Cisco Policy Suite 18.3.0 Release Notes (Restricted Release) (2)

First Published: November 8, 2021

Last Updated: November 8, 2021

IMPORTANT: CPS 18.3.0 is a Short Term Support (STS) release with availability and use restrictions. Contact your Cisco Account or Support representatives, for more information.

Introduction

This release note identifies new features and enhancements, limitations and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 18.3.0. Use this release note in combination with the documentation listed in the Related Documentation section.

This release note includes the following sections:

New and Changed Feature Information

This section identifies features that are new or modified in this release.

ANDSF

No new features or changes were introduced in this release.

ATS

Support for HTTP/2 Client

PATS now supports HTTP/2 client. You can configure HTTP/2 version and other properties in the config.properties file. This functionality helps users to:

- Send HTTP/2 request from SITE to any HTTP/2 enabled endpoint.
- Verify any HTTP/2 response received at the SITE.
- Use all the HTTP methods like GET, POST etc. while sending a request via HTTP/2

For more information, contact your Cisco Technical Support Representative.

Round-Robin Traffic for Performance Test of Multiple Peer Communication

Currently, PATS/SITE Diameter driver supports multiple peer connection for server stack. You can choose any particular peer by providing destination FQDN and Destination Realm.

PATS/SITE Diameter driver waits for first peer. In this release, a new timer parameter is introduced to allow a wait time for other peer connection establishment. The following parameter is included in timer.properties file:

Diameter.MultiplePeer.WaitTime=X

This parameter specifies the wait time in milliseconds to allow other peer to be connected after the first peer is established. Default Value: 0 (No wait time)

For more information, contact your Cisco Technical Support Representative.

Enhanced Grammars for CoAP Requests and Responses

In this release, the following new grammars are included for CoAP requests and responses:

- Validate message ID and reference message ID in requests and responses
- Send custom and duplicate message ID in requests and responses
- Validate received responses using attributes and/or message reference
- Send asynchronous requests and validate responses
- Validate reference token in request and response
- Send custom and duplicate token in request

For more information, contact your Cisco Technical Support Representative.

Enhanced Control for Test Execution

<TBD – Yet to receive SFS>

Behavior Changes

CSCvg99670 – SNMP - VM UP trap for pcrfclient01 is not coming when pcrfclient01 is cold started.

Old Behavior: Currently, on pcrfclient01 if Policy Server (qns) process is down, pcrfclient is not raising alarm for the down process.

New Behavior: In CSP 18.3.0 and later releases, on pcrfclient node, if Policy Server (qns) process is down, 'logstash_process_status' program stops the logstash process so that the alarm is raised from another pcrfclient node.

Impact on Customer: None

Geographic Redundancy

No new features or changes were introduced in this release.

LWR

No new features or changes were introduced in this release.

Mobile

Session State Update after RAA Error Code

In CPS 18.3.0, a new check box **Save Session State** is added under **REFERENCE DATA** > **Diameter Clients** > **Gx Clients** in Policy Builder GUI.

When enabled Gx session state is restored following a failed Gx RAA (Result-Code AVP value not equal to DIAMETER_SUCCESS (2001)) to the state it was before the Gx RAR was sent. The behavior is same for both sync and async Gx RAR.

For more information, see *Basic Options* under *Gx Clients* section in the *CPS Mobile Configuration Guide*.

Support for MCPTT

CPS is enhanced to support MCPTT bit (bit 17) from Feature-List-ID 1 in Rx TGPP Spec. MCPTT-Identifier AVP in RxAAR is ignored if the MCPTT feature is not negotiated. CPS supports MCPTT-Identifier as an input column AVP pair for RxSTGConfiguration and RxSTGDefaultBearerConfiguration service configurations.

For more information, see *CPS Mobile Configuration Guide*.

Support for NB-IOT Devices

PCRF supports devices using narrow band Internet of Things (NB-IoT) RAT that is a 3GPP radio interface to support IoT devices.

