth-link option to Cisco IOS XE SD-WAN devices, when configuring an interface that allows tunneling. This option reduces control plane traffic and is intended for use primarily on cellular WAN links, where bandwidth limitations and charges for traffic use require minimizing bandwidth.
VRF Configuration	Support for VRF configuration increased from a total of 100 to a total of 300 VRFs. Supported on: Cisco ASR 1001-HX and Cisco ASR 1002-HX
Device Configuration CLI Templates	The CLI Templates feature has been updated to support device configuration-based CLIs. You can use these templates to push the device configuration (yang-cli) to devices directly.
Routing	
MPLS-BGP Support on the Service Side	This features allows you to enable support on Multiprotocol Label Switching (MPLS). Multiple Service VPNs use inter autonomous system (AS) BGP labelled path to forward the traffic, which in turn helps scaling the service side VPNs with less control plane signaling. Label distribution for a given VPN routing and forwarding (VRF) instance on a given device can be handled by Border Gateway Protocol (BGP).
Mapping Multiple BGP Communities to OMP Tags	This features allows you to display information about OMP routes on Cisco vSmart Controller and Cisco IOS XE SD-WAN devices. OMP routes carry information that the device learns from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well as direct, connected, and static routes.
Support for Multicast Overlay Routing Protocols	This feature enables efficient distribution of one-to-many traffic. The multicast routing protocols like, IPv4 Multicast, IGMPv3, PIM SSM, PIM ASM, Auto RP and Static RP distribute data (for example, audio/video streaming broadcasts) to multiple recipients. Using multicast overlay protocols, a source can send a single packet of data to a single multicast address, which is then distributed to an entire group of recipients.
Bridging	
Support for Configuring Secondary IP Address	You can configure up to four secondary IPv4 or IPv6 addresses, and up to four DHCP helpers. Secondary IP addresses can be useful for forcing unequal load sharing between different interfaces, for increasing the number of IP addresses in a LAN when no more IPs are available from the subnet, and for resolving issues with discontinuous subnets and classful routing protocol.
Forwarding and QoS	
Per-Tunnel QoS	This feature lets you apply a Quality of Service (QoS) policy on individual tunnels, ensuring that branch offices with smaller throughput are not overwhelmed by larger aggregation sites. This feature is only supported for hub-to-spoke network topologies.
Policies	

Feature	Description
Device Access Policy on SNMP and SSH	This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. The control plane of Cisco IOS XE SD-WAN device processes the data traffic for local services (like SSH and SNMP) from a set of sources in a VPN. Routing packets are required to form the overlay.
Path Preference Support for Cisco IOS XE SD-WAN Devices	This feature extends to Cisco IOS XE SD-WAN devices, support for selecting one or more local transport locators (TLOCs) for a policy action.
Support for upto Eight SLA Classes	This feature allows you to configure upto a maximum of eight SLA classes. In previous releases, you could only configure upto four SLA classes. This allows for additional options to be configured in an application-aware routing policy.
Security	
SHA256 Support for IPSec Tunnels	This feature adds support for HMAC_SHA256 algorithms for enhanced security.
Firewall FQDN Support	This enhancement adds support to define a firewall policy using fully qualified domain names (FQDN), rather than only IP addresses. One advantage of using FQDNs is that they account for changes in the IP addresses assigned to the FQDN if that changes in the future.
SSL/TLS Proxy	The SSL/TLS Proxy feature allows you to configure an edge device as a transparent SSL/TLS proxy. Such proxy devices can then decrypt incoming and outgoing TLS traffic to enable their inspection by Unified Thread Defense (UTD) and identify risks that are hidden by end-to-end encryption. This feature is part of the Cisco SD-WAN Application Quality of Experience (AppQoE) and UTD solutions.
Auto-registration for Cisco Umbrella Cloud Services	This feature adds the ability to register devices to Cisco Umbrella using the Smart Account credentials to automatically retrieve Umbrella credentials (organization ID, registration key, and secret). This offers a more automatic alternative to manually copying a registration token from Umbrella.
Support for Automatic Tunneling to Secure Internet Gateways	This feature allows you to integrate your routers with a Secure Internet Gateway to perform security processing and ensure that your device's performance is not affected by processing security rules.
Manual Configuration for GRE Tunnels and IPsec Tunnels	This feature lets you manually configure a GRE tunnel by using the Cisco VPN Interface GRE template or an IPSec tunnel by using the Cisco VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.
Network Optimization and High Availability	

