Cisco Policy Suite 24.1.0 Release Notes for vDRA

First Published: March 14, 2024

Last Updated: April 18, 2024

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 24.1.0. 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 24.1.0 software package (ISO/VMDK image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/24.1.0

Md5sum Details

DRA

08f8a54f4bffc92fe936ed061f10b9fb	CPS_Microservices_DRA_24.1.0_Base.release.vmdk.SPA.tar.gz

847bc765a4663aff2fe28dbbb46f1a8c	CPS_Microservices_DRA_24.1.0_Deployer.release.vmdk.SPA.tar.gz
4fcaa763b0a700f8cc158468dac7b355	CPS_Microservices_DRA_24.1.0.release.iso.SPA.tar.gz
cd58a9bbf1e0fe96bd2a4384e9d1b7c9	CPS_Microservices_DRA_Binding_24.1.0.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	24.1.0.release
Custom Reference Data	24.1.0.release
DRA	24.1.0.release
Microservices Enablement	24.1.0.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 24.1.0 in a VMware environment, see the *CPS Installation Guide for VMware*.

Prerequisite for upgrading to 24.1 from 23.2.0 or 23.1.0

The following are the common prerequisites:

1. Run the following CLI before upgrade:

   ```
   #database genericfcvcheck 4.4
   ```

   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 23.2 P1 and if it is upgraded from 23.2 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.

- 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 24.1 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 24.1 ISO upgrade.

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

- After ISSM or mongo resiliency testing in fPAS, observing mongo PRIORITY: 1 for some members.

  Issue : During DB VM Resiliency or after ISSM, observed PRIORITY: 1 for some members.

  Workaround :

  - Use the **show database status** on CLI to fetch the current primary member having PRIORITY:1 replicaset.
  - Connect to primary member using mongo shell.
  - Execute rs.conf() on primary mongo shell and find out index position of priority:1 member.

  For example, if index position is 4, then execute below commands to set priority properly from mongo shell.

  ```
  cfg=rs.conf()

  cfg.members[4].priority = 15

  cfg.members[4].votes = 1

  rs.reconfig(cfg,{ force : true})

  exit
  ```

CSCwi16378: Mongo 5.0 Site-Failover issue, Static sessions&BAU not created,Binding Storage &High DB Cache Memory

vDRA now supports database `dwccheck` CLI command to verify and set the defaultWriteConcern on the databases.

For more information, see the *CPS vDRA Operations Guide*.

CSCwi47188: WT tuning for Mongo 4.2

- vDRA supports the `database wiredTiger-Concurrent-Transactions get-transaction` CLI command to set read and write values for wire tiger transactions on the mongo clusters.

  For more information, see the *CPS vDRA Operations Guide.*
- vDRA supports the `database wiredTiger-concurrent-transactions set-transaction static` CLI command to set the wire tiger concurrent read and write static transactions values.

  For more information, see the *CPS vDRA Operations Guide.*
- vDRA supports the `database wiredTiger-concurrent-transactions set-transaction dynamic` CLI command to set the wire tiger transactions for read and write values to the mongo clusters dynamically.

  For more information, see the *CPS vDRA Operations Guide.*
- vDRA supports the `show database details` CLI command to display the actual concurrent transaction values from the mongo process.

  For more information, see the *CPS vDRA Operations Guide.*

CSCwi62314: HIGH_CPU_USAGE on DBP VMs supporting IMSI_MSISDN Cluster

vDRA supports `binding imsi-msisdn enable-aggregate-query` CLI Command to enable or disable the DB Aggregate status query for IMSI & MSISDN binding tables.

For more information, see the *CPS vDRA Operations Guide*.

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
CSCwi06786	vDRA - After the DB VNF VMDK upgrade, the health check status of the database shows unhealthy for some time and recovers automatically
CSCwj25183	vDRA - After ISSM or mongo resiliency testing in fPAS, observed mongo PRIORITY: 1 for some members
CSCwj60942	Incorrect notification alert for the release 24.1 in GUI

Resolved CDETS

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

Table 3 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwh40414	vDRA : Fix collect-db-logs script to remove mongo status containers
CSCwh77197	vDRA: Increase size of system-history buffer
CSCwd95690	Config changes to be recorded in actual username instead of "orchestrator"
CSCwi00816	After VMDK Upgrade/Downgrade user needs to be re-enable Fluentbit Feature or elastic search feature
CSCwh54897	show system software available-version is showing "No entries found"
CSCwh54570	Invalid IP,IPv6/range validation missing for CRD table PACL csv import from CPS Central
CSCwh97387	vDRA : Restart of job collectd job in stats-relay container does not kill old collect process
CSCwi31716	In some cases, active_peer_count kpi value is not matching with actual number of peers connected
CSCwh75549	vDRA : journalctl log optimisations
CSCwi07569	After VMDK 23.2 upgrade by default in audit logs node printed as a ubuntu, it should be VMs hostname
CSCwi47188	WT tuning for Mongo 4.2
CSCwh24926	Need additional panels included to existing default dashboards
CSCwi79251	WPS Rx AARs over relay to remote vPAS (non-mated sites) are failing
CSCwi45809	Exception while dispatching message in Interim Msg Manager
CSCwi75974	Dynamic rate limit kpi is present for PGs that are not throttled currently
CSCwh40628	Prometheus Scrape interval boundary values of >= 5sec and <= 300 sec are not being enforced
CSCwi00799	vDRA-"send_listener_drop" KPI is showing wrong message class for WPS calls as DEFAULT
CSCwi62314	HIGH_CPU_USAGE on DBP VMs supporting IMSI_MSISDN cluster
CSCwf96470	Enhance the control plane message processing to avoid congestion when control message burst comes
CSCwi35498	Linux kernel ,Intel Microcode,GnuTLS,Avahi,Traceroute,Apache HTTP Server,nghttp2 Vulnerabilities
CSCwi91239	OpenLDAP,Linux kernel,GnuTLS,libssh vulnerabilities

CDETS ID	Headline
CSCwi65551	libssh,OpenSSH,Traceroute,SQLite Vulnerabilities
CSCwh41416	Vim vulnerabilities(USN-6302-1),PostgreSQL vulnerabilities(USN-6296-1)
CSCwh98813	Vim,curl,Samba,Linux Kernel,libx11,Open VM Tools vulnerabilities
CSCwj15637	GNU binutils, Linux kernel, Bind, PostgreSQL, libxml2 Vulnerabilities
CSCwi16378	Mongo 5.0 Site-Failover issue,Static sessions&BAU not created,Binding Storage &High DB Cache Memory

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.