PCRF can create a session with UE having RAT-type as NB-IOT and provides all functionalities (such as policy control and charging rule functionality) to an NB-IOT devices.

The existing input variable, ratType, for the condition, Diameter Gx TGPP Session Exists, in Use Case Initiator is enhanced to support NB-IoT RAT-type.

For more information, see *CPS Mobile Configuration Guide*.

MOG

Local Session Affinity in MOG

New session lookup type called "local" is added to support local session affinity. When session lookup type is set to "local", local session database is used for read/write session irrespective of site lookup configuration.

For more information, see *Configure MOG Lookup Value* section in the *CPS MOG Guide*.

vPAS Interface Changes

vPAS configuration in Policy Builder is enhanced with the following changes:

- **vPAS Query For Put Requests**: new check box to configure whether MOG should send vPAS Query after PUT request or not.
- Default value of the polling interval is modified from 30 minutes to 0 minutes.

For more information, see *vPAS Configuration* section in the *CPS MOG Guide*.

Operations

API Additions or Changes

No changes were introduced in this release.

MIB Additions or Changes

No changes were introduced in this release.

KPI Additions or Changes

No changes were introduced in this release.

Log Additions or Changes

No changes were introduced in this release.

SNMP Alarm Additions or Changes

No changes were introduced in this release.

Statistics Additions or Changes

The following new statistics are included for the vDRA feature "Support for Session Route Key Configuration for vDRA Rx AAR Fallback Routing":

- com.broadhop.unifiedapi.statistics:name=rest.get: Success and Failure stats of API called by DRA
- db_stats (new label "source" with values "pcrf" and "gx"): Gauge for current number of IPv6 bindings based on PCRF session query.

The following new statistics are included for the vDRA feature "Support for Load Balancing IPv6 Binding Session Queries Across PCRFs in a Group":

- Pcrf_heartbeat_request_send: Counter for total number of Keepalive REST API requests sent to PCRF for checking REST API interface status. Labels: url_endpoint, status

Performance Improvement

MongoDB Automatic Recovery process Enhancement

In CPS 18.3.0, replica-set creation has been automated so that the downtime during recovery process is minimal. The following new components have been added:

- AIDO server: Responsible to create/update replica-sets
- AIDO client: Responsible to start mongod on database node

CPS and AIDO do not support sharded option. By default, only non-sharded is supported.

Operations such as, create and add-member in build_set.sh commands is now changed and they verify the replica-set status and AIDO handles all the operations.

build_set.sh --all –-create: This command verifies all the local members configured in replica-set and replica-set is UP.

If someone wants to use build_set.sh to creates replica-set, then you need to use newly added --**force** option.

For more information, see the *CPS Installation Guide for VMware* and *CPS Geographic Redundancy Guide*.

Upgrade MongoDB to 3.2.19

In CPS 18.3.0, Mongo has been upgraded from 3.2.13 to 3.2.19. To verify MongoDB version on VMs, execute the following command from Cluster Manager:

cat /etc/broadhop/mongoConfig.cfg | grep -e '^MEMBER' -e '^ARBITER=' | cut -d= -f 2 | while read hnp; do echo $hnp; mongo --quiet $hnp --eval "db.version()"; done

pcrfclient01:27717

3.2.19

sessionmgr01:27717

3.2.19

sessionmgr02:27717

3.2.19

Note: Post upgrade all the data members and arbiters for all the replica-sets must show the same mongo version i.e. 3.2.19.

Enhanced Installation Script

TBD

Platform

OpenStack Queens

In CPS 18.3.0, CPS can be installed on OpenStack Queens.

For more information, see the *CPS Installation Guide for OpenStack*.

Upgrade VMX Version and vCenter

In CPS 18.3.0, support for VMX11 is added only for fresh install. In option 2 (offline upgrade)/option 3 (ISSU), only CPS software on an existing VM is upgraded. Hence VMX version is not upgraded in option 2/3.

For more information, see *Deploy the Cluster Manager VM* section in the *CPS Installation Guide for VMware*.

Policy Reporting

No new features or changes were introduced in this release.