Feature	Description
Cloud onRamp for SaaS, Cisco IOS XE SD-WAN Devices	Cloud onRamp for SaaS is available for Cisco IOS XE SD-WAN devices, with a configuration workflow that is entirely different from the workflow that applies to Cisco vEdge devices. This feature is released as a fully functional beta in Cisco IOS XE Release Amsterdam 17.2.1r. The provisioning workflow is subject to change in future releases.
Monitor Cluster Activation Progress	This feature displays the cluster activation progress at each step and shows any failures that may occur during the process. The process of activating a cluster takes approximately 30 minutes or longer, and you can monitor the progress using the vManage task view window and events from the Monitoring page.
QoS on Service Chains	This feature classifies the network traffic based on the Layer 2 virtual local-area network (VLAN) identification number. The QoS policy allows you to limit the bandwidth available for each service chain by applying traffic policing on bidirectional traffic. The bidirectional traffic is the ingress side that connects Catalyst 9500-40X switches to the consumer and egress side that connects to the provider.
VNF States and Color Codes	This feature allows you to determine the state of a deployed VM using color codes, which you can view on the Monitor > Network page. These color codes help you make decisions on creating service chains based on the state of the VM.
Network Utilization Charts for SR-IOV Enabled NICs and OVS Switch	This feature allows you to view network utilization charts of VM VNICs connected to both SR-IOV enabled NICs and OVS switch. These charts help you determine if the VM utilization is optimal to create service chains.
AppNav-XE	This feature lets you configure policy-based redirection of LAN-to-WAN and WAN-to-LAN traffic flows to WAAS nodes for WAN optimization on Cisco IOS XE SD-WAN devices . This feature was already available on Cisco IOS XE platforms and is being extended to Cisco IOS XE SD-WAN platforms in this release.
Monitor and Maintain	
Event Notifications Support for Cisco IOS XE SD-WAN Devices	This feature adds support for event notifications, for Cisco IOS XE SD-WAN devices.
Monitoring Event Trace for OMP Agent and SD-WAN Subsystem	This feature enables monitoring and controlling the event trace function for a specified SD-WAN subsystem. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems.
QoS Monitoring in Cisco vManage	This release extends the capability of viewing interface-wise QoS information through Cisco vManage to support Cisco IOS XE SD-WAN devices. Before this release, QoS information for Cisco IOS XE SD-WAN devices could only be monitored through device CLI.
Forwarding Serviceability	This feature enables service path and tunnel path under Simulate Flows function in the vManage template and displays the next-hop information for an IP packet. This feature enables Speed Test and Simulate Flow functions on the Cisco IOS XE SD-WAN devices.

Feature	Description
Admin-tech Enhancements	This feature enhances the admin tech file to include show tech-support memory , show policy-firewall stats platform and show sdwan confd-log netconf-trace commands in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.
Command Reference	
Enable Layer 7 Health Check to Zscaler	The Enable Layer 7 Health Check feature helps in maintaining tunnel health by providing ability to load balance or failover of the tunnels. For more information, see the tracker command.

Table 2: Cisco IOS XE Catalyst SD-WAN Release 17.2.1v

Feature	Description
Systems and Interfaces	
Additional Commands Qualified for CLI Add-On Feature Templates	With each release, we qualify commands for use with CLI add-on feature templates. In this release, commands for the following were qualified: ACL, AppNav, AppQoE, Bridge Domain, BGP, BFD, Class Map, Crypto, EIGRP, Global Configuration, Interface GigabitEthernet, IP, Licensing, Logging, NAT, NTP, Object Group, OMP, OSPF, Policy, Policy Map, QoS Policy, RADIUS, Security, SNMP, SSL Proxy, System, UTD, Voice, VRF, Zone Based Firewall.

Supported Devices

For device compatibility information, see Cisco SD-WAN Device Compatibility.

