Cisco Policy Suite 23.2.0 Release Notes for vDRA

First Published: August 24, 2023

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 23.2.0. 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

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 23.2.0 software package (ISO image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/23.2.0

Md5sum Details

DRA

67deb906afd6a0cd752967a9f30834d4	CPS_Microservices_DRA_23.2.0_Base.release.vmdk_signed.tar.gz

503a66940f03afd5888cc748271c5b39	CPS_Microservices_DRA_23.2.0_Deployer.release.vmdk_signed.tar.gz
49657f979514d594e91fde44fd2a1fda	CPS_Microservices_DRA_23.2.0.release.iso_signed.tar.gz
034b3bce19864542197dc514bb128ea6	CPS_Microservices_DRA_Binding_23.2.0.release.iso_signed.tar.gz

Component Versions

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

Table 1 - Component Versions

Component	Version
Core	23.2.0.release
Custom Reference Data	23.2.0.release
DRA	23.1.0.release
Microservices Enablement	23.2.0.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 23.2.0 in a VMware environment, see the *CPS Installation Guide for VMware*.

Prerequisite for upgrading to 23.2 from 23.1.0 and rollback from 23.2 to 23.1.0

As there is no mongo version change in 23.2.0 release, from 23.1.0 to 23.2.0 no mongo pre-requisite required.

Weave version upgraded from 1.9.4 to 2.8.1, hence 23.1.0 Patch-1 / 22.2.0 P2 is pre-requisite for 23.2.0 upgrade.

The following are the common prerequisites for upgrade and roll back from 22.2.0 to 23.2.0:

1. Run the following CLI before upgrade:

   ```
   #database genericfcvcheck 4.2
   ```

   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).

Prerequisite for upgrading grafana

From DRA 23.2.0 release, grafana version is upgraded to v9.2.3. To maintain backward compatibility during downgrade, ensure to take the backup of custom dashboard JSON files before upgrade. This is applicable if upgrade done from 22.2.0.

Prerequisite for SVN

Issue: In DRA 23.2.0 release, SVN version is upgraded to 1.13.0 from 1.9.7. Due to this, we are seeing an intermittent issue where the downgrade is getting stuck due to SVN incompatibility.

To maintain backward compatibility during downgrade, SVN backup has to be taken as SVN DB format version changed to 8 from 7.

Step1: Before doing upgrade to 23.2 , the below two files to be copied from SVN container to external VM.

```
# /var/tmp/restore.test.gz
#/var/tmp/backup.tar.gz
```

Step2: To avoid SVN format version gets changed during policy configuration commit after upgrade to 23.2 , restart SVN container before every PB commit.

From CLI , `# docker restart container-id svn`

If still SVN format version is changed , then before doing downgrade, svn backup taken in step-1 should be restored on the SVN container and restart the SVN process.

To check the SVN format version,

```
root@svn:/# cat /var/www/svn/repos/db/format
```

7 → If this value is above 7, then below WA to be applied during downgrade.

Step 3: During downgrade, if the cc-monitor or container fails to downgrade with below error, then restore the SVN backup taken from step 1.

3a. Stop all the process in SVN container and delete SVN backup,

```
#supervisorctl stop all
#kill -9 1998 1999 2000 << FOREGROUND process ID >>
#rm -rf /var/tmp/restore.test.gz
```

3b. Remove SVn backup from mongo admin DB .

From CLI,

```
#db connect mongo
#use backup
#db.fs.files.find()
#db.fs.files.remove({"filename" : "backup.svn.gz" })
```

NOTE: All the new configuration after the backup data will be lost.

3c. Restore backed up files to /var/tmp on SVN container and restart the process.

```
#docker cp restore.test.gz svn:/var/tmp/
#docker cp backup.tar.gz svn:/var/tmp/
#supervisorctl start all
```

Additional Notes

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

- Grafana page not loading after upgrade or installation.

  Issue: Grafana page does not load after upgrade/installation.

  Workaround: Restart grafana process with the following command docker exec grafana:

  ```
  supervisorctl restart grafana
  ```

- Grafana page not loading after upgrade or installation.

  Issue: Grafana page does not load after upgrade/installation.