Policy Reporting

No new features or changes were introduced in this release.

Product Security

Redis Authentication

In CPS 18.3.0, you can restrict the access to Redis Server by enabling authentication to prevent unauthorized access. Redis authentication must be configured explicitly (TRUE/FALSE) for fresh installations. By default, Redis authentication is enabled for fresh installations.

All access to Redis Server from CPS requires a password after the server is enabled with authentication. CPS reads the encrypted password from environment variable, decrypts it, and uses it to connect to Redis Server.

If the password matches the password in the configuration file, the server responds, with the OK status code and starts accepting commands. Otherwise, an error is returned and you need to re-enter the password.

For more information about Redis authentication, refer the following sections:

In *CPS Installation Guide for VMware*:

- General Configuration Parameters table
- Redis Authentication
- Redis Authentication for Upgrading/Migrating Systems

In *CPS Installation Guide for OpenStack*:

- Configuration Parameters - HA System table

  Redis Authentication for Upgrading/Migrating Systems

Security Enhancements

This section lists enhancements introduced to support Cisco Product Security Requirements and the Product Security Baseline (PSB). For more information about Cisco Product Security Requirements, refer to: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html

PSB Requirement Support for CPS 18.3.0

CPS now supports the following PSB requirements:

- Prevents exposure of credentials and other critical data
- Provides cryptographic protection outside controlled space

UDC

Support to Stop Window Buffer

CPS can be configured to stop window buffer on receiving particular diameter messages.

For more information, see *CPS UDC Administration Guide*.

UI Enhancements

Support for Safeguard Warning Messages in Policy Builder

CPS is enhanced to notify users with notifications and warning messages when a new policy is applied by selecting a plugin configuration which overrides the existing configuration.

For more information, see *CPS Mobile Configuration Guide*.

Search Table Groups Listed Based on Evaluation Order Value

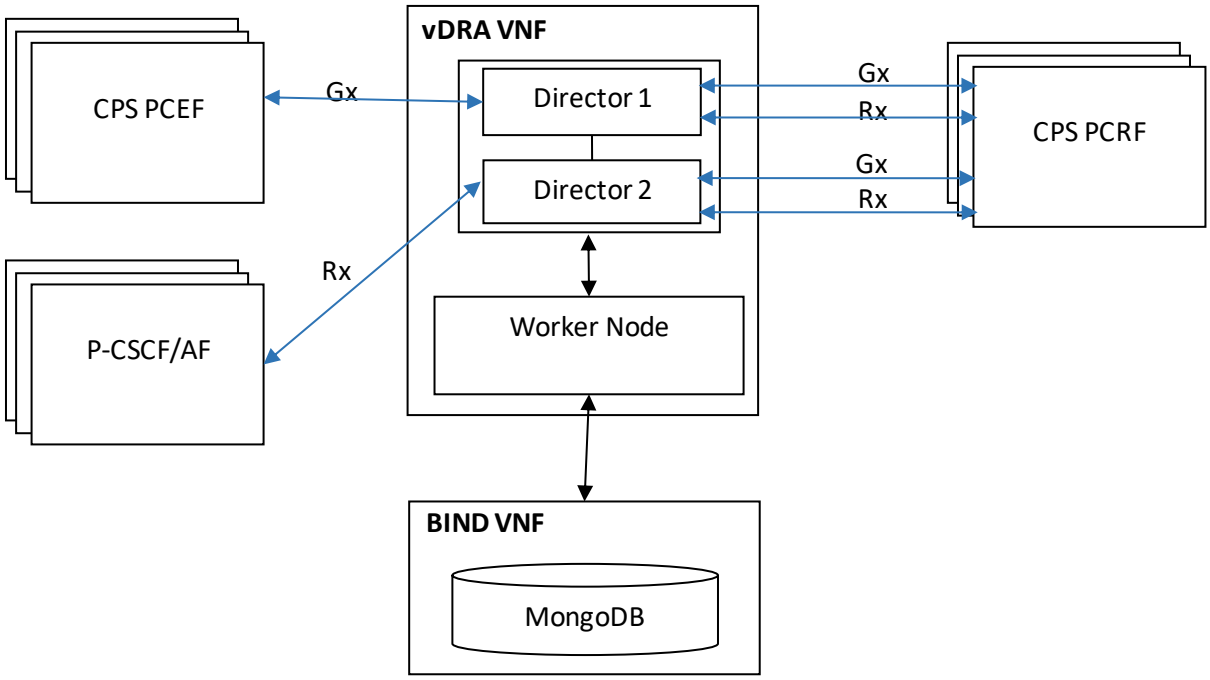
CPS now supports listing of search table groups and their respective CRD tables based on the evaluation order value. If the evaluation order value is same for two or more tables then they are listed alphabetically.