Important Notes, Known Behavior, and Workaround

- Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- When you complete a Cisco SD-WAN software downgrade procedure on a device, the device goes into the configuration mode that it was in when you last upgraded the Cisco SD-WAN software on the device. If the device is in a different configuration mode when you start the downgrade than it was when you last upgraded, the device and Cisco SD-WAN Manager show different configuration modes after the downgrade completes. To put the configuration modes back in sync, reattach the device to a device template. After you reattach the device, both the device and Cisco SD-WAN Manager show that the device is in the vManage configuration mode.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, the behavior of the Cisco SD-WAN Overlay Management Protocol (OMP) routes changed. Cisco IOS XE Catalyst SD-WAN devices install OMP routes in the Route Information Base (RIB) including the interface.

  Example output starting from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r:

  ```
  m 192.168.1.0/24 [251/0] via 10.10.10.13, 00:00:50, Sdwan-system-intf
  ```

  Example output prior to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r:

  ```
  m 192.168.1.0/24 [251/0] via 10.10.10.13, 00:00:09
  ```

Note In cases where the static route's next-hop may recurse over an OMP route, the OMP route installation behavior change starting from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r installs the static route in the routing table, such as for the following configured static route:

```
ip route 192.168.100.0 255.255.255.0 192.168.1.1
```

The static IP route gets installed in the routing table starting from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

192.168.1.1 is considered fully resolved by way of OMP route 192.168.1.0/24 using 10.10.10.13 as the next-hop with an explicit specification of the egress interface (Sdwan-system-intf).

Prior to Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, 192.168.1.1 is considered unresolved because OMP route 192.168.1.0/24 using 10.10.10.13 as the next-hop does not have an explicit interface.

Cisco SD-WAN Manager Upgrade Paths

Table 3:

Starting Cisco SD-WAN Manager Version	Destination Version	
	19.2.x	**20.1.x**
18.x/19.2.x	Direct Upgrade	Direct Upgrade
20.1.x	Not Supported	Direct Upgrade
20.3.x	Not Supported	Not Supported
20.4.x	Not Supported	Not Supported

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Bugs for Cisco IOS XE Release 17.2.2

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

Resolved Bugs for Cisco IOS XE Release 17.2.2

Table 4: Resolved Bugs

Bug ID	Description
CSCvt01532	SD-WAN router running 16.10.3 crashes with cpp_cp_svr fault
CSCvt05373	SDWAN device and vmanage is not in sync when manual software reset is done
CSCvt12299	XE SD-WAN : Cannot specify the specific vpn except <1-512> in show sdwan app-fwd cflowd flows vpn x
CSCvt33358	SdwanDataPolicyDrops with centralized app route policy with invalid backup preferred color
CSCvt35444	XE SDWAN router crashes with cFlowd enabled
CSCvt50136	ASR1k - all Platform : Observing IpFragErr for EMIX traffic with basic IPSEC config
CSCvt76326	app-route policy logic is not working when backup pref color is config and primary not meeting sla
CSCvu38473	ISR1100-4GLTE not showing when SIM is Locked
CSCvv21398	sdwan multicast Cisco IOS XE rpf failure even with unicast route present in rib and omp

Open Bugs for Cisco IOS XE Release 17.2.2

Table 5: Open Bugs

Bug ID	Description
CSCvs29562	ISRv-Cisco IOS XE SD-WAN 16.12.1b RFC2544 IPv4 performance on CSP5436: 8VCPU SRIOV throughput degrade significant
CSCvs97077	Chassis number for platform getting modified when bootstrapped with a different platform config
CSCvt45700	[17.2.1]:policy service path and tunnel path commands stop working after reload
CSCvt63948	Enabling aggregate route in OMP causes OMP to crash and sends router into a repeated crash loop
CSCvt81979	ASR IOS-XE SDWAN router bfd sessions not coming up if BGP routing is not providing a local next hop.
CSCvu22463	ACL lost when interface is moved between VPNs
CSCvu46417	ASR 1000 crash when doing a FIB lookup
CSCvu53184	Cisco IOS XE SD-WAN - CLI should ask for confirmation of request software reset

