Cisco Policy Suite 18.4.0 Release Notes (Restricted Release)

First Published: September 14, 2018

Last Updated: September 14, 2018

IMPORTANT: CPS 18.4.0 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 18.4.0. 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 Diameter T4 Interface

In this release, ATS now supports call flows for Diameter T4 Interface.

For more information, contact your Cisco Technical Support Representative.

WS Driver Extension for HTTP2 Server and REST Delete

In this release, you can:

- Receive and verify HTTP/2 request from PATS to any HTTP/2 enabled endpoint.
- Send any HTTP/2 response for request received at PATS Web Service Driver.
- Use all the HTTP methods like GET, POST and so on while sending a request via HTTP/2.
- Send DELETE requests through REST client with request body that can contain some specific value/parameter.
- Send DELETE request and configuration reference can be provided in the message bundle.
- JSON,YAML, XML message type content is allowed to send DELETE request.
- Content can be provided from message bundle.

For more information, contact your Cisco Technical Support Representative.

Behavior Changes

CSCvi89606 – Certain Stats Using E-Notation (Scientific)

Previous Behavior: In previous releases, java automatically converted the gauge data source type value to E-notation if the value exceeds 7 digits.

New Behavior: In this release, the code has been modified and E-notation values for gauge data source values are not seen in bulkstats.

Impact on Customer: None

CSCvm17454 - DRA DB stats shows different count for different binding workers/

CSCvm15870 - vPAS: Very high CPU usage on MSISDN+ IMSI binding DB

Previous Behavior: In previous releases, all the binding workers were populating the database count and aggregate statistics.

New Behavior: In this release, the code has been modified so that only one of the binding workers populates the database count and aggregate statistics at a time. If the binding worker populating the database count and aggregating statistics goes down, another binding worker (only one) picks up the task.

Impact on Customer: Grafana dashboard now shows the count statistics from only one worker and not from all the workers.

Cisco Ultra eSCEF

Cisco Ultra eSCEF, Release 18.4.0 is qualified for lab testing and for limited controlled live trial purposes only.

Geographic Redundancy

No new features or changes were introduced in this release.

LWR

No new features or changes were introduced in this release.

Mobile

Optimized CRD Refresh

CPS now supports optimization of the CRD refresh process and restricts CRD cache rebuild caused by any CRD data change. The following new parameters are introduced:

- crd.next.reload.delay.time
- crd.reload.max.delay.interval

For more information, contact your Cisco Technical Support Representative.

Session State Update after RAA Error Code

In this release, 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*.

SPR Cache Cleanup by Backup Database

CPS now supports removal of subscriber records located on remote SPR Mongo databases during Gx termination (CCR-T).

When SPR cache cleanup is enabled, CPS writes the subscriber record ID to a sprCleanupQueue that runs on each Policy Server (qns) node when a cross-site remove action occurs. The process MonitorSprCleanupQueue fetches these messages off the queue at configured intervals and writes them to the cleanupSubscriber database maintained on the local hot standby database. Another process, MonitorCleanUpSubscriberDB, fetches the records in a batch from the cleanupSubscriber database and remove these to their respective Remote SPR databases cross-site. In most cases, these records are already deleted. If this action deletes the record, or fails to find the record (previously deleted), the record is then removed from the cleanupSubscriber database. If CPS fails to delete the record because of connectivity, or other blocking issues, the record is retained to be tried again.

The following table lists the new statistics that have been added:

Table 1 New Statistics

Statistics	Description
subscriberCleanup.addedToQueue	SPR record added to the queue.
subscriberCleanup.removedFromQueue	SPR record deleted from the queue.
subscriberCleanup.insert.success subscriberCleanup.insert.failure	Number of remote subscribers written from queue to subscriber-Cleanup database on hot standby.
spr.remote.cleanupDelete.success." + dbAddress spr.remote.cleanupDelete.failure." + dbAddress	Counter registers when a subscriber is deleted on a remote SPR. Note: Most transactions do not delete any records as the records have already been removed. Example: spr.remote.cleanupDelete.success.site1-ses-sionmgr05:27720

Support for Presence Reporting Area Identifiers

CPS is enhanced to support multiple Presence Reporting Area (Multiple-PRA) over Gx and Sd interfaces as per Gx TGPP specification Release 14.