For more information, see *CPS Central Administration Guide*, *CPS vDRA Administration Guide* and *CPS Mobile Configuration Guide*.

vDRA

Support for Diameter Load Balancing to Same Peer Across Multiple DRA Directors

CPS now includes diameter load balancing. Previously, when a PCRF is connected to multiple directors and the PCEF traffic comes on one director only, all the traffic would be handled by director-PCRF connection where PCEF is connected. In this release, the requests are load balanced across multiple DRA directors, as shown in the following illustration.



This load balancing is irrespective of the type of routing: destination, host, SRK-based, or table-driven routing.

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

Support for Session Route Key Configuration for vDRA Rx AAR Fallback Routing

CPS provides the option to configure the session route key (Session Route Key in Unified API Plugin Configuration) that vDRA uses to look up the peer group and route the Rx AAR message to the correct PCRF.

When vDRA makes REST API requests to multiple PCRFs for session query using the IPv4 or IPv6 address received in the Rx AAR message, the PCRF that has the corresponding Gx session sends the session routing key in the response.

vDRA then uses this key to look up the peer group and routes the Rx AAR message to the correct PCRF.

vDRA also includes a new option "Create IPv6 Bindings based on PCRF Session Query" that you enable to create IPv6 record: When PCRF session query result (success) is received and if IPv6 record is not present in the database, vDRA creates an IPv6 binding record based on the response from the PCRF. If any CCR-I is received for the same IPv6 record, then it overwrites the IPv6 binding record. For any CCR-T, vDRA deletes the IPv6 binding record from database. The Stale Binding Expiry and Refresh Minutes are used to clear these binding records from the database.

For more information about this feature, see the following documents:

- Configure the session route key in the Unified API plugin configuration as described in the *CPS Mobile Configuration Guide*.
- Configure the PCRF session query CRD for Rx AAR fallback routing: see "PCRF Session Query Peers" in the *CPS vDRA Configuration Guide*.
- Enable both the PCRF Session Query and the Create IPv6 Bindings based on PCRF Session Query options in the vDRA plugin configuration as described in the *CPS vDRA Configuration Guide*.

Support for Load Balancing IPv6 Binding Session Queries Across PCRFs in a Group

vDRA supports load balancing of IPv6 binding queries across multiple PCRF API endpoints (VIPs). Previously, all REST queries were sent to the primary endpoint and only if the primary query fails, then the request is sent to secondary. Now, the requests are load balanced across the different PCRF endpoints within a peer group. If the session query results indicate that the PCRF does not have the corresponding Gx session for the IPv6 prefix, then vDRA does not send the query to the other PCRF configured in the same group. Similarly, for all other failures, vDRA sends the session query request to the secondary PCRF in the group. If there are more than two PCRF API endpoints configured in the PCRF group, then vDRA only uses the first two entries and remaining PCRFs are ignored. If there is no group name, the PCRF API endpoint is considered as a standalone PCRF.

For more information, see *CPS vDRA Configuration Guide*.

Configuration of HTTP Response Codes for REST API JSON Codes

vDRA supports configuration of the HTTP response error code (such as 4xx, 5xx) corresponding to each vDRA Rest API JSON error response code for the GET binding (for example imsi, imsiApn, msisdn, msisdnApn, ipv4, ipv6) Rest API.

