Cisco Policy Suite 22.1.1 Release Notes

First Published: June 16, 2022

Last Updated: Nov 07, 2022

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 22.1.1. Use this Release Note in combination with the documentation listed in the *Related Documentation* section.

NOTE: This document overrides the same document available in the 22.1.0. For other functionality refer to the 22.1.0 documentation.

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 22.1.1 software package (ISO image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/22.1.1

Md5sum Details

PCRF

3139507cac8a053a2174b2ca0d440891	CPS_22.1.1_Base.release.qcow2_signed.tar.gz
4588af534bc0b74beaced5ef29708581	CPS_22.1.1_Base.release.vmdk_signed.tar.gz

4bb3525677f2deb59e9b8d73101e6681	CPS_22.1.1.release.iso_signed.tar.gz

DRA

058484ecf96688293049867b4ad5b5b6	CPS_Microservices_DRA_22.1.1_Base.release.vmdk_signed.tar.gz
95cde02024f330991af96ed746db42bc	CPS_Microservices_DRA_22.1.1_Deployer.release.vmdk_signed.tar.gz
d32d12a6c9748b10dd26828804c03dd4	CPS_Microservices_DRA_22.1.1.release.iso_signed.tar.gz
b8ec037bc7d2e44abb4361e145c9db2f	CPS_Microservices_DRA_Binding_22.1.1.release.iso_signed.tar.gz

MongoDB supports only “WiredTiger” storage engine from 4.2 release, which will be supported from CPS 22.2 release. CPS 22.1 runs MongoDB 4.0 with storage engine as MMAP. To upgrade to CPS 22.2, it is essential to run with storage engine “WiredTiger”.

As part of this release, CPS DRA shall support MongoDB version 4.0.27 with wired Tiger (WT) storage engine.

Component Versions

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

Table 1 - Component Versions

Component	Version
Audit	22.1.1.release
API Router	22.1.1.release
Balance	22.1.1.release
Cisco API	22.1.1.release
Cisco CPAR	22.1.1.release
Congestion Reference Data	22.1.1.release
Control Center	22.1.1.release
Core	22.1.1.release
CSB	22.1.1.release
Custom Reference Data	22.1.1.release
EMM	22.1.1.release
DRA	22.1.1.release
DHCP	22.1.1.release
Diameter2	22.1.1.release
Fault Management	22.1.1.release
IPAM	22.1.1.release
ISG Prepaid	22.1.1.release
LDAP	22.1.1.release

Component	Version
LDAP Server	22.1.1.release
LWR	22.1.1.release
Microservices Enablement	22.1.1.release
Notification	22.1.1.release
NRF	22.1.1.release
Policy Intel	22.1.1.release
POP-3 Authentication	22.1.1.release
Radius	22.1.1.release
Recharge Wallet	22.1.1.release
SCE	22.1.1.release
Scheduled Events	22.1.1.release
SPR	22.1.1.release
TIM-AVP	22.1.1.release
UDC	22.1.1.release
UDSN Interface	22.1.1.release
Unified API	22.1.1.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 22.1.1 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 22.1.1 in an OpenStack environment, see the *CPS Installation Guide for OpenStack*.

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.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide*. CPS migration is supported from CPS 21.1.0/CPS 21.2.0 to CPS 22.1.1.

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.

NOTE: As CPS 22.1.1 supports ESXi 6.7/7.0, make sure OVF tool version 4.3.0 is installed in CPS 21.1.0 from where you are migrating.

Version 4.3.0 for VMware 6.7/7.0: VMware-ovftool-4.3.0-13981069-lin.x86_64.bundle

You can download the OVF tool version 4.3.0 from https://code.vmware.com/web/tool/4.3.0/ovf.

NOTE: In CPS 22.1.1, MongoDB version is upgraded to 4.0.27. MongoDB v4.0.27 requires mandatory Java driver upgrade. In CPS 21.2.0 and earlier releases, CPS runs with 3.7.2 version of Mongo Driver. Patch should be applied with updated driver 3.12.x as a prerequisite before moving to CPS 22.1.1.

For more information, consult your Cisco Technical Representative.

Upgrade an Existing CPS Installation

In-Service Software Upgrade (ISSU) is not supported when migrating from CPS 21.1.0/CPS 21.2.0 to CPS22.1.1.

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

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.