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

MOG

No new features or changes were introduced in this release.

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

Critical File Monitoring and Notification

In this release, CPS now sends a critical alarm (Critical File Operation Alert) notification when a critical file such as /etc/hosts is modified.

You can monitor the critical files only on Cluster Manager.

For more information, see the following sections:

- *Component Notifications* in *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Testing Traps Generated by CPS* in *CPS Troubleshooting Guide*

Statistics Additions or Changes

SPR Cache Cleanup by Backup Database

The following new statistics have been added:

- subscriberCleanup.addedToQueue: SPR record added to the queue.
- subscriberCleanup.removedFromQueue: SPR record deleted from the queue.
- subscriberCleanup.insert.success/subscriberCleanup.insert.failure: Number of remote subscribers written from queue to subscriberCleanup database on hot standby.
- spr.remote.cleanupDelete.success." + dbAddress/spr.remote.cleanupDelete.failure." + dbAddress: Counter registers when a subscriber is deleted on a remote SPR.

  Note: Most transactions do not delete any records as the records have already been removed.

Example: spr.remote.cleanupDelete.success.site1-sessionmgr05:27720

ZMQ IPC Endpoint Heartbeat Failure Statistic

The following new statistic is added:

- node[x].counters.ZMQ_IPCEndpoint_<VM HOST NAME>_<ZMQ IPC Endpoint Port number>_Down.qns_count: When ZMQ IPC Endpoint heartbeat fails in updating details in ADMIN DB then the corresponding ZMQ IPC endpoint is treated as down and this counter is incremented. The VM hostname and port are taken from the ZMQ tcp connection, by default there is IPADDRESS in tcp connection and the application determines VM name by searching for IPADDRESS in "/etc/hosts" file. If the IPADDRESS is not present in "/etc/hosts" then IPADDRESS is specified instead of VM hostname.

Performance Improvement

Upgrade MongoDB to 3.4.16

In this release, Mongo has been upgraded from 3.2.19 to 3.4.16. 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

3.4.16-1

sessionmgr01:27717

3.4.16-1

sessionmgr02:27717

3.4.16-1

Note: Post upgrade all the data members and arbiters for all the replica-sets must show the same mongo version i.e. 3.4.16-1.

Platform

Critical File Monitoring and Notification

In this release, CPS now sends a critical alarm notification when a critical file such as /etc/hosts is modified.

You can monitor the critical files only on Cluster Manager.

You can get multiple alarms for files modified during upgrade/migrate. You can neglect these alarms.

For more information, see *Critical File Monitoring Configuration* section in *CPS Installation for VMware* and *CPS Installation for OpenStack*.

Support for DSCP Marking

In this release, you can configure the DSCP bits on a per logical interface basis. This allows for all the traffic to be sent over that interface OUT to be marked with the desired DSCP bits.

By default, DSCP marking is supported for fresh installation. You can also enable DSCP marking after the CPS system is upgraded/migrated.

For more information, see *DSCP Configuration* section in *CPS Installation for VMware* and *CPS Installation for OpenStack*.

Policy Reporting

No new features or changes were introduced in this release.

Product Security

No new features or changes were introduced in this release.

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 18.4.0

CPS now supports the following PSB requirements:

- Provides log session and authentication
  - Monitoring session creation or attempted session creation.
  - Monitoring session termination by user logout.
  - Monitoring session termination caused by timeout, excessive user sessions, or other resource management.
  - Monitoring session termination caused by error.
  - Monitoring administrative session termination or session locking.
  - Monitoring successful or unsuccessful resumption of administratively locked or suspended sessions.
- Provides log authentication changes
  - Monitoring parameters such as required credential strength and re-authentication interval.
- Provides log authorization changes
  - Monitoring creation or deletion of principals.
  - Monitoring modification of privileges, group assignments, and marks of authority associated with principals.
  - Monitoring creation or deletion of groups and roles.
  - Monitoring modification of privileges or access associated with groups.

