AOS-CX 10.10.1060 Release Notes

9300 Switch Series

a Hewlett Packard Enterprise company

Published: May 2023

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Products supported

This release applies to the Switch Series. The following table lists any applicable minimum software versions required for that model of switch.

If your product is not listed in the below table, no minimum software version is required.

Product number	Product name	Minimum software version
R9A29A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Front-to-Back 6 Fans 2 AC PSU Bundle	10.10.1000
R9A30A	Aruba 9300-32D 32p 100/200/400G QSFP-DD 2p 10G SFP+ Back-to-Front 6 Fans 2 AC PSU Bundle	10.10.1000
R8Z96A	Aruba 9300-32D 32-port 100/200/400G QSFP-DD 2-port 10G Switch	10.10.1000

Important information for 9300 Switches

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Diffie-Helman algorithm is no longer enabled by default for key exchange. To enable using Diffie-Helman for key exchange, use the command `ssh key-exchange-algorithms <KEY-EXCHANGE-ALGORITHM-LIST>`."

AOS-CX BGP implementations support resolving a BGP route's nexthop to a default route (0.0.0.0/0). However, this is not generally recommended in network deployments. Considering the default route to be the last resort route, resolving the BGP route's nexthop to a default route can cause potential routing loops in the network, if they are not properly designed and monitored. Route flaps and/or traffic drops may be observed in such cases.

In a future release, AOS-CX will not support the BGP route's nexthop resolving to a default route in the Route table. To avoid this problem and to be prepared for the update, Aruba recommends configuring a more specific static route (or host route) for BGP nexthops that are multihops away that are resolving via the default route.

If using the Web UI, you should clear the browser cache after upgrading to this version of software before logging into the switch using a Web UI session. This will ensure the Web UI session downloads the latest changes.

If a switch has RPVST enabled and the native VLAN ID configured for a trunk interface is not the default VLAN ID 1, and the native VLAN ID is also used as the management VLAN, the switch may not be accessible over the trunk interface after upgrading from any 10.04.00*xx* version of software.
To fix the issue after an upgrade, log into the switch using the OOBM interface or serial port console and configure the following:

```
switch# configure
switch(config)# spanning-tree rpvst-mstp-interconnect-vlan <VLAN_ID>
```

where *<VLAN_ID>* is the native VLAN ID configured on the trunk interface.
If there are multiple trunk interfaces configured on the switch, each with a different VLAN ID, contact the Aruba Support Team.

To upgrade to:	Your switch must be running this version or later ***
AOS-CX 10.10.xxxx Note: 10.10 is an LSR, recommended release is 10.10.10xx.	AOS-CX 10.06.0110

**** Note that all switch models may not support this minimum upgrade version.*

Refer to the Approved Product Lists sites for the Common Criteria, FIPS 140-2 and DoDIN APL to obtain the product certification details. Products should be used as evaluated and defined in the respective configuration guides.

- Common Criteria: https://www.niap-ccevs.org/Product/
- FIPS 140-2: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search
- DoDIN APL: https://aplits.disa.mil/processAPList.action

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open-source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

```
Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
U.S.A.
```

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at: https://hpe.com/software/opensource

Version history

All released versions are fully supported by Aruba, unless noted in the table.

Version number	Release date	Remarks
10.10.1060	2023-05-04	Released, fully supported, and posted on the Web.
10.10.1050	2023-03-17	Released, fully supported, and posted on the Web.
10.10.1040	2023-02-08	Released, fully supported, and posted on the Web.
10.10.1030	2022-12-08	Released, fully supported, and posted on the Web.
10.10.1020	2022-11-07	Released, fully supported, and posted on the Web.
10.10.1010	2022-09-22	Released, fully supported, and posted on the Web.
10.10.1000	2022-08-14	Initial release of AOS-CX for the 9300 Switch Series.

Compatibility/interoperability

The switch web agent supports the following web browsers:

Browser	Minimum supported versions
Edge (Windows)	41
Chrome (Ubuntu)	76 (desktop)
Firefox (Ubuntu)	56
Safari (MacOS)	12
Safari (iOS)	10 (Version 12 is not supported)

Internet Explorer is not supported.

