Cisco Policy Suite 23.2.0 Release Notes for PCRF

First Published: August 24, 2023

Last Updated: January 25, 2024

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
- 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 23.2.0 software package (ISO image) from:

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

Md5sum Details

PCRF

be48e60771caa89a8288e5a033126c33 CPS_23.2.0_Base.release.qcow2_signed.tar.gz

aa42db962a2ae96906dd0b07f3f13017 CPS_23.2.0_Base.release.vmdk_signed.tar.gz

3c415c6febbd4342337dbb5806a09cf4 CPS_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
API Router	23.2.0.release
Audit	23.2.0.release
Balance	23.2.0.release
Cisco API	23.2.0.release
Cisco CPAR	23.2.0.release
Congestion Reference Data	23.2.0.release
Control Center	23.2.0.release
Core	23.2.0.release
CSB	23.2.0.release
Custom Reference Data	23.2.0.release
DHCP	23.2.0.release
Diameter2	23.2.0.release
DRA	23.2.0.release
Fault Management	23.2.0.release
IPAM	23.2.0.release
ISG Prepaid	23.2.0.release
LDAP	23.2.0.release
LDAP Server	23.2.0.release
LWR	23.2.0.release
Microservices Enablement	23.2.0.release
Notification	23.2.0.release

Component	Version
Policy Intel	23.2.0.release
POP-3 Authentication	23.2.0.release
RADIUS	23.2.0 release
Recharge Wallet	23.2.0.release
SCE	23.2.0.release
Scheduled Events	23.2.0.release
SPR	23.2.0.release
UDC	23.2.0.release
UDSN Interface	23.2.0.release
Unified API	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
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 23.2.0 in a VMware environment, see the *CPS Installation Guide for VMware*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have access to Graphite database, and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after fresh installation. However, you need to configure the Graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

OpenStack Environment

To perform a new installation of CPS 23.2.0 in an OpenStack environment, see the *CPS Installation Guide for OpenStack*. From CPS 23.2.0 release onwards, OSP 16 support has been newly added for PCRF.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have access to Graphite database, and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after fresh installation. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

Upgrade Alma Linux to 8.7 in PCRF

In CPS 23.2.0 release, Alma Linux version is upgraded from 8.6 to 8.7 along with upgrading to latest rpm packages and their dependencies.

With Alma Linux 8.7, the kernel version is modified to:

```
root@localhost ~]# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-425.19.2.el8_7.x86_64
[root@localhost ~]#

[root@localhost ~]# cat /etc/redhat-release
AlmaLinux release 8.7 (Stone Smilodon)
[root@localhost ~]#

[root@localhost ~]# uname -a
Linux localhost.localdomain 4.18.0-425.19.2.el8_7.x86_64 #1 SMP Tue Apr 4 05:30:47
EDT 2023 x86_64 x86_64 x86_64 GNU/Linux
[root@localhost ~]#
```

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide*. CPS migration is supported only from CPS 22.2.0 or CPS 23.1.0 to CPS 23.2.0.

NOTE: Before migration, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured before migration. If you fail to add the user, then Grafana will not have access to Graphite database, and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after migration. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

For more information, consult your Cisco Technical Representative.

Post Migration/Upgrade Steps

Re-Apply Configuration Changes

After the migration/upgrade is complete, compare your modified configuration files that you backed up earlier with the newly installed versions. Re-apply any modifications to the configuration files.

Verify Configuration Settings

After the migration/upgrade is finished, verify the following configuration settings.

NOTE: Use the default values listed below unless otherwise instructed by your Cisco Account representative.

NOTE: During the migration/upgrade process, these configuration files are not overwritten. Only during a new install will these settings be applied.

- `/etc/broadhop/qns.conf`
  - `-Dmongo.client.thread.maxWaitTime.balance=1200`
  - `-Dmongo.connections.per.host.balance=10`
  - `-Dmongo.threads.allowed.to.wait.for.connection.balance=10`
  - `-Dmongo.client.thread.maxWaitTime=1200`
  - `-Dmongo.connections.per.host=5`
  - `-Dmongo.threads.allowed.to.wait.for.connection=10`
  - `-Dcom.mongodb.updaterIntervalMS=400`
  - `-Dcom.mongodb.updaterConnectTimeoutMS=600`
  - `-Dcom.mongodb.updaterSocketTimeoutMS=600`
  - `-DdbSocketTimeout.balance=1000`
  - `-DdbSocketTimeout=1000`
  - `-DdbConnectTimeout.balance=1200`
  - `-DdbConnectTimeout=1200`
  - `-Dcontrolcenter.disableAndsf=true`
  - `-DnodeHeartBeatInterval=9000`
  - `-DdbConnectTimeout.balance=1200`

- -Dstatistics.step.interval=1
- -DshardPingLoopLength=3
- -DshardPingCycle=200
- -DshardPingerTimeoutMs=75
- -Ddiameter.default.timeout.ms=2000
- -DmaxLockAttempts=3
- -DretryMs=3
- -DmessageSlaMs=1500
- -DmemcacheClientTimeout=200
- -Dlocking.disable=true

NOTE: The following setting should be present only for GR (multi-cluster) CPS deployments:

```
-DclusterFailureDetectionMS=1000
```

NOTE: In an HA or GR deployment with local chassis redundancy, the following setting should be set to true. By default, it is set to false.

```
-Dremote.locking.off
```

- /etc/broadhop/diameter_endpoint/qns.conf
  - -Dzmq.send.hwm=1000
  - -Dzmq.recv.hwm=1000

Reconfigure Service Option

After upgrading from previous release to the current CPS release, Service option configured with Subscriber-Id becomes invalid and you need to reconfigure multiple Subscriber Id in SpendingLimitReport under Service Configurations.

