Cisco Policy Suite 26.2.0 Release Notes for vDRA

First Published: Oct 23, 2026

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 26.2.0. 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
- Installation Notes
- Limitations
- Open and Resolved CDETS
- Related Documentation
- Obtaining Documentation and Submitting a Service Request

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 26.2.0 software package (ISO/VMDK image) from:
https://software.cisco.com/download/home/284883882/type/284979976/release/26.2.0

Md5sum Details

DRA

85d5f97fee85ff8c9c38215e0f2e9fcc	CPS_Microservices_DRA_26.2.0.release.iso.SPA.tar.gz
7183b5943119cb991f9092719335bf8e	CPS_Microservices_DRA_Binding_26.2.0.release.iso.SPA.tar.gz

Cisco Confidential

c85f035a8e3ec9835ca80eb25f17bd85	CPS_Microservices_DRA_26.2.0_Base.release.vmdk.SPA.tar.gz
d108d00c563e5d7410697f496fb05533	CPS_Microservices_DRA_26.2.0_Deployer.release.vmdk.SPA.ta

Component Versions

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

Table 1 - Component Versions

Component	Version
Core	26.2.0
Custom Reference Data	26.2.0
DRA	26.2.0
Microservices Enablement	26.2.0

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 26.2.0 in a VMware environment, see the *CPS vDRA Installation Guide for VMware*.

Prerequisite for upgrading to 26.2 from 26.1

The following are the common prerequisites:

1. Run the following CLI before upgrading:

   #database genericfcvcheck 7.0

   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 using 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.

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).

Prerequisite for upgrading Ubuntu 24.04

Before performing an ISSM upgrade or downgrade between CPS DRA 26.1 and 26.2, ensure that the required Consul snapshot from the running 26.1 cluster is available.

1. Ensure that the VMware ESXi host is version 7.0 or later.
2. Before upgrading from CPS DRA 26.1 to 26.2, verify that all seven Consul servers (consul-1 through consul-7) are HEALTHY:

   #show consul-status

3. Take a snapshot of the running CPS DRA 26.1 cluster (Consul 1.5.3) before the upgrade:

   #consul save-snapshot consul-1.5.3-backup

4. Verify that the snapshot is saved and record its name:

#consul list-snapshots

NOTE: Use the saved 26.1 snapshot for a downgrade to 26.1. Consul 1.18.0 and Consul 1.5.3 are not backward-compatible at the Raft log level; a snapshot created on 26.2 cannot replace the required 26.1 snapshot.

5. Before downgrading to 26.1, include the consul-downgrade option and the saved snapshot name with the system downgrade CLI command.

Downgrade troubleshooting workaround

Consul Raft leader unavailable

If consul-1 through consul-3 restart repeatedly or Consul logs report invalid CA or Intention operations, the cluster might not have a Raft leader.

1. Follow the Consul cleanup and snapshot restore procedure in the CPS Troubleshooting Guide. Clear incompatible Consul 1.18.0 Raft data and restore the saved 26.1 snapshot.
2. Restart the Consul services. Continue after at least five Consul servers are HEALTHY.

haproxy-common containers remain in STARTING

The orchestrator scheduler might stall while haproxy-common containers remain in STARTING.

3. Restart the orchestrator container on the host:

#docker restart orchestrator

4. Wait approximately 30 seconds. Connect to the orchestrator and check the programs:

#docker connect orchestrator

#supervisorctl status all

5. If a haproxy-common container remains in STARTING, identify and restart that container:

#show docker service | tab | include haproxy-common

#docker restart haproxy-common-s101

HAProxy fails in diameter-endpoint or binding containers

If an affected container reports HAProxy FATAL or remains unhealthy after downgrade, apply these steps in that container.

1. Remove the # Overrides: comment from /etc/resolv.conf. Write the filtered content back to the existing file; do not replace the bind-mounted file with a rename.

tmp=/tmp/resolv.conf.$$ && sed '/^# Overrides:/d' /etc/resolv.conf > "$tmp" && cat "$tmp" > /etc/resolv.conf && rm -f "$tmp"

Confirm that the comment is gone. The command should return no output:

grep 'Overrides' /etc/resolv.conf

2. Inspect the sibling helper script without modifying it, and restore /usr/local/bin/run-haproxy as the wrapper for the HAProxy binary.

cat /usr/local/bin/run-haproxy-process

cat > /usr/local/bin/run-haproxy << 'EOF'

#!/bin/bash

exec /usr/local/sbin/haproxy -f /etc/haproxy/haproxy.cfg -W -db

EOF

chmod +x /usr/local/bin/run-haproxy

3. Identify the malformed lbvip02 entry in /etc/haproxy/haproxy.cfg:

grep -n 'Overrides\|lbvip02' /etc/haproxy/haproxy.cfg

4. Fix the corrupt server directive in haproxy.cfg.

   ```
   python3 -c "
   content = open('/etc/haproxy/haproxy.cfg').read()
   bad = '       server lbvip02 lbvip02.weave.local\nOverrides::11211 check inter 10s resolvers dns resolve-prefer ipv4'
   good = '       server lbvip02 lbvip02.weave.local:11211 check inter 10s resolvers dns resolve-prefer ipv4'
   open('/etc/haproxy/haproxy.cfg','w').write(content.replace(bad, good))
   ```

5. Validate the HAProxy configuration, then restart the supervisor-managed services:

   ```
   /usr/local/sbin/haproxy -f /etc/haproxy/haproxy.cfg -c

   supervisorctl restart all
   ```

6. Confirm that the services affected are HEALTHY.

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
CSCwr50315	SSLHandshakeFailed error msgs seeing in db logs on requireTLS mode in 25.2 Sprint7 drop2

Resolved CDETS

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

Table 3 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwu98894	Memory depletion seen when peer connections rejected by applying PACL deny
CSCww19847	vDRA: WPS AAR fallback cases are failing for remote site
CSCwt85456	CPS vDRA, 23.2, Error seen while adding new IPv6 zone at secondary site
CSCww39124	Password showing during DB CLI check in output
CSCwt72044	VIM vulnerabilities
CSCwu33880	Apache HTTP, Vim, kmod, nghttp2, OpenSSH, curl, sed, Linux kernel, jq, libcap vulnerabilities
CSCwv23670	GnuTLS, libarchive, Bind, rsync,PostgreSQL vulnerabilities
CSCwt68183	Linux kernel, CURL, PostgreSQL, NSS, Intel Microcode Vulnerabilities
CSCwt68333	Gx CCR-I timeout when enabling IPC priority threadpool in PB

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. RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2026 Cisco Systems, Inc. All rights reserved.