Recommended versions of network management software for switches found in this release note:

Management software	Recommended version(s)
NetEdit	2.6.1
Aruba Fabric Composer	6.2.0
Aruba CX Mobile App	2.8.4
Network Automation	10.10, 10.11, 10.20, 10.21, 10.30, 10.40
Network Node Manager	10.10, 10.20, 10.21, 10.30, 10.40

For more information, see the respective software manuals.

To upgrade software using NetEdit, make sure to upgrade to the above version of NetEdit first and then execute the switch software upgrade on devices discovered by this version of NetEdit.

Enhancements

This section lists enhancements added to this branch of the software.

The number listed with the category is used for tracking purposes.

Enhancements for 9300 Switches in AOS-CX 10.10.1060

There are no enhancements introduced in this release.

Fixes

This section lists released builds that include fixes found in this branch of the software. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

For a list of issues fixed in previous releases, refer to the AOS-CX Release Notes Portal.

The Bug ID is used for tracking purposes.

Resolved issues for 9300 Switches in AOS-CX 10.10.1060

Category	Summary	Description
BGP	242032	**Symptom**: BGP peers are unable to ping the loopback configured in VRF-A although the loopback route is leaked into VRF-B from VRF-A. **Scenario**: This issue occurs in a deployment with two VRFs where both are configured for dynamic Route Leaking, when the switch has an iBGP peering in VRF-B, and connected loopbacks are redistributed using BGP from VRF-A to VRF-B. Although routing tables appear correctly on both VRFs, the loopback is not advertised by the egress VRF-A.
Central	258065	**Symptom**: A switch will not be able to establish a connection with an Activate server and Central server. **Scenario**: In order to authenticate with Central, mutual authentication is performed via certificates. An AOS-CX switch sends its device certificate (DevID) when a connection with Central or Activate is established, and Central/Activate then validates this certificate against a certificate authority (CA). Access to the TPM module can be blocked if three simultaneous accesses are made by the SW internal processes. When blocked, any process reading the private key will get stuck waiting for an answer. If an ISP is down, and the switch makes several attempts to connect with

Category	Summary	Description
		Activate, the TPM is blocked, and every new connection with Activate times out.
L3 addressing	253444	**Symptom:** Users are unable to configure a reserved IPv6 anycast address on an interface. **Scenario:** This issue occurs while configuring an IPv6 address with the interface identification field **ffff**.
PKI	252882	**Symptom:** Certificate verification on the switch for a service or client trying to connect to switch may fail at the OCSP verification stage for some PKI configurations. **Scenario:** This issue can occur if the peer certificate representing the remote server or client has an OCSP URL embedded, and if its OCSP signer CA certificate is an intermediate certificate and installed as a TA profile in the switch before its root CA and other higher CAs in the certificate chain.
REST	256915	**Symptom:** TACACS+ Authorization packets are sent with empty values in the remote address field for REST-API based user sessions, causing the firmware upgrade to fail. **Scenario:** While using the REST API on the switch with TACACS+ Authorization configured, the switch will send a request packet with an empty value for the remote address field. Some TACACS+ servers require the remote address field to contain a unique value to identify the network device. The requests would be rejected without a valid remote IP address. **Workaround:** Check if the TACACS+ server supports ignoring the remote address field.
SSH	257866	**Symptom:** The command **checkpoint auto <timeout>** fails and generates the error message, **Failed to create bus connection: Permission denied.** **Scenario:** This issue occurs when a user with the same username exists locally and remotely. If SSH authentication succeeds with RADIUS or TACACS+, the user account of the user that logs in will be slightly incorrect. This error causes the checkpoint command to fail due to permissions. **Workaround:** When the **checkpoint auto <timeout>** command fails due to this reason, when the switch is booted again the configuration will revert back to the configuration that was present when the checkpoint auto command was called. To avoid this side effect, issue the command **erase checkpoint TEMPAUTOCHECK**, which is intended for this purpose only.
VSX	258006	**Symptom**: In a VSX scaled environment, the MCLAG links take a long period of time to move to the forwarding or up state. **Scenario**: During the software upgrade process, a secondary device upgrades first, followed by the primary device. If the links are taking more than a minute to come up, then in order to continue the software upgrade, the secondary notifies the primary to start the upgrade, which will bring down the links on the primary. As a result, traffic loss can occur since the links are down on both sides. **Workaround:** Manually upgrade the VSX software in a scaled VSX environment.

Feature caveats

The following are feature caveats that should be taken into consideration when using this version of the software.