Verify logback.xml Configuration

Make sure the following line exists in the logback.xml file being used. If not, then add the line:

<property scope="context" name="HOSTNAME" value="${HOSTNAME}" />

To ensure logback.xml file changes are reflected at runtime, the scanPeriod must be explicitly specified:

<configuration scan="true" scanPeriod="1 minute">

NOTE: In case scanPeriod is missing from already deployed logback.xml file, the application needs to be restarted for the updated scanPeriod configuration to be applicable.

After completing the updates in logback.xml, execute the following command to copy the file to all the VMs:

SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml

Change Mongo Storage Engine from MMapV1 to WiredTiger in CPS Product

Starting from CPS 22.1.1 release, MongoDB Storage Engine is changed from MMAPv1 to WiredTiger.

WiredTiger storage engine change in MongoDB Server requires additional CPU resources of ~15% and additional memory (RAM) resources of ~40% in the Session Manager VMs. WiredTiger consumes up to ~40% extra memory from total memory(RAM) than MMapV1.

For example, If the sessionmgr VM (150GB) with MMapV1 uses 60GB, then WiredTiger requires 120GB(MMapV1 usage 60GB + 40% of total memory).

As per mongo documentation, the wiredtigercachegb can be configured as [50% of (RAM - 1 GB)] in the VM.

If “n” mongo processes are running in the VM, the wiredtigercachegb can be configured as [50% of (RAM - 1 GB)]/n per mongo process.

For example, in the setup:

• Sessionmgr VMs configured RAM: 157GB

• The number of mongo processes will be running on VM: 6

• Each process cache size can be configured : [50% of (157GB-1GB)]/6 ==> 78/6 = 13GB(can rounded to 12 GB)

NOTE: OS can consume 40-50GB of buffer/cache memory towards system/kernel operations.

The following values must be configured in mongoConfig.cfg:

• WT_CACHESIZEGB=12

• WT_CACHEARBSIZEGB=1

Additional Notes

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

- Session Manager Configuration: After a new deployment, session managers are not automatically configured.

  a. Edit the */etc/broadhop/mongoConfig.cfg* file to ensure all the data paths are set to /var/data and not /data.

  b. Then execute the following command from pcrfclient01 to configure all the replication sets:

  /var/qps/bin/support/mongo/build_set.sh --all --create

- Default gateway in lb01/lb02: After the installation, the default gateway might not be set to the management LAN. If this is the case, change the default gateway to the management LAN gateway
- By default, pending transaction feature is enabled. If you are not using it, Cisco recommends disabling pending transaction feature post deployment.

  To disable pending transaction, the following parameter can be configured in */etc/broadhop/qns.conf* file:

  com.broadhop.diameter.gx.pending_txn.attempts=0

  After adding the parameter in qns.conf file, restart all VMs using *stopall.sh*/*startall.sh* or *restartall.sh* command.

- Add support to disable syncing carbon database and bulk stats files (ISSM)

  Add the following flags in */var/install.cfg* file:

  SKIP_BLKSTATS

  SKIP_CARBONDB

  Example to disable synching:

  SKIP_BLKSTATS=1

  SKIP_CARBONDB=1

- Add the following parameters in */var/install.cfg* file to skip installation type selection and initialization steps during ISSU/ISSM:

  INSTALL_TYPE

  INITIALIZE_ENVIRONMENT

  Example:

  INSTALL_TYPE=mobile

  INITIALIZE_ENVIRONMENT=yes

- Inconsistency in DPR sent by CPS on executing `monit stop` command

  Issue: When `monit stop all` is executed on Policy Director (LB) VMs with active VIP, DPR is not sent to all the diameter peers.

  Conditions: `monit stop all` executed on Policy Director (LB) VMs with active VIP

  Cause: DPR is sent to all the connected diameter peers. However, since `monit stop all` is executed , all the processes on the Policy Director (LB) go down including corosync/haproxy. As a result, some of the DPR messages go out and some are not delivered based on the order of the services going down.

  Workaround: Instead of `monit stop all`, you can stop all the qns process on Policy Director (LB) VMs by executing `monit stop qns-2/3/4` and then issue a `monit stop all` comand.

  With this workaround, processes such as, haproxy/coronsync are up when DPR messages are generated, CPS makes sure that all DPR messages generated by the Policy Directors are delivered.

- 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
  ```

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.

CPS Open CDETS

None in this release.

Resolved CDETS

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

CPS Resolved CDETS

Table 2 - CPS Resolved CDETS

CDETS ID	Headline
CSCwe46480	sync_times.sh script is not working properly
CSCwe72147	LB VM are getting into memory depletion due to flooding in pacemaker log
CSCwf6694	genmac script generating Invalid out-of-range MAC Addresses for VMware

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 Advanced Tuning Guide*
- *CPS Backup and Restore Guide*
- *CPS CCI Guide for Full Privilege Administrators*
- *CPS CCI Guide for View Only Administrators*
- *CPS Central Administration Guide*
- *CPS Documentation Map*
- *CPS Geographic Redundancy Guide*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide – VMware*
- *CPS Migration and Upgrade Guide*
- *CPS Mobile Configuration Guide*
- *CPS Operations Guide*
- *CPS Policy Reporting Guide*
- *CPS Release Change Reference*
- *CPS Release Notes*
- *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *CPS Troubleshooting Guide*
- *CPS Unified API Reference 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.