  Workaround: Restart grafana process with the following command docker exec grafana:

  ```
  supervisorctl restart Grafana
  ```

- TCPDUMP Command failed with operation not permitted error

  `Issue :` tcpdump failed on ubuntu-20.04 with permission denied error even with sudo .
  Command : `sudo tcpdump -i any -s 0 -w /var/broadhop/docker/DPR_Issue.pcap -W 50 -C 100`

  `Conditions:`

```
Ubuntu-18.04 --> By default tcpdump file created with root user and which has access to
all the folders by default
-rw-r----- 1 root root 30713657 Jun 29 16:46 Issue.pcap00

Ubuntu-20.04 --> By default tcpdump created with tcpdump user and which does not have
access to all the folders due to which it was failing with permission denied error.
-rw-r----- 1 tcpdump tcpdump 3698 Jun 29 16:32 Issue.pcap00

Workaround:
Recommended to run tcpdump command with target folder user name . (-Z user)
sudo tcpdump -i any -Z root -s 0 -w /var/broadhop/docker/sample1.pcap -W 50 -C 100
sudo tcpdump -i any -Z cps -s 0 -w /var/broadhop/docker/sample2.pcap -W 50 -C 100
```

- As part of 23.2 redis password stored in confd database.

  Issue: Redis Password configuration not backed up as part of running config

  Conditions: Configured redis password is not backed up as part CLI configuration backup.

  Solution:

  As part of 23.2 release, this behavior changed to store the password in confd.

  If the password is already configured, then it will not be displayed in running config , to mitigate this priblem, redis password to be reconfigured post 23.2 ISO upgrade.

  NOTE: If redis password is not configured already, then this can be ignored.

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
CSCwe89900	vPAS performance not scaling beyond 130K in M4 servers
CSCwc07906	vPAS-fPAS: Observing Binding storage failed message, mongo exception in consolidated QNS log
CSCwe28971	Halo E : Assign Roles in Grafana for OIDC authenticated users
CSCwd80008	TLS Client Peers are closing after sometime of DRA-ISO upgrade

CDETS ID	Headline
CSCvx14701	Gx / Rx Timeout dashboard shows incorrect message processing time
CSCwh33463	vDRA - 23.2 ISO Downgrade is getting stuck due to SVN issue

Resolved CDETS

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

Table 3 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwc34736	DRA does not support TDR for Dest-host AVP empty call scenario
CSCwd99609	Unreachable weave peers aren't removing after VMDK deployment, Msg not displaying for deleting the VM
CSCwe21217	Trigger the alert based on Default Zone IPV6 DB count instead of DB Operations.
CSCwe50552	Elastic Search configurations and logs are reflected when configured external server Flunetbit
CSCwe61074	CPS DRA 23.2 Ubuntu 18.04 LTS : Python vulnerability (USN-5767-3)
CSCwe68444	DRA Central failed login need username added as part of warn logs in consolidated-pb
CSCwe81076	Enhancement to validate the Mandatory plugins configs in systemDefault.xmi as well.
CSCwe89044	CPS vDRA, 22.2, Mongo DB WireTiger DB Recovery Script (port from mmapv1 storage engine script)
CSCwe91380	CPS DRA 23.2 Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS curl vulnerabilities (USN-5964-1)
CSCwf00459	Observed Primary member priority is showing as 0, due to this Primary member is missing for IMSI-DB
CSCwf03298	vDRA : Add weave metrics to prometheus and Grafana
CSCwf20579	CPS DRA 23.2 Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / Vim vulnerabilities (USN-6026-1)
CSCwf26043	Gracefully handle any mongo connectivity issues with mongo-admindb
CSCwf28202	CPS DRA 23.2 Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS Cloud-init vulnerability (USN-6042-1)
CSCwf36264	Modify default time zone and data source of the Grafana Dashboard
CSCwf43562	While upgrading ISO from 22.2 to 23.1, There are some errors are getting observed.
CSCwf47021	No proper Error message when user exceeds logging for more than 50 Subscribers
CSCwf49743	Monitoring is not happening clusters are configured in upper case
CSCwf56626	vDRA : Support sssd.conf file parsing for strings with spaces in them
CSCwf58345	vDRA : Disable sudo queries to external ldap/gtac server in sssd.conf
CSCwf59559	CPS DRA 23.2 Ubuntu 18.04 LT /20.04 LTS /22.04 LTS:GNU binutils vulnerabilities (USN-6101-1)
CSCwf59981	DRA Subscriber Trace Utility exporting huge data file not working properly for single subscriber
CSCwf61439	CPS DRA 23.2 Ubuntu 20.04 LTS / 22.04 LTS /22.10/ 23.04 : libssh vulnerabilities
CSCwf87519	redis password is not storing in show running config for dra-vnf

CDETS ID	Headline
CSCwf96204	Enhancement - To include exclude environment scenario check on PB import from GUI.
CSCwh10828	CPS DRA 23.2 Vim,Openssh,curl Vulnerabilities
CSCwh12953	VMDK upgrade automation issues
CSCwh21362	CPS DRA 23.2 OpenSSL Vulnerabilities

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. 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)