Cisco Policy Suite 24.1.0 Release Notes for PCRF

First Published: March 14, 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
- 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 24.1.0 software package (ISO image) from:

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

Cisco Confidential

Md5sum Details

PCRF

27552391aa6a7ae7f4f3decb76ceb5ce CPS_24.1.0_Base.release.qcow2.SPA.tar.gz

37b02d1b5ddc4869a39d9b6efd9a9daa CPS_24.1.0_Base.release.vmdk.SPA.tar.gz

3def1be629c04bf377f5a796d6028f14 CPS_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
API Router	24.1.0.release
Audit	24.1.0.release
Balance	24.1.0.release
Cisco API	24.1.0.release
Cisco CPAR	24.1.0.release
Congestion Reference Data	24.1.0.release
Control Center	24.1.0.release
Core	24.1.0.release
CSB	24.1.0.release
Custom Reference Data	24.1.0.release
DHCP	24.1.0.release
Diameter2	24.1.0.release
DRA	24.1.0.release
Fault Management	24.1.0.release
IPAM	24.1.0.release
ISG Prepaid	24.1.0.release
LDAP	24.1.0.release
LDAP Server	24.1.0.release
LWR	24.1.0.release
Microservices Enablement	24.1.0.release
Notification	24.1.0.release

Cisco Confidential

Component	Version
Policy Intel	24.1.0.release
POP-3 Authentication	24.1.0.release
RADIUS	24.1.0 release
Recharge Wallet	24.1.0.release
SCE	24.1.0.release
Scheduled Events	24.1.0.release
SPR	24.1.0.release
UDC	24.1.0.release
UDSN Interface	24.1.0.release
Unified API	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.

Cisco Confidential

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*.

CPS 24.1.0 release provides support for VMware ESXi™ Hypervisor 7.0.3. For details about deploying CPS on ESXi 7.0.3, refer to 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.

Upgrade Alma Linux to 8.8 in PCRF

In CPS 24.1.0 release, Alma Linux version is upgraded from 8.7 to 8.8 along with upgrading to latest rpm packages and their dependencies.

With Alma Linux 8.8, the kernel version is modified to:

```
# rpm -qa | grep kernel-[0-9]
kernel-4.18.0-477.27.1.el8_8.x86_64

## cat /etc/redhat-release
AlmaLinux release 8.8 (Sapphire Caracal)

# uname -a
Linux localhost.localdomain 4.18.0-477.27.1.el8_8.x86_64 #1 SMP Thu Feb 08 13:51:50 EST 2024
x86_64 x86_64 x86_64 GNU/Linux
```


Cisco Confidential

Upgrade MongoDB Version 5.0

This release provides support for MongoDB version 5.0. Following are the supported and unsupported CPS releases to upgrade to Mongo 5.0.

- Supported CPS Releases for upgrading to 5.0:

You can upgrade CPS 23.1.0 or 23.2.0 (using mongoDB version 4.4.18) to CPS 24.1.0 (using mongoDB version, 5.0.20). Upgrade to MongoDB 5.0 is supported only from MongoDB 4.4. For example, if you are running a 4.2 series, you must first upgrade to 4.4 before you can upgrade to 5.0.

- Un Supported CPS Releases for upgrading to 5.0:

Any CPS version before CPS 23.1.0 or 23.2.0 such as CPS 22.2.0 (using mongoDB version 4.2.20) or CPS 22.1.1 (using mongodb version 4.0.27) or previous versions of CPS (using mongoDB version 3.x) does not support direct upgrade to CPS 24.1.0.

To upgrade the mongoDB version to 5.0, you must upgrade to CPS version 23.2.0 or 23.1.0, which uses the mongoDB 4.4 version.

For example, if you are running a mongoDB 3.6 series in your CPS release, it is required to first upgrade to 4.0, then to 4.2, and then to 4.4 before planning for any upgrade to 5.0.

To upgrade the Replica set to 5.0 refer the MongoDB documentation.