- Monitoring changes to permission settings or access control lists on data objects such as files, database or tables.
- Monitoring changes to firewall filtering or network access lists.
- Monitoring changes to information authorizing resource consumption (quotas and rate limits).

Web PSB Requirements Support for CPS and Micro-services

CPS now supports the following web PSB requirements:

- Display of user privileges such as ADMIN and READONLY in PB2 application.
- Specify encoding in response headers for Control Center application to ensure security.

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

UDC

No new features or changes were introduced in this release.

UI Enhancements

No new features or changes were introduced in this release.

vDRA

Graceful Shutdown of vDRA Containers

This release includes the following new commands that provide graceful shutdown and starting of vDRA containers:

- docker stop <container-id>
- docker start <container-id>

This command ensures the following tasks are completed before the container is stopped:

- required DPR messages are sent out to all connected peers.
- VIP moves to a different Director.

In this release, these commands are supported for Diameter-endpoint containers only.

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

Increased TPS per TCP Peer-Connection

In this release, vDRA can support up to 10K TPS on a single TCP peer connection in order to reduce the number of peer connections required.

Support Multiple Peer Connections

In this release, vDRA supports reverse path route answer to a peer when there are multiple connections to that peer on the same DRA director.

If multiple remote peers (having same FQDN) are connected with DRA and one remote peer goes down after sending a request then response message is also dropped. DRA does not send the request to any other remote peers (having same FQDN).

Support for Best Effort Binding Creation

CPS is enhanced to support best effort binding creation option to configure on a per APN basis. The configuration is enabled on a per APN basis and controls any or all of the following bindings (for best effort):

- IPv6
- IPv4
- MSISDN/APN
- IMSI/APN
- Session

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

Installation Notes

Download ISO Image

Download the 18.4.0 software package (ISO image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/18.4.0

Md5sum Details

e922208742c595a418cee6d7d0c0ceb2	CPS_18.4.0_Base.qcow2.release.tar.gz
8e273ad6a91a70396b58abaf4d4aa65b	CPS_18.4.0_Base.vmdk.release.tar.gz

4e0c5f1e1615ae66c36fb6c4e49a2037	CPS_18.4.0.release.iso
b27e56f599b8286b2caf2cf248ba1cde	CPS_Microservices_18.4.0_Base.release.qcow2
a4fba96d685d3baa877ec8f5c4a1c7db	CPS_Microservices_18.4.0_Base.release.vmdk
563b7feafe297cf3a2e02501b615ace6	CPS_Microservices_18.4.0_Deployer.release.qcow2
8bdab971850e17c1b291984e44451591	CPS_Microservices_18.4.0_Deployer.release.vmdk
1a3cfd900e6a1894d3a5e7f25b39cf3c	CPS_Microservices_DRA_18.4.0.release.iso
60f91a896394bbba5a5b67449392c695	CPS_Microservices_DRA_Binding_18.4.0.release.iso

Component Versions

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

Table 2 Component Versions

Component	Version
ANDSF	18.4.0.release
API router	18.4.0.release
Audit	18.4.0.release
Balance	18.4.0.release
CALEA	18.4.0.release
Cisco API	18.4.0.release
Cisco CPAR	18.4.0.release
Congestion Reference Data	18.4.0.release
Control Center	18.4.0.release
Core	18.4.0.release
CSB	18.4.0.release
Custom Reference Data	18.4.0.release
DHCP	18.4.0.release
Diameter2	18.4.0.release
DRA	18.4.0.release

Component	Version
Entitlement	18.4.0.release
Fault Management	18.4.0.release
ISG Prepaid	18.4.0.release
LDAP	18.4.0.release
LDAP Server	18.4.0.release
LWR	18.4.0.release
Microservices Enablement	18.4.0.release
Notification	18.4.0.release
NRF	18.4.0.release
NSLB	18.4.0.release
NSSF	18.4.0.release
PCF	18.4.0.release
Policy Intel	18.4.0.release
POP-3 Authentication	18.4.0.release
RADIUS	18.4.0.release
Recharge Wallet	18.4.0.release
SCE	18.4.0.release
SCEF	18.4.0.release
Scheduled Events	18.4.0.release
SPR	18.4.0.release
UDC	18.4.0.release
UDSC Interface	18.4.0.release
Unified API	18.4.0.release

New Installations

- VMware Environment
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 18.4.0 in a VMware environment, see the *CPS Installation Guide for VMware*, *Release 18.4.0*.