This HTTP response error code is used in the response for any GET binding Rest API request. If this CRD is not configured with HTTP response error codes, then vDRA returns the default HTTP response status code.

For more information about the CRD, see the *CPS vDRA Configuration Guide*.

If you do not configure the Rest API HTTP Error Code in the CRD, vDRA uses the default HTTP error codes for GET binding Rest API. For a list of the default HTTP error codes, see the *CPS vDRA Troubleshooting Guide*.

Support to Synchronize Repositories

DRA is now enhanced to support synchronizing of Policy Builder (PB) repository information from an active PB to a passive PB. This helps passive PB to access the latest PB repository details when the active session goes down.

Note: When an active PB session is down, do not try to manage (add/edit/delete) the PB repositories from the passive PB. After the active PB is up, the passive PB repository details is overwritten by the active PB.

Support for Auto Refresh in DRA GUI

CPS DRA is enhanced to support Auto-refresh option which refreshes data every 30 seconds and displays the Data Last Refreshed field that indicates the time when data is fetched from server.

For more information, see *CPS vDRA Administration Guide*.

Upgrading DRA Open Source Components

CPS is enhanced to upgrade the following DRA components:

- Grafana to version 5.1.4 – To receive timely updates of Grafana and other security issues.
- Azul Zing Binding Worker – Specific to launching worker nodes.

Installation Notes

Download ISO Image

Download the 18.3.0 software package (ISO image) from:

TBD

Md5sum Details

TBD

Component Versions

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

Table 1 Component Versions

Component	Version
ANDSF	18.3.0.release
API router	18.3.0.release
Audit	18.3.0.release
Balance	18.3.0.release
CALEA	18.3.0.release
Cisco API	18.3.0.release
Cisco CPAR	18.3.0.release
Congestion Reference Data	18.3.0.release
Control Center	18.3.0.release
Core	18.3.0.release
CSB	18.3.0.release
Custom Reference Data	18.3.0.release
DHCP	18.3.0.release
Diameter2	18.3.0.release
DRA	18.3.0.release
Entitlement	18.3.0.release
Fault Management	18.3.0.release
ISG Prepaid	18.3.0.release
LDAP	18.3.0.release
LDAP Server	18.3.0.release
LWR	18.3.0.release
Microservices Enablement	18.3.0.release
Notification	18.3.0.release
NRF	18.3.0.release
NSLB	18.3.0.release
NSSF	18.3.0.release
PCF	18.3.0.release
Policy Intel	18.3.0.release
POP-3 Authentication	18.3.0.release
Recharge Wallet	18.3.0.release

Component	Version
SCE	18.3.0.release
SCEF	18.3.0.release
Scheduled Events	18.3.0.release
SPR	18.3.0.release
UDC	18.3.0.release
UDSC Interface	18.3.0.release
Unified API	18.3.0.release

New Installations

- VMware Environment
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 18.3.0 in a VMware environment, see *CPS Installation Guide for VMware*, *Release 18.3.0*.

OpenStack Environment

To perform a new installation of CPS 18.3.0 in an OpenStack environment, see *CPS Installation Guide for OpenStack*, *Release 18.3.0*.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see *CPS Migration and Upgrade Guide, Release 18.3.0*. CPS migration is supported from CPS 14.0.0, CPS18.0.0 and CPS 18.1.0.

Upgrade an Existing CPS Installation

To upgrade an existing CPS installation, see *CPS Migration and Upgrade Guide*, Release 18.3.0. CPS upgrade is supported from CPS 18.2.0.

During ISSU from CPS 18.2.0 to CPS 18.3.0, if the following issue is observed then one needs to reboot Cluster Manager and start ISSU again:

/dev/mapper/control: open failed: No such device

Failure to communicate with kernel device-mapper driver.

Check that device-mapper is available in the kernel.

Incompatible libdevmapper 1.02.140-RHEL7 (2017-05-03) and kernel driver (unknown version).