MongoDB recovery Script for Network Partition Resilience

Starting with CPS 24.1.0 release, that use MongoDB 5.0, when a majority of replica set members are unavailable, the MongoDB storage undergoes exponential growth, potentially resulting in a complete database crash.
MongoDB recovery Script for Network Partition Resilience is designed to handle such scenarios during failover, so that majority of the replica set members are available.

The following configuration.csv parameters are introduced as part of this feature:

- enable_mongodb_majority_failover_monit - Set the value as true or false to enable or disable the feature respectively. Default Value: false
- majority_failover_monit_cycles- Set the time interval value in seconds to periodically run the MongoDB recovery Script. Default Value: 180 Seconds
- majority_failover_action - Choose any of the following actions on the member which is/are down.
  - REDUCE_PRIORITY - Reduce the priority and vote of the member to 0. (Default, Recommended)
  - REMOVE_MEMBER - Remove the member from the replica set.
- majority_failover_iteration_threshold - Number of iterations the MongoDB recovery Script can wait before taking majority_failover_action on a member that is is down. Default Value: 3

Following is the sample configuration:

```
enable_mongodb_majority_failover_monit,true,
majority_failover_monit_cycles,180,
majority_failover_action,REDUCE_PRIORITY,
majority_failover_iteration_threshold,5,
```

NOTE: The above MongoDB configuration.csv parameter values change from deployment to deployment, depending on factors such as disk usage and the number of SM VMs per site. We recommend you use appropriate values, as default values might not be suitable for all deployments.

To enable this feature:

1. Edit the configuration.csv file with appropriate values for suggested parameters.
2. Run `import_deploy.sh` (from cluman).
3. Verify if the feature is enabled in the "monit summary" output as shown in the sample output.

```
[root@localhost ~]# monit summary | grep mongodb_majority_failover
mongodb_majority_failover OK Program
[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 23.1.0 or CPS 23.2.0 to CPS 24.1.0.

CPS 24.1.0 release provides support for VMware ESXi™ Hypervisor 7.0.3.

For details about deploying CPS on ESXi 7.0.3, refer to the *CPS Installation Guide for VMware.*

NOTE:: As CPS 24.1.0 supports ESXi 7.0 (version until 7.0.3), make sure OVF tool version 4.3.0 is installed in CPS 23.1.0 and CPS 23.2.0 from where you are migrating.

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

Cisco Confidential

- -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

Cisco Confidential

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

Cisco Confidential

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.

Cisco Confidential

CPS Open CDETS

Table 2 - CPS Open CDETS

CDETS ID	Headline
CSCwi85397	Diagnostics is not showing the replicaset status correctly in resiliency case
CSCwj14032	cps24.1 FCV not able to disable mongodb_majority_failover

Resolved CDETS

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

CPS Resolved CDETS

Table 3 - CPS Resolved CDETS

CDETS ID	Headline
CSCwh45392	TACACS account user unable to login
CSCwh67147	Bulk terminate job stopped due to corrupted session.
CSCwh85448	orchestration log notice - Insufficient data in CSV, ignoring empty additionhosts.js entries
CSCwh99662	Sy_SLR Intermediate loop with same SessionID on receipt of 5002 Diameter Unknown Session from OCS
CSCwi10241	IOManager in PCRF keeps restarting, when process is initialized or manually restarted.
CSCwi15203	mongostat output is missing last member data in sessionmgr VMs
CSCwi16736	Apache ActiveMQ CVE-2023-46604 (CVSS 10) is vulnerable to Remote Code Execution.
CSCwi22395	gen-svn-traps.sh generates false positives due to Apache unavailability during logrotation
CSCwi23012	config_br.py script is failing to take user's backup

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*

Cisco Confidential

- *CPS Geographic Redundancy Guide*
- *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.

Cisco Confidential

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)

© 2024 Cisco Systems, Inc. All rights reserved.

Cisco Confidential