Feature	Description
BGP	If a route-map is applied and none of the routes satisfy the match condition(s) in any of the route-map entries, then all routes are dropped.
TFTP	Blocksize greater than 1480 is not supported in 4100i, 6100 and 6000 Switch series.
VRRP	The same virtual link-local address cannot be used across different VRFs.
VRRP	MD5 authentication interoperation is not supported with Comware-based switches
REST	Boundary values for **match vni** and **set local preference** in a route-map system cannot be set via the REST API and must be manually configured on the switch via the CLI.

BGP	In multi-VRF environments, while performing mutual route leaking on the VRRP peers with BGP neighborship established in between and towards the upstream network, the switch will install both routes as ECMP instead of preferring the leaked route. Use route-maps to give lower/higher preference to the routes received from an iBGP peer. For example:
	`!`
	`route-map rmap permit seq 10`
	`set local-preference 50`
	`!`
	`router bgp 100`
	`vrf red`
	`neighbor 1.1.1.2 remote-as 100`
	`address-family ipv4 unicast`
	`neighbor 1.1.1.2 activate`
	`neighbor 1.1.1.2 route-map rmap in`
	`exit-address-family`
	In the above example, since a lower value of local-preference (i.e. 50, whereas default value is 100) has been set to the routes received from iBGP peer, the leaked routes get preferred and get installed as best routes.

DHCP Server DHCP Relay DHCP Snooping	Note the following caveats for these features: ▪ DHCP Relay and DHCP Snooping can co-exist on the same switch. DHCP Snooping and DHCP Server cannot co-exist on the same switch. ▪ DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.

BGP	The **next-hop-unchanged** option needs to be explicitly configured to preserve nexthop while advertising routes to eBGP peers, in the L2VPN EVPN address-family. For example:
	`router bgp 1`
	`neighbor 1.1.1.1 remote-as 2`
	`address-family l2vpn evpn`
	`neighbor 1.1.1.1 activate`
	`neighbor 1.1.1.1 next-hop-unchanged`
	`neighbor 1.1.1.1 send-community extended`
	`exit-address-family`
	`!`

Classifiers	Classifier policies, IPv6 and MAC ACLs are not supported on egress.
Classifiers	DSCP remarking is performed only on routed packets.

Feature	Description
Classifiers	For Classifier policy modifications to be secure, Aruba strongly encourages modifications be done as a three-step process: Bring down the port, modify, and bring the port back up.
Classifiers	IPv4 egress ACLs can be applied only to route-only ports.
Classifiers	Policies containing both MAC and IPv6 classes are not allowed.
CMF	Automatic downgrade of the startup-config is not supported during a software downgrade.
CMF	No other checkpoint besides "startup-configuration" gets migrated during the upgrade process.
Counters	Classifier Counters: Max number Classifier entries with count action: JL363A=32K, JL365A=32K, JL366A=16K.
Counters	Counters are shared between ACL and Layer 3 ports. The Max number of ACL entries with count action plus Layer 3 counters is: JL363A=24K, JL365A=24K, JL366A=8K. Enabling counters on a Layer 3 port consumes 6 ACL counter entries.
Counters	Layer 3 Route-only port counters are not enabled by default. Enabling them will remove them from the counter resources shared with ACLs.
DHCP Server, DHCP Relay, and DHCP Snooping	DHCP Snooping and DHCP Server cannot co-exist on the same switch. DHCP Snooping, DHCP Relay, and DHCP Server together cannot co-exist on the same switch.
EVPN	iBGP split-horizon rule is not followed between different address families. Use route-map to block the routes getting advertised to the iBGP peer.
ICMP Redirect	The switch may only software forward an 100pps IP frame that triggers ICMP redirect.
ICMP Redirect	The switch may incorrectly duplicate an IP frame that triggers ICMP redirect.
IGMP/PIM on Loopback and GRE interfaces	▪ IGMP cannot be enabled on both Loopback and GRE interfaces. ▪ PIM can be enabled on a Loopback interface. ▪ PIM will not work on GRE tunnels and 6in6.
Multicast and VXLAN	▪ VXLAN must be configured prior to configuring VSX. ▪ IPv6 multicast is not supported for VXLAN overlay. ▪ Multicast support for static VXLAN in the overlay has limited support. Contact Aruba Support for details.
MVRP and VSX	MVRP is mutually exclusive with VSX.
Network Analytics Engine (NAE)	After management module failover, up to 5 minutes of alert history could be lost.
Network Analytics Engine (NAE)	Agents monitoring a resource that has column type enum with a list of strings (as opposed to a single string enum) is not supported.
Network Analytics Engine (NAE)	Network Analytics Engine (NAE) agents execute Command Line Interface (CLI)