Change mongo storage engine from MMapV1 to WiredTiger in CPS product

CPS 22.1 supports Mongo 4.0 with MMapV1 storage engine, and it does not support WiredTiger storage engine.

Since Mongo 4.0 is nearing End of Life (EOL) soon, and Mongo 4.2 does not support MMapv1, CPS 22.2 should be upgraded to Mongo 4.2 that supports only WiredTiger storage engine.

For example, to upgrade from previous versions of CPS 22.1 to CPS 22.2, you must first upgrade to CPS 22.1(Mongo MMapv1) and then change the storage to mongo 4.0 WiredTiger engine with patch ISO, then upgrade to 22.2(mongo 4.2 WiredTiger), which requires additional MW/efforts.

CPS 22.1.1 release is a special release that includes storage engine change from WiredTiger in mongo 4.0 and thereby reducing an additional MW.

Additional Information

WiredTiger storage engine change in MongoDB Server 4.0 requires additional CPU resources of ~15% and additional memory (RAM) resources of ~40% in the Session Manager VMsUp to ~40% extra memory being consumed more by wiredtiger from total memory(RAM) than MMapV1.

For example: If sessionmgr VM (150GB) with MMapV1 using 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 below values must be configured in mongoConfig.cfg.

- WT_CACHESIZEGB=12
- WT_CACHEARBSIZEGB=1

Prerequisites for ISSM:

- Take a copy of the mongoConfig.cfg file from the old clumans.
- Update the below values in mongoConfig.cfg file
  - WT_CACHESIZEGB=12
  - WT_CACHEARBSIZEGB=1
- Execute import_deploy.sh before performing the ISSM procedure.
- Make sure that the system is running mongo 3.6 and the java driver patch is applied.

After prerequisites conditions are met, perform the ISSM process.

Considerations for Rollback:

- Before performing a rollback, restore the copied mongoConfig.cfg file in older clumans.
- Execute *import_deploy.sh* before performing the ISSM rollback procedure.

NOTE: If the deployment uses custom scripts for deploying the environment and custom scripts are using/modifying the mongoConfig.cfg, then change the custom scripts as needed.

Introduced new mongo statistics “used” and “dirty”. Both parameters represent the value in percentage.

- The used parameter represents the current utilization of memory from the configured wiredTigerCacheSizeGB.
- The dirty parameter represents the modified data in the cache until it is persisted in the data files in the MongoDB data path via a periodic checkpoint.

These new statistics can be created and accessed in the grafana using cisco.quantum.qps.*.*sessionmgr*used.percent and cisco.quantum.qps.*.*sessionmgr*dirty.percent.

Mongo’s new statistics Grafana sample is shown below. You can create/modify the Grafana dashboard as needed.