Command failed

The issue is observed only when the kernel is updated for the first time. In subsequent ISSU, the kernel issue is not observed.

Post Migration/Upgrade Steps

Re-Apply Configuration Changes

After the migration/upgrade is finished, 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 Technical 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 t o 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.

- CSCvf52617: GR_ST: Grafana stops displaying all mongostats in dashboard when Primary member of one DB goes down

  Issue: In case any member of a replica-set is not reachable, you will not be able to see Mongo statistics in grafana. Not reachable can happen due to network problems or blade going down or member is intentionally stopped.

  Workaround: Make non-reachable member reachable. For example:

  - If the member is intentionally stopped then one has to start using /etc/init.d/sessionmgr-* start script.
  - If there is a network issue, then this issue the network issue needs to be fixed.

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

  a. Edit the /etc/broadhop/mongoConfig.cfg file to ensure all of 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 to disable 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.

- CSCvb74725: Avoid manual steps in API based GR installation

  Issue: The fresh install of API based GR installation does not execute set priority properly.

  Workaround:

  a. The fresh install of API does not execute set priority properly. You need to set the priority manually by executing the following command:

  ```
  set_priority.sh --db all
  ```

  b. You need to delete the default ring configuration present in cache_config database. After fresh install in case Active/Active Geo-HA feature is enabled, default ring configuration needs to be deleted manually. To remove/replace ring config, following two options are available:

  - Delete directly from database. Remove from “cache_config”, if “shards” is empty. This may need restart of qns services.

    OR

  - Run OSGi command `setSkRingSet <ringId> <setId> <servers>` which replaces existing values.

  c. Unused replica-set need to be removed manually.

  There is no API support for removing replica-set. So you need to remove the replica-set manually by executing the following command:

  ```
  build_set.sh --<databasename> --remove-replica-set <setname>
  ```

  For example,

  ```
  build_set.sh --spr --remove-replica-set --setname set04
  ```

  d. If someone changes `qns.conf` parameters using API post system is deployed using PATCH method, then `restartall.sh` has to be executed manually so that configuration changes become effective.

  e. You need to be set the priority manually for members after adding via addMember API by executing the following command:

  ```
  set_priority.sh --db all
  ```

- CSCvd30781: set_priority.sh broken ImportError: No module named util when running set_priority.sh on pcrfclient01

  Issue: `set_priority.sh` from pcrfclient01 and pcrfclient02 is broken. No module named util is found when running `set_priority.sh`.

  Workaround: Execute `set_priority.sh` from Cluster Manager. If you do not have replication network on the Cluster Manager, you need to copy the **util** sub-directory from the Cluster Manager to pcrfclient01 and pcrfclient02.

  Source on Cluster Manager: `/var/qps/install/current/scripts/modules/util`

  Destination on pcrfclient01/02: `/var/qps/bin/install/current/scripts/modules/util`

- CSCvc66672: System is crashing when run more than 6k tps

  Issue: High response time is observed when system is running with all the default features installed and has Gx traffic with 6K TPS.

  Consideration: It is recommended to create session replica-set as per performance requirements for scaling.

  Solution:

  - Create/update /etc/broadhop/mongoConfig.cfg file on Cluster Manager VM to create session cache shards in criss-cross fashion.

    [SESSION-SET1]

    SETNAME=set01

    OPLOG_SIZE=5120

    ARBITER1=arbitervip:27717

    ARBITER_DATA_PATH=/var/data/sessions.1

    MEMBER1=sessionmgr01:27717

    MEMBER2=sessionmgr02:27717

    DATA_PATH=/var/data/sessions.1/1

    [SESSION-SET1-END]

    [SESSION-SET2]

    SETNAME=set07

    OPLOG_SIZE=5120

    ARBITER1=arbitervip:27727

    ARBITER_DATA_PATH=/var/data/sessions.7

    MEMBER1=sessionmgr02:27727

    MEMBER2=sessionmgr01:27727

    DATA_PATH=/var/data/sessions.1/2

    [SESSION-SET2-END]

  - For further information on how to create replica sets, see Create Specific Replica-set and Session Cache Replica-set sections in CPS Installation Guide for VMware.