Feature	Description
	actions as 'admin' user, so they have permission to run any command by default. However, when the authentication, authorization and accounting (AAA) feature is enabled, the same restrictions applied to 'admin' will also apply to NAE agents. When using AAA, make sure to give the admin user the permissions to run all commands needed by enabled NAE agents. Otherwise, some CLI commands may be denied and their outputs won't be available. Actions other than CLI won't be affected and will execute normally. Also, NAE agents won't authenticate, thus the AAA service configuration must not block authorization for unauthenticated 'admin' user. ClearPass doesn't support such configuration, so it cannot be used as a TACACS+ server.
Network Analytics Engine (NAE)	The following tables are not supported for NAE scripts: OSPF_Route, OSPF_LSA, OSPF_Neighbor, BGP_Route.
OSPF	OSPFv2 and OSPFv3 do not support detailed LSA **show** commands.
RADIUS	Authorization by means of HPE VSAs is not supported.
REST	REST supports the 'admin' and 'operator' roles but does not work with TACACS+ command authorization.
RIP/RIPng	Redistribute RIP/RIPng is not supported in BGP/BGP+.
RIP/RIPng	RIP/RIPng metric configuration support is not available.
RPVST+ and MSTP	Spanning Tree can only run in MSTP or RPVST+ mode.
RPVST+ and MVRP	RPVST+ is mutually exclusive with MVRP.
sFlow and Mirroring	sFlow and port mirroring are mutually exclusive per port. A port cannot support both sFlow and mirroring at the same time.
Sub-interface	BFD is not supported on a sub-interface. A sub-interface as underlay for EVPN-VXLAN is not supported
UDLD	For a UDLD-enabled interface to not lose traffic during a failover operation, the result of multiplying 'interval' and 'retries' should be at least 8 seconds. The default values are 7000 ms (interval) x 4 (retries) = 28 seconds.
Tunnels	When configuring tunnels (VXLAN/IP tunnels) with the underlay as a static route, the next-hop IP should be an SVI or ROP IP and not configured as the Active-Gateway.
VRF	VRF names are limited to 31 characters.
VRRP	The same virtual link-local address cannot be used across different VRFs.
VRRP-MD5 authentication interop	Not supported with Comware-based switches
VRRP and VXLAN	VRRP and VXLAN are mutually exclusive.
VSX and Static VXLAN	Static VXLAN on VSX configuration is not supported. Use VSX and EVPN or VSX and HSC.
VXLAN	DSCP-enabled packets carried in a VXLAN tunnel are treated as best-effort traffic.
VXLAN	Static vxlan is not supported.

Known issues

The following are known open issues with this branch of the software. The **Symptom** statement describes what a user might experience if this is seen on the network. The **Scenario** statement provides environment details and trigger summaries. When available, the **Workaround** statement provides a workaround to the issue.

Category	Bug ID	Description
VXLAN	226965	**Symptom**: Continuous ICMP6 Echo Reply packets are sent for single ICMP6 Echo Request. **Scenario**: This issue occurred when a ping was sent from a host to a switch virtual interface (SVI) IPv6 address on the switch, where the host is reachable over an L3VNI. **Workaround**: Issue the command **no ip icmp redirect**.

Chapter 2
Other resources

Aruba is committed to ensuring you have the resources you need to be successful. Check out these learning and documentation resources:

- AOS-CX switch software documentation portal: https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
- AOS-CX 10.10 playlist of technical training videos on YouTube: https://www.youtube.com/playlist?list=PLsYGHuNuBZcZmHTZQC9LuivtrVecOx5vk

Chapter 3
Aruba security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

The Aruba security policy can be found at https://www.arubanetworks.com/en-au/support-services/sirt/. Security bulletins can be found at https://www.arubanetworks.com/en-au/support-services/security-bulletins/. You can sign up at https://sirt.arubanetworks.com/mailman/listinfo/security-alerts_sirt.arubanetworks.com to initiate a subscription to receive future Aruba Security Bulletin alerts via email.