Cisco Policy Suite 24.2.0 Release Notes for vDRA

First Published: September 17, 2024

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 24.2.0. 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 24.2.0 software package (ISO/VMDK image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/24.2.0

Md5sum Details

DRA

5e979aac7ff3b3ed0f47d7e6c8c29572 CPS_Microservices_DRA_24.2.0_Base.release.vmdk.SPA.tar.gz

02c8a794757ada69c4d5c8260c2ec443 CPS_Microservices_DRA_24.2.0_Deployer.release.vmdk.SPA.tar.gz

fa7936bd6303de817f3b51b414958b8a CPS_Microservices_DRA_24.2.0.release.iso.SPA.tar.gz

fb479d5c85ab3740864af34e7ae1a67e CPS_Microservices_DRA_Binding_24.2.0.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	24.2.0.release
Custom Reference Data	24.2.0.release
DRA	24.2.0.release
Microservices Enablement	24.2.0.release

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

Prerequisite for upgrading to 24.2.0 from 24.1.0

The following are the common prerequisites:

1. Run the following CLI before upgrade:

   ```
   #database genericfcvcheck 5.0
   ```

   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
   ```

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.

Issue: DB write transactions in particular worker (binding container) continuously fails after DB ISSM.
In Grafana, continuous 4xxx errors are seen for Gx CCR-I in "Specific errors" panel and continuous failures seen in "Failed Queries" panel for a specific binding container.

Note: It is an inconsistent issue which is not seen on every set/ISSM.

Work Around:

Restart the application in that binding container, "supervisorctl restart app".

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.

vDRA Open CDETS

Table 2 - vDRA Open CDETS

CDETS ID	Headline
CSCwi06456	During ISSM worker VMDK redeployment, 4xxx errors are seen in some of binding containers randomly

Resolved CDETS

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

Table 3 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwi75037	vDRA : Fix crd access-restriction for nacm table groups in DRA Central GUI
CSCwi86852	Log rotation is not happening, DB logs size is increased to high value
CSCwj15637	GNU binutils, Linux kernel, Bind, PostgreSQL, libxml2 Vulnerabilities
CSCwj19030	ISSM redeployment is throwing exception after completing the deployment
CSCwj25183	During Resiliency testing for DB VM's in fPAS, Observed PRIORITY: 1 and 0 for some members

CSCwj29417	Getting special character at end of labels for peer_message_total - dest_host,dest_realm peer_grp
CSCwj53681	Vim,Linux kernel,AccountsService,python-cryptography,c-ares vulnerabilities
CSCwj59677	vDRA: orchestrator log optimizations
CSCwj68249	vDRA: ISSM Automation, after VMDK install ntp warnings consumes more time to complete post checks
CSCwj73893	vDRA : stop timesyncd service in DRA vms.
CSCwj79893	In non-mated site, prioirty Rx AAR forwarded to non-wps pcrf
CSCwj91439	GNU C,Linux Kernel,Apache HTTP,NSS Vulnerabilities
CSCwk04910	In remote site, Rx AAR is not routed to default peer when wps peer is inactive
CSCwk36862	File not found error for elastic server and fluent bit server KPIs
CSCwk44152	DRA is not sending CC-Request type ,CC-Request-number AVP as part of 3xxx response
CSCwk61487	DRA inserting bogus dest-host/realm data on answer messages
CSCwk64510	SSSD ,CUPS,Netplan,Wget vulnerabilities
CSCwk75053	DRA Peer Connection API not working for GTAC users using CURL
CSCwk93884	Bind,Python,Openssl Vulnerabilities

vDRA Open Vulnerabilities

This section lists the open vulnerabilities in this release:

- Critical 204784 Docker Engine < 23.0.15 / 26.x < 26.1.5 / 27.x < 27.1.1 Authentication Bypass
- High 202292 Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6896-1)
- High 205223 Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6951-1)
- High 204835 Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6924-1)
- High 206077 Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6973-1)

Related Documentation

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

Release-Specific Documents

Refer to the following documents for better understanding of Cisco Policy Suite.

- *CPS Release Change Reference*
- *CPS Release Notes for vDRA*
- *CPS vDRA Administration Guide*
- *CPS vDRA Advanced Tuning Guide*
- *CPS vDRA Configuration Guide*
- *CPS vDRA Installation Guide for VMware*
- *CPS vDRA Operations Guide*
- *CPS vDRA SNMP and Alarms Guide*
- *CPS vDRA Troubleshooting Guide*

These documents can be downloaded from 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.

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.

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.