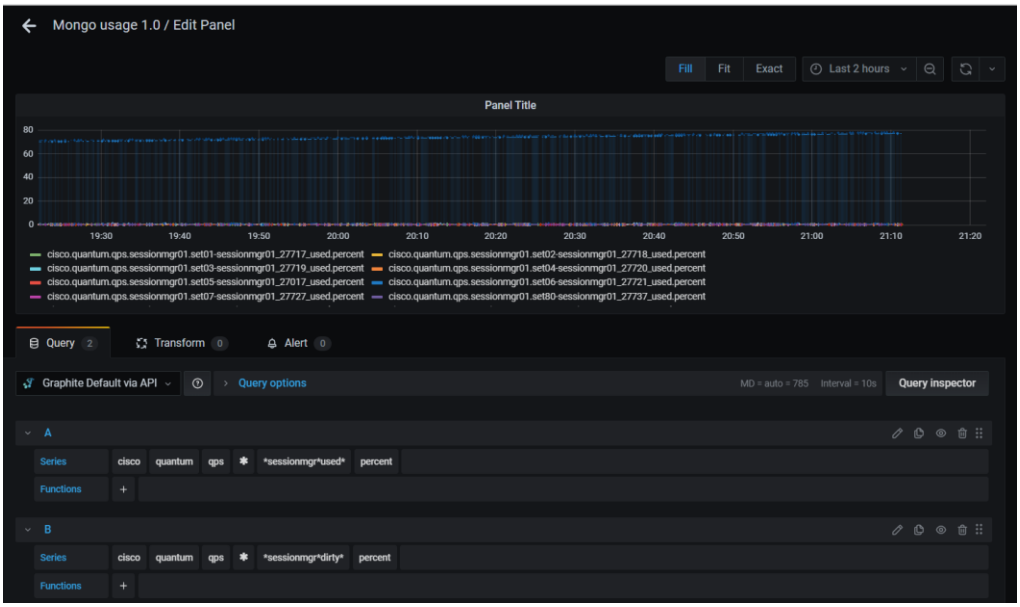

Figure 1 – Grafana Dashboard

Supported DRA Releases for Upgrading to 22.1.1

- DRA 22.1.0 (MongoDB version 4.0.27 MMAP) to DRA 22.1.1 (MongoDB version 4.0.27 WT)
- DRA 22.1 Patch 1 (MongoDB version 4.0.27 MMAP) to DRA 22.1.1 (MongoDB version 4.0.27 WT)
- DRA 21.1 Patch4 (MongoDB version 3.6.9 MMAP) to DRA 22.1.1 (MongoDB version 4.0.27 WT)

Prerequisite for Upgrading to 22.1.1 and Rollback from 22.1.1

NOTE: This is common prerequisite for both upgrade and rollback.

Run the following CLI before upgrade:

#database fcvcheck

NOTE: Make sure to run the above CLI before upgrade and / or downgrade on all sites.

Following are the two CLI options:

- **Set**: This option checks and sets FCV only on primary.
- **Check**: This option only checks FCV on all members(primary/secondary/arbiter).
  It is recommended to use set option first and then check to make sure FCV is replicated on secondary members as well. 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 /downgrade.

Upgrade Procedure for 22.1.1

1. Run the pre-requisite steps mentioned above
2. Follow the standard documented procedure for upgrade.
3. After upgrade is successful, execute the following additional post checks:
   - *show running-config database | include storage*

   Output of the above CLI contains storage-engine WT.

   admin@orchestrator[fPAS-site3-master-1]# docker exec mongo-s104 "ps -efww"
==========output from container mongo-s104==========
root 32 1 88 May19 ? 12-15:30:18 mongod --keyFile=/mongodb.key --enableMajorityReadConcern false --ipv6 --bind_ip_all --port 27021 --dbpath=/data/db/wt-27021 --replSet rs-app_shardCD-ipv6-1 --quiet --slowms 500 --logpath /data/db/mongo-27021.log --setParameter diagnosticDataCollectionEnabled=true --logappend --oplogSize 3221 --logRotate reopen --wiredTigerCacheSizeGB 4.40
output of above cli should contain 4.40 value for–wiredTigerCacheSizeGB parameter.
admin@orchestrator[fPAS-site3-master-1]# docker exec mongo-s104 "df -hT"
==========output from container mongo-s104==========
Filesystem Type Size Used Avail Use% Mounted on
tmpfs tmpfs 7.6G 1.6G 6.0G 21% /data/db/wt-27026
tmpfs tmpfs 500M 301M 200M 61% /data/db/wt-27029
Output of above CLI contains 7.6G size (for non-arbiters) and 500M (for arbiters) size tmpfs partitions.

Downgrade Procedure from 22.1.1

1. Run the steps mentioned in the prerequisite section.
2. Execute the below CLI to convert database config from WT to MMAP.
   #database changeConfigToMMAP
3. After running the above two prerequisites, follow the standard documented procedure for downgrade.

Mongo DB Storage and WT Cache Calculation in 22.1.1

Deployment Type	Total Memory	No.of MongoDB Instances	Memory Calculation
FPAS	64GB	Non arbiter (data bearing member) = 4 Arbiter: 0 to 2	wiredTigerCache per MongoDB (non-arbiter) = **4.4GB** [30 % of RAM / 4] wiredTigerCache per MongoDB (arbiter) = **250MB** /tmpfs per MongoDB(non-arbiter) = **7.6 GB** [50 % of RAM / 4] /tmpfs per MongoDB(arbiter) = **500MB**
vPAS	64Gb session 128 Gb Binding	Non arbiter (data bearing member) = 4 Arbiter:0 to 4	**For 64 GB:** Calculation is same as FPAS. **For 128GB:** wiredTigerCache per MongoDB (non-arbiter) = **8.81GB** [30 % of RAM / 4] wiredTigerCache per MongoDB (arbiter) = **250MB** /tmpfs per MongoDB(non-arbiter) = **16GB** [50 % of RAM / 4] /tmpfs per MongoDB(arbiter) = **500MB**

New KPIs Added:

In binding VNF, below 4 KPIs are added in Database monitor dashboard:

- **WT Cache Usage %: (mongo_current_bytes_into_cache/mongo_max_bytes_configured)*100** – *Monitors WT cache usage in %age.*
- **WT Tracked Dirty Usage %: (mongo_tracked_dirty_bytes_in_cache/mongo_max_bytes_configured)*100 -** Monitors dirty bytes in WT cache in %age.