- Set session database priority so that the PRIMARY members will be on separate VM:

```
cd /var/qps/bin/support/mongo
./set_priority.sh --db session
```

For more information about `set_priority.sh` script, see *CPS Operations Guide* and *CPS Geographic Redundancy Guide*.

- To create session shards, see the Create Session Shards section in CPS Installation Guide for VMware.

- CSCve40105: Session databases do not recover on power outage

  Issue: Session databases do not recover after full system outage.

  Condition: Replica configuration is not available after system outage on Arbiter VIP. This is verified using the following command (XXXXX is port number):

```
mongo --host arbitervip:XXXXX --eval "rs.isMaster()['info']" --quiet
Does not have a valid replica set config
```

  Probable Cause: This happens as VIP was up on different pcrfclient (e.g. pcrfclient01) when outage took place and after recovery it is on another pcrfclient (e.g. pcrfclient02). Thus, previous mongo configuration is not available with current active pcrfclient and recovery script is not able to recover data.

  Workaround: User has to flip the VIP when the session databases mounted on tmpfs do not recover after full system outage. To force a switchover of the arbiter VIP to the other pcrfclient, you have to execute the following command:

```
ssh arbitervip service corosync stop
service corosync stop
```

- CSCvg28401: CPS diameter dictionary gets corrupted when there is a change in custom AVP list.

  Issue: CPS Diameter dictionary gets corrupted when there is a change in custom AVP list.

  Probable Cause: The dictionary corruption happens when Policy Builder is published with custom AVP changes. This results in one thread of execution clearing up the AVP cache and populating the cache with the updated AVPs.

  During this, if the thread of call processing uses the AVP cache before it is populated with the AVPs, it pushes NullAvpRepresentation object in the cache for which it did not find any definition. This results in decoding failure of the Diameter message. This is a race condition which manifests during high TPS.

  Workaround: After configuring custom AVP list, restart CPS using the `restartall.sh` script.

- 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

- CSCvi48586: change_passwd.sh script is getting stuck for root user after fresh deploy.

  Issue: change_passwd.sh script is getting stuck for root user after fresh installation.

  Workaround: The point where the script gets stuck, enter the existing password (not the changed one) for the root user. The script runs successfully after this point in few seconds.

- CSCvi21871: Permission denied when connecting DRA cli and not able to connect dra central

  Issue: Permission denied when connecting to DRA orchestrator CLI with the default admin credentials.

  Workaround: Log into the orchestrator container from the master VM and reload the aaa_init.xml file into confd.

  cps@master-0:/data/orchestrator$ docker exec -it orchestrator bash

  root@orchestrator:/# /var/confd/bin/confd_load -l -m /data/cdb/aaa_init.xml

  root@orchestrator:/# exit

  exit

  cps@master-0:/data/orchestrator$

Primary Member is Isolated from all Arbiters

Issue: If the primary database member gets isolated from all the arbiters then diagnostics output displays incorrect states.

Solution: If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, most likely an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status.

Limitations and Restrictions

This section covers the following topics:

Limitations

- The following restriction applies to LWR:
  - In this release, LWR supports read and write of one user attribute to the replication framework specific to the ADTM bearer counting attribute.
    In future releases, UDC and other applications will be enhanced to provide support of new attributes or user profile details that may require replication

- Solicited Application Reporting

  The following are some restrictions on configuration for the new service options:

  - The pre-configured ADC rule generated by CRD lookup has ADC-Rule-Install AVP definition with support for only three AVPs ADC-Rule-Name, TDF-Application-Identifier, Mute-Notification.
  - For AVPs that are multi-valued, CRD tables are expected to have multiple records - each giving the same output.
  - Comma(,) is not a valid character to be used in values for referenced CRD column in SdToggleConfiguration.
  - AVP Table currently only supports OctetStringAvp value for AVP Data-type.
- During performance testing, it has been found that defining a large number of QoS Group of Rule Definitions for a single session results in degraded CPU performance. Testing with 50 QoS Group of Rule Definitions resulted in a 2x increase in CPU consumption. The relationship appears to be a linear relationship to the number of defined QoS Group of Rule Definitions on a service.
- Hour Boundary Enhancement

  Change in cell congestion level when look-ahead rule is already installed:

  If a cell congestion value changes for current hour or any of the look-ahead hours, there will be no change in rule sent for the rules that are already installed.

