Cisco Policy Suite 26.1.0 Release Notes for vDRA

First Published: April 23, 2026

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 26.1.0. Use this Release Note in combination with the documentation listed in the *Related Documentation* section.

NOTE: The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

This Release Note includes the following sections:

New and Changed Feature Information

For information about a complete list of features and behavior changes associated with this release, see the *CPS Release Change Reference*.

Installation Notes

Download ISO Image

Download the 26..1.0 software package (ISO/VMDK image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/CPS_26.1.0

Md5sum Details

DRA

73ddbe4910a7dd92b986e860397a6def	CPS_Microservices_DRA_26.1.0_Base.release.vmdk.SPA.tar.gz
3768305e8d35786fa5ecac7eb9997f8f	CPS_Microservices_DRA_26.1.0_Deployer.release.vmdk.SPA.tar.gz

3164083224fd9ac2fae2b8da3880b70e	CPS_Microservices_DRA_26.1.0.release.iso.SPA.tar.gz
9e5c50cae24775459a1fb90b1c24341d	CPS_Microservices_DRA_Binding_26.1.0.release.iso.SPA.tar.gz

Component Versions

The following table lists the component version details for this release.

Table 1 - Component Versions

Component	Version
Core	26.1.0
Custom Reference Data	26.1.0
DRA	26.1.0
Microservices Enablement	26.1.0

Additional security has been added in CPS to verify the downloaded images.

Image Signing

Image signing allows for the following:

- Authenticity and Integrity: Image or software has not been modified and originated from a trusted source.
- Content Assurance: Image or software contains code from a trusted source, like Cisco.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the md5sum checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image on cisco.com.

If md5sum is correct, run *tar -zxvf* command to extract the downloaded file.

The files are extracted to a new directory with the same name as the downloaded file name without extension (.tar.gz).

The extracted directory contains the certificate files (.cer), python file (cisco_x509_verify_release.py), digital certificate file (.der), readme files (*.README), signature files (.signature) and installation files (.iso .vmdk, .qcow2 and .tar.gz).

Certificate Validation

To verify whether the installation files are released by Cisco System Pvt. Ltd and are not tampered/modified or infected by virus, malware, spyware, or ransomware, follow the instruction given in corresponding *.README file.

NOTE: Every installation file has its own signature and README file. Before following the instructions in the README file, make sure that cisco.com is accessible from verification server/host/machine/computer. In every README file, a Python command is provided which when executed connects you to cisco.com to verify that all the installation files are released by cisco.com or not. Python 2.7.4 and OpenSSL is required to execute cisco_x509_verify_release.py script.

New Installations

- VMware Environment

VMware Environment

To perform a new installation of CPS 26.1.0 in a VMware environment, see the *CPS vDRA Installation Guide for VMware*.

Prerequisite for upgrading to 26.1 from 25.x / 24.2.0

NOTE: If upgrade from 25.x planned, then this pre-requisite not required.

The following are the common prerequisites:

1. Run the following CLI before upgrade:

   ```
   #database genericfcvcheck 6.0
   ```

   NOTE: Make sure to run the above CLI before upgrade and / or downgrade on all sites.

2. Specify any one of the CLI options:

   a. **Set**: This option checks and sets FCV only on primary.

   NOTE: We recommend to use Set option first and then Check to make sure that FCV is replicated on secondary members. Upgrade/downgrade should not be triggered if any error is found in above CLI or FCV is not replicated on secondary members. Make sure to resolve the CLI error, rerun the CLI, and then only proceed for upgrade or downgrade.

   b. **Check**: This option only checks FCV on all members (primary, secondary, and arbiter).

3. Run the following CLI before upgrade:

   ```
   #database dwccheck
   ```

   NOTE: CLI automatically takes care of Default Write Concern version on all databases. This CLI will be available in 24.2 P1 and if it is upgraded from 24.2 CCO then the following steps should be performed manually.

4. Specify any one of the CLI options:

   a. **Set**: This option checks and sets dwc on primary members.

   b. **Check**: This option only checks dwc on all members.

   (set/check) << set

   i. **Set**: This option checks and sets defaultWriteConcern.

   ii. **Check**: This option only checks only checks defaultWriteConcern on all members(primary/secondary).

Additional Notes

This section provides additional notes necessary for proper installation/working of CPS.

- **CSCwq27394:** Upgrade Prometheus to 3.5.0 version

  Issue: During upgrade, there is a risk of up to 2 hours of data loss. In-memory and uncompacted data stored by Prometheus may not be fully written to disk, resulting in up to a 2-hour gap in Grafana data.

  Workaround: The Prometheus binary in Prometheus containers has been upgraded from version 2.3.1 to 3.5.0:

- The data directory for the new Prometheus 3.5.0 binary is:
    - On the VM: /stats/prometheus-hi-res/3.5
    - In the container: /data-3
- The data directory for the old Prometheus 2.3.1 binary is:
    - On the VM: /stats/prometheus-hi-res/2.0
    - In the container: /data-2
- All existing Prometheus data will remain in the /data-2 directory
- All new Prometheus data will be stored in the /data-3 directory
- Ensure Prometheus is shut down gracefully before starting the upgrade by running the following command:

```
docker exec prometheus- "supervisorctl stop all"
```

In case if the Prometheus containers are unhealthy and the upgrade is not proceeding, follow the below steps:

Delete Wal folder in all prometheus containers & restart all process inside container

```
1) rm -rf /data-2/wal/*

2) supervisorctl restart all
```

- **CSCwt68223** - Frequent REPL logs: "Cannot select sync source because it is not readable" due to an arbiter being considered as a sync source candidate.