- **WT Pages Read into Cache (MB): mongo_pages_read_into_cache/(1024*1024) -** Monitors number of pages that are read into cache in MB.
- **WT Pages Written from Cache (MB): mongo_pages_written_from_cache/(1024*1024) -** Monitors number of pages that are written from the cache in MB.

Limitations

For DRA 22.1.1 release runtime database configuration change is not supported and not recommended. It is done to support in service storage engine conversion from MMAP to WT and vice versa. To perform any changes, you need to stop the database and reconfigure with appropriate configuration changes.

Additional Information

WiredTiger storage engine change in MongoDB Server 4.0 requires additional resources:

- CPU utilization of ~10-15 [under the threshold] on DBP VMs while no significant change observed in rest of the VMs [distributor / director / worker]
- DBP VMs consume up to ~20 - 30% extra memory more by wiredtiger from total memory (RAM) than MMapV1

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

Table 2 - CPS Open CDETS

CDETS ID	Headline
CSCwc54243	Session manager VM reachability from QNS or UDC shard pinger timing out intermittently
CSCwb94871	While publishing the PB SVN sync is not happing from pcrfclient01 to pcrfclient02
CSCwb89647	High number of tcp connections observed in PCRFclient VMs
CSCwc01554	In Overload testing for one SM process PCRF MONGO response time took 1.66hr

vDRA Open CDETS

Table 3 - vDRA Open CDETS

CDETS ID	Headline
CSCwc18592	vPAS: Grafana shows -ve values in CPU Utilization during Set-2 Site-A DRA ISSM in 22.1 CCO Image

Resolved CDETS

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

CPS Resolved CDETS

Table 4 - CPS Resolved CDETS

CDETS ID	Headline
CSCwb50834	httpd segmentation fault due to httpd reload via logrotate.d
CSCwb05329	Deleted stale session cleaner log files are still open and consuming space on disk on pcrfclients
CSCwb86849	Custom patch support - build_images.sh is exiting with an error
CSCwb61911	CRD import using xlsx is failing from Control center in 22.1
CSCvz65793	ASPR puppet is failing while enabling ASPR117
CSCvz65801	Need to have keys rotation mechanism for mech users as well
CSCwb53474	top_qps.sh logs errors on pcrfclient service-qns logs
CSCwb06735	session destination-realm parameter is not getting updated post-CCR-U with a different origin-realm
CSCwc27019	Session manager ports are not coming up post rollback from 22.2 to 22.1M

vDRA Resolved CDETS

Table 5 - vDRA Resolved CDETS

CDETS ID	Headline
CSCwb02113	Disable Dynamic Rate limiting during run time not clearing old cache
CSCwb09318	DRD SSL Certificate Signed Using Weak Hashing Algorithm (SHA1)
CSCwa96412	Connection Count is not implemented in Relay Peer monitoring GUI Page
CSCwb22705	vPAS - Some of the regex expression search not working in CRD GUI
CSCwb23885	vPAS Metadata DB health check fails during worker down scenario
CSCwb17404	Peer routing table not taking latest values from CRD
CSCwb33247	DRA failed to rate limit ingress API requests as per configured rate limit
CSCwa01913	Message type label not updated for 3002 error message kpi in some scenarios
CSCwb27614	DRA_21.1: Make the Prometheus data retention period configurable by user
CSCwa85192	SSH cipher/ MAC weak algorithms found on 21.1 release.
CSCwa80670	Observing 3002 timeouts with mongo timeout exception in logs during fPAS longevity

CDETS ID	Headline
CSCwa97125	Database FCV check does not include fPAS IMSI_MSISDN DB shard members
CSCwc00660	Observed less free memory and more memory in CACHE in master and control VMs
CSCwb98129	vPAS: Observed 4007 Errors during ISSM Upgrade

Related Documentation

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

Release-Specific Documents

Refer to the following CPS 22.1.1 documents:

- *CPS Release Change Reference*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide – VMware*
- *CPS Migration and Upgrade 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.

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*
- *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.