Bug ID	Description
CSCvu53340	Template push is failing as Cisco SD-WAN Manager is trying to disable link recovery for cellular controller.
CSCvv11071	Cisco SD-WAN Manager is attempting to strip multiple LTE modem configs from ISR 1000 and template push fails
CSCvv14263	Day 0 Config Bringup after Power OFF/ON | C1121X-8PLTEP
CSCvv48632	"propagate-aspath" -> as-path not populated into BGP table for OMP route
CSCvv50783	IPSEC tunnels to AWS TGW failing when VPN tunnel doesn't allow all traffic
CSCvv55435	ASR1001-X ftmd crash: ftm_tunnel_sla_tunnels_get_object
CSCvv57506	Cisco IOS XE SD-WAN Device can not establish control connections automatically once last-resort-circuit is enable.
CSCvv58070	Automatic mode switch hangs when insufficient bootflash space
CSCvv66190	ISR 4000 crashed after 17.3.1 image installation
CSCvv66589	Cisco IOS XE SD-WAN Device is not able to ping its own loopback
CSCvv67689	Cisco IOS XE SD-WAN Device data-policy breaks SRST media stream with default-action accept or accept in sequence
CSCvv69449	Cisco IOS XE SD-WAN Device IR1101: 802.1x/MAB settings pushed to Cisco IOS XE SD-WAN Device via template missing from the device
CSCvv69614	CSR's launched by basic template going "Out of Sync"

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1v

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1v

Table 6: Resolved Bugs

Bug ID	Description
CSCvq42698	Update "bandwidth remaining percent" doesn't take effective reliably on datapath
CSCvr09310	vManage should be able to work with cEdge banners in the same way as with vEdges
CSCvs96540	SDWAN device admin-tech has empty "show running config" in /tech/ios file
CSCvt10750	QoS policy config "random-detect" gets lost after upgrade cEdge image from 16.12 to 17.2 release
CSCvt16988	Existing configuration on a cEdge could not be modified by a new template

Bug ID	Description
CSCvt18190	Router crash when doing 'show bgp ipv6 unicast summary'
CSCvt21833	Per-Tunnel QoS policy doesn't take effective with IPv6 TLOC
CSCvt28541	XE SD-WAN : cflowd not working after re attaching template
CSCvt58825	qfp-ucode-tsn-le core observed while executing cExpress suites for TSN platform
CSCvt80226	vmanage throws error when attempting to push cli template with "ip multicast route-limit 2147483647"
CSCvt80373	"no ip address" not shown in "show sdwan run" for cellular interfaces
CSCvt98034	BGP communities: changes to route-map which sets BGP communities discards existing communities
CSCvu14946	Cloud onRamp SaaS not working on ASR1k
CSCvu18773	[DyT]: Cxp doesn't compute loss/latency even with reachability due to Tracker status down
CSCvs84169	IPSec HMAC drops between after stress traffic and link flap

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1v

Table 7: Open Bugs

Bug ID	Description
CSCvs75489	New Password is asked even when the Template used a non default admin Password
CSCvt01532	SD-WAN router running 16.10.3 crashes with cpp_cp_svr fault
CSCvt05373	SDWAN device and vmanage is not in sync when manual software reset is done
CSCvt12299	XE SD-WAN : Cannot specify the specific vpn except <1-512> in show sdwan app-fwd cflowd flows vpn x
CSCvt33358	SdwanDataPolicyDrops with centralized app route policy with invalid backup preferred color
CSCvt35353	Manually configured TCP MSS adjust does not affect datapath
CSCvt35444	XE SDWAN router crashes with cFlowd enabled
CSCvt54384	FTMD: Connection to DBGD went down during cedge speedtest and router crashes
CSCvt73140	CLI Device template: Config Preview fails with server error
CSCvt50136	ASR1k - all Platform: Observing IpFragErr for EMIX traffic with basic IPSEC config