OpenStack Environment

To perform a new installation of CPS 18.4.0 in an OpenStack environment, see the *CPS Installation Guide for OpenStack*, *Release 18.4.0*.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide, Release 18.4.0*. CPS migration is supported from CPS 14.0.0 to CPS 18.4.0.

Upgrade an Existing CPS Installation

To upgrade an existing CPS installation, see the *CPS Migration and Upgrade Guide*, Release 18.4.0. CPS upgrade is supported from CPS 18.2.0 and CPS 18.3.0 to CPS 18.4.0.

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 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 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.

- 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

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 3 CPS Open CDETS

CDETS ID	Headline
CSCve87564	ISSM:'/mnt/iso/migrate.sh rollback' cli triggers restart for set-2
CSCvh53895	Rx AARs are not routed via secondary when Mongo DB primaries are down.
CSCvi01695	Create shards api shows success even though failure was diagnosed due to failed rebalance
CSCvi23619	After ISSU, diag shows list of alarms not cleared, while conn btwn LB & PCEF/CSCF/TDF clients came up
CSCvj29993	vPAS DRA: Region 1 failure cause 1 minute outage on region 2.
CSCvj39710	Unable to locate 'startqps' file intermediately after reboot to pcrfclient VM on CSP 18.2

CDETS ID	Headline
CSCvj49386	Warning messages "Mongo is still not restored: " in consolidated qns logs on CPS18.2
CSCvj51119	Intermediate failure of clearing/removing session's through session_catch_ops.sh script in CSP18.2
CSCvj53529	ISSM 13.1 to 18.2 - After traffic swap grafana should print from pcrfclient02
CSCvj55766	svn import failing in CPS 18.2 when call from console
CSCvj55932	ZeroMQConnectionError alarm active in the customer CPS platform
CSCvj80096	ISSM 13.1 to 18.2 - /mnt/iso/migrate.sh traffic restore command success with exceptions.
CSCvj88208	Bulk terminate command not working/getting exception in logs
CSCvj94859	During pcrfclient01 stop and start, stats with prometheus query stopped coming to pcrfclient01
CSCvj97328	TPS is not reaching expected level after Traffic Switch over (Site Failure in GR Setup)
CSCvk26197	start-db-traps.sh is not finishing with success and report the following error in /var/log/messages
CSCvk30283	LDAP TPS unable to recover when QNS are down
CSCvk30832	18.3 CPS AppScan Issue: Missing HTTP Strict-Transport-Security Header
CSCvk52072	During longevity run with Redis enable, system response time for CCR-I/T increased upto ~8-9 ms.
CSCvk64916	vPAS: calls failed while binding db is recovering after replication network restore.
CSCvk65479	GC pause due to huge Temp characters
CSCvk75734	Opening Control center asks authentication to be done for Spring Security application
CSCvk76501	/etc/hosts lost during update
CSCvm02970	Evaluation of qps for August CPU Side-Channel Information Disclosure Vulnerabilities
CSCvm04614	Disable Remote Scans for Sync Messages and Single Session Update
CSCvm04646	SPR Deletes: Stale SPR Records - Avoiding the extra processing of SPR.find() - failover improvements
CSCvm04898	improve performance on GR setups with singe sh and single sy enabled
CSCvm08851	PCRF sending out Sd RARs without dest-host AVP for few calls.
CSCvm09662	No CALEA alarms when CALEA peers go down
CSCvm12653	Wide discrepancies in OSP vs VMWare VM sizing
CSCvm13136	mongo in UNKNOWN state failed to start and assertion error
CSCvm15802	Evaluation of qps for CVE-2018-5391 (FragmentSmack)
CSCvm20606	Exception - All parameters must be Serializable