  No applicability to QoS Rules:

  The look-ahead works for PCC rules only where we have rule activation/deactivation capabilities and can install upcoming changes in advance. However, if the RAN Congestion use case is changed to use the QoS-Info AVP instead of using PCC rules, we need to fall back to the current RAR on the hour boundary implementation for that use case since the standard do not let us install QoS-info changes ahead of time like we can with PCC rules.
- The Cluster Manager's internal (private) network IP address must be assigned to the host name “installer” in the `/etc/hosts` file. If not, backup/restore scripts (`env_import.sh`, `env_export.sh`) will have access issues to OAM (pcrfclient01/pcrfclient02) VMs.
- The Linux VM message.log files repeatedly report errors similar to the following:

  `vmsvc [warning] [guestinfo] RecordRoutingInfo: Unable to collect IPv4 routing table.`

  This is a known issue affecting ESXi 5.x. Currently, there is no workaround for this. The messages.log file entries are cosmetic and can be safely ignored. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2094561
- CSCva02957: Redis instances continue to run, even after redis is disabled using the parameter `-DenableQueueSystem=false` in qns.conf (`/etc/broadhop/`) file and `/etc/broadhop/redisTopology.ini` file.
- CSCva16388: A split-brain scenario (that is, VIPs are up on both nodes) can still occur when there is connectivity loss between lb01 and lb02 and not with other hosts.

Common Vulnerabilities and Exposures (CVE)

No CVEs were found in this release.

Open and Resolved CDETS

The following sections list open and resolved CDETS for this release. For your convenience in locating 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

CDETS ID	Headline

Microservices Open CDETS

Table 3 Microservices Open CDETS

CDETS ID	Headline

Resolved CDETS

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

CPS Resolved CDETS

Table 4 CPS Resolved CDETS

CDETS ID	Headline

CDETS ID	Headline

CDETS ID	Headline

CDETS ID	Headline

Microservices Resolved CDETS

Table 5 Microservices Resolved CDETS

CDETS ID	Headline

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 ANDSF Configuration Guide*

- *CPS ANDSF SNMP and Alarms 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 Geographic Redundancy Guide*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide – VMware*
- *CPS LWR Guide*
- *CPS LWR Installation Guide - OpenStack*
- *CPS LWR Installation Guide - VMware*
- *CPS Migration and Upgrade Guide*
- *CPS Mobile Configuration Guide*
- *CPS MOG API Reference*
- *CPS MOG Guide*
- *CPS MOG Installation Guide - OpenStack*
- *CPS MOG SNMP, Alarms, and Clearing Procedures Guide*
- *CPS MOG Troubleshooting Guide*
- *CPS Operations Guide*
- *CPS Policy Reporting Guide*
- *CPS Release Notes*
- *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *CPS Troubleshooting Guide*
- *CPS UDC API Reference*
- *CPS UDC Administration Guide*
- *CPS UDC Installation Guide*
- *CPS UDC Session Migration Guide*
- *CPS UDC SNMP and Alarms Guide*
- *CPS Unified API Reference Guide*
- *CPS vDRA Administration Guide*
- *CPS vDRA Configuration Guide*
- *CPS vDRA Installation Guide - OpenStack*
- *CPS vDRA Operations Guide*
- *CPS vDRA SNMP and Alarms Guide*
- *CPS vDRA Troubleshooting Guide*

These documents can be downloaded from the following links:

- All Guides

https://www.cisco.com/c/en/us/support/wireless/quantum-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.