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

Table 8: Resolved Bugs

Bug ID	Description
CSCvq65906	admin/admin credentials are lost after reload
CSCvq71198	Customer has to be enforced for admin password changes with new boot up cEdge router
CSCvq75871	SDWAN ipsec anti-replay drops for all packets when NAT session flap
CSCvq84015	ISR1100 not booting up after power cycle and gets stuck in boot loop - cdb itself gets corrupted
CSCvq88669	C1111-8P -- Crash with ipv4_nat_alg_get_appl
CSCvr27819	Add/remove of symmetric nat on WAN link multiple times makes the link BFDs down forever
CSCvr36383	Next-hop is missing from route table for default route when change from WAN to sub-interface
CSCvr42619	No ARP ping packets generated after loading xe-sdwan 16.10.3a image on asr1k
CSCvr47688	local data policy classification issue with prefix less specific than /24 on ISR1100 platform
CSCvs38028	cEdge_Policy_regression: Service IPv6 ping is failing if the interface vrf forwarding is replaced
CSCvs48162	Seeing IpsecOutput drop for cEdge even though ip packet size is less than 1442.
CSCvs63841	SDWAN ISR1100: No SW Image listed when .bin image booted from flash / usb
CSCvs90207	On cEDGE all the BFD session flap if there is a control connection flap to vmanage
CSCvs98389	Packet drops in XE-SDWAN because of "IN_CD_COPROC_ANTI_REPLAY_FAIL" errors
CSCvt28357	Cloudexpress Symlinks missing for httping, timeout, nslookup utility in ASR1K
CSCvt30545	Probe reported 100% Loss for SaaS while network and configuaration are all good.
CSCvt37676	cEdge crashes after changing flow-sampling-interval within a cflow policy
CSCvt50461	cEdge crashes after the push of a template for Umbrella
CSCvs17374	cEdge TSN local datapolicy remove/add ACL feature-manager exmem-usage changed

Bug ID	Description
CSCvt06922	hidden policies and classifiers IOS native yang model config from "show sdwan running-config"
CSCvs35368	ISR 4331 rebooted with "CPU Usage due to Memory Pressure exceeds threshold" when running traffic
CSCvt30974	BFD connections are down after the tear down of extra vsmart and TLOC delete during GR
CSCvt79990	Enable/Disable SSLproxy CLI needs to be removed as it is not effective for ISR4321 and ASR1k
CSCvs84169	IPSec HMAC drops between after stress traffic and link flap

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

Table 9: Open Bugs

Bug ID	Description
CSCvs96540	SDWAN device admin-tech has empty "show running config" in /tech/ios file
CSCvs96732	SDWAN cEdge VRRP fail recovery take 10-15 mins for OMP tracking, with prefix list tracking no output
CSCvt04548	cEdge is not displaying BFD "up" alert although the tunnel shows to be up on the device
CSCvt05373	SDWAN device and vmanage is not in sync when manual software reset is done
CSCvt28541	XE SD-WAN : cflowd not working after re attaching template
CSCvt35444	XE SDWAN router crashes with cFlowd enabled
CSCvt44918	Incorrect PMTU programmed for XE SDWAN router tunnel control-plane while data-plane is correct
CSCvt51383	ISR1127- Not able to push template.
CSCvt55610	BFD session not able to form - stuck in create state
CSCvt21833	Per-Tunnel QoS policy doesn't take effective with IPv6 TLOC
CSCvt45700	[17.2.1]:policy service path and tunnel path commands stop working after reload
CSCvt58825	qfp-ucode-tsn-le core observed while executing cExpress suites for TSN platform
CSCvt63948	Enabling aggregate route in OMP causes OMP to crash and sends router into a repeated crash loop
CSCvq42698	Update "bandwidth remaining percent" doesn't take effective reliably on datapath

Bug ID	Description
CSCvt76792	AppQoE SN not coming up intermittently due to TCP config callback not received from confd
CSCvt74694	Cert validation failures seen for traffic after template push with SSL
CSCvt76326	app-route policy logic is not working when backup pref color is config and primary not meeting sla
CSCvt50136	ASR1k - all Platform: Observing IpFragErr for EMIX traffic with basic IPSEC config

Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for Cisco IOS XE Routers
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Deferral Notices
- Cisco Bulletins

© 2020–2021 Cisco Systems, Inc. All rights reserved.