CDETS ID	Headline
CSCvm24223	Getting an ArrayIndexOutOfBoundsException in qns logs when PB Publish is issued.
CSCvm32449	Error executing IPolicyAsyncAction: null error observed in qns logs
CSCvm33832	Pcrfclient01 not upgraded during ISSU from 18.3 to 18.4
CSCvm34004	Asking for root password of installer during execution of change_password after Fresh Install
CSCvm36161	CPS: Unknown action com.broadhop.calea.iface.CaleaGetTargetAction for SY messages
CSCvm37391	UDC is returning the Sy counters only for the First APN for an subscriber
CSCvm39065	ISSU 13.1 to 18.0 - Found mongotimeout exception, while moving back primary member of replica sets
CSCvm42276	session failover failback causing 5002 5065 Timeout Errors
CSCvm42670	No stats to track mongo remote SPR insert operations
CSCvj93662	Race condition when qns processes are taken down, diameter peer down alarm may be missed
CSCvk36604	BEMS850443: P1, AT&T, Neo CPS 18/13.1: Updates required in QPS_Statistics.xls
CSCvk67829	remove whisper .wsp file older than 90 days or configurable param value.
CSCvm37043	about.sh does not properly parse all possible IPv6 address formats in haproxy.cfg
CSCvm50304	Np interface: Missing/wrong functionalities need to be implemented/corrected as per requirement

Microservices Open CDETS

Table 4 Microservices Open CDETS

CDETS ID	Headline
CSCvj99199	BEMS809710-Sy/Gymessages succeed with P-bit set as "0" disabled in answer message with Real OCS
CSCvk64592	DRA database status moves to STARTUP2 status for all shards when a switched Off DB is started
CSCvk64945	vPAS: Few alls are getting timeout after binding db is covered and replication network restored
CSCvk69501	vPAS:3002 errors when bring up the DD1 after powered off and powered on.
CSCvm02492	Grafana - Hi-Res datasource is giving inconsistent data/graphs for Sy STRs on Application dash-board.
CSCvm04809	DRA-Bindings + Session DB's entries clearance is not consistent in make-break call model
CSCvm12119	DRA doing diameter connection reset 2 times after VIP is restored on higher priority director VM

CDETS ID	Headline
CSCvm16842	Few Central GUI functions not available after doing blade reboot testing
CSCvm36837	DRA - DB operation errors in Overload handing during busrt of CCR-I msgs
CSCvm39095	DRA-High response time for db operations on RAA 5002 from GW and AAR timeouts at DRA at High AAR TPS
CSCvm43194	very high db queries response time and poor performance on 18.4 FCV drop1
CSCvm43197	System don't sustains the traffic, Longevity Broken after couple of hours.
CSCvm43257	vPAS:DRA: Grafana displayed inconsistent data.

Resolved CDETS

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

CPS Resolved CDETS

Table 5 CPS Resolved CDETS

CDETS ID	Headline
CSCvh95120	CPS supposed to send the Allocation-Retention-Priority.Priority-Level AVP in CCA-I
CSCvh77676	vPAS DRA: Diameter Relay for Inbound VIP is also connecting
CSCvj19639	receiving redundant information during arbiter vm upgrade with option-2
CSCvj10152	DRA Security Testing- VulScan Result-SSL Certificate Issues on 18.2
CSCvj33194	Gx_RAR is triggered from CPS when STR is received for Rx session for which no RAR triggered on AAR
CSCvj48906	'yum check-update' shows ~19 packages for upgrade on fresh install
CSCvj62031	Insecure ports 80 open on CPS, Need to be Fixed ASAP
CSCvj73028	monit process on one of lb VM is in stopped state after fresh 18.2 CCO fresh deployment
CSCvj82917	RAA does not have Result Code:2001 in engine and qns logs
CSCvj93363	Error code : 5012 observed post External and Replication VLAN down GR CPS18.3
CSCvj97239	CentOS 7 : glibc (CESA-2018:0805)
CSCvj97328	TPS is not reaching expected level after Traffic Switch over (Site Failure in GR Setup)
CSCvj98488	using pcrfclinet01 as arbiter in HA, but when we do reinit it is getting added in pacemaker resource

CDETS