  Issue - Some secondary members are generating the following MongoDB REPL log message, with the candidate host pointing to arbiter member IPs:

  Cannot select sync source because it is not readable

  (REPL component, id: 3873107, ctx: ReplCoordExtern-0)

  This indicates that the secondary evaluated an arbiter as a potential sync source and then rejected it, even though it is syncing from primary. This process continues until MongoDB is restarted. Arbiters are vote-only replica-set members and do not store replica-set data, so they are not valid readable sync sources.

  Workaround: The following runtime script can be used as a mitigation to refresh the sync source on affected secondary members by directing them to a valid data-bearing member

  ```
  /var/broadhop/cli/mongo-sync-source-refresh-runtime <cluster-id> <shards> --check | --set
  ```

  Notes:

  - --check validates the current sync-source condition without making changes
  - --set applies the mitigation on the targeted shard members
  - This is a mitigation, not a permanent product fix
  - The workaround uses MongoDB's supported sync-target override approach (replSetSyncFrom) to direct secondaries to a valid sync source. MongoDB notes that secondaries can be configured to sync from a specific member, subject to replica-set sync-target rules.
  - A 20 MB MongoDB log file is compressed to approximately ~2 MB (.gz) due to repetitive log patterns with 10 rotated files.

- No functional and replication impact observed. Replica-set members are healthy, and replication is working as expected.

Open and Resolved CDETS

The following sections list open and resolved CDETS for this release. For your convenience in location CDETS in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description.

NOTE: If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website: https://tools.cisco.com/bugsearch

To become a registered cisco.com user, go to the following website: https://tools.cisco.com/RPF/register/register.do?exit_url=

Open CDETS

The following table lists the open CDETS in this release.

Table 2 - vDRA Open CDETS

CDETS ID	Headline
CSCwq11542	In fPAS, slowness is seen when connecting mtls-ipv6-client peers in overlay network
CSCwr12961	During Active-Active and Failover longevity,observed Rx_AAR timeouts when setup is in Overlay and mongo_TLS enabled
CSCwr13040	Mongo over TLS Enabled (All Sites) + Overlay Network, Non-VoLTE traffic fails
CSCwr50315	SSLHandshakeFailed error msgs seeing in db logs on requireTLS mode on orchestrator container
CSCwt68333	Gx CCR-I timeout when enabling IPC pirority threadpool in PB
CSCwt78810	API call, expected output is KEY column should be the first and rest of the column should be listed. Order is now reversed. **Note**: Use the schema parameter as true at the end of the API ("?schema=true"). This will ensure the correct column output order.

Resolved CDETS

This section lists the resolved/verified CDETS in this release.

Table 3 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwo62460	Command to view the DRA VMDK Versions
CSCwr02395	vDRA/ Rx_STR Looping caused in DRA Relay Scenario due to AF FQDN in both Origin and Destination Host AVPs
CSCwr26245	Grafana data loss observed after DB/DRA ISO upgrades in 25.2 Sprint7
CSCwr56246	Removal of a local user account named 'ubuntu' on the virtual machine drc01 in the fPAS DRC01 VM.
CSCwr57702	Grafana dashboard is not empty despite queries being enabled
CSCwr79628	Alert for Peer Connection throttle is fluctuating

CDETS ID	Headline
CSCwr95446	CPS vDRA, 23.2, Gx CCRI Timeouts are being seen during MSISDN Bindings Removal from lab
CSCws06928	GNU binutils,libxml2,Linux kernel,libssh,Bind,Samba Vulnerabilities
CSCws11933	Add support for logback in orchestrator jar
CSCws21344	vDRA HealthCheckUp process to consider details in Systems-default xmi as well
CSCws28723	Add timeout value and default value for cps deployment script
CSCws65433	urllib3,GNU binutils,libpng,Linux kernel,python-apt,CUPS vulnerabilities
CSCws66653	DRA MongoDB version upgrade for CVE-2025-14847 Vulnerability
CSCws69224	Add CLI support for tracking/displaying reachability of all replicaset members and DB VMs
CSCwt01048	Enable / disable or configuring network compressors (snappy, zstd, zlib) for mongoDB instance
CSCwt17966	Apache HTTP,Avahi ,pyasn1,libxml2,GNU vulnerabilities
CSCwt31534	Show database status takes 10-20 mins to update status
CSCwt37695	Update the destination_host, destination_realm, peer_group labels in peer_message_total kpi only when debug enabled
CSCwt43696	Peers getting connected despite rule being set to Deny
CSCwt56723	Upgrade fluentbit to 4.2.2
CSCwt68183	Linux kernel,curl,PostgreSQL,NSS,Intel Microcode Vulnerabilities
CSCwt71869	Add CLI to show fluentbit cluster status
CSCwt72044	VIM vulnerabilities
CSCwt78582	pyOpen,LibTIFF,systemd,Bind,Vim Vulnerabilities

Related Documentation

This section contains information about the documentation available for Cisco Policy Suite.

Release-Specific Documents

For more information on the Cisco Policy Suite, refer to the documents for this release available at:

https://www.cisco.com/c/en/us/support/wireless/policy-suite-mobile/products-installation-and-configuration-guides-list.html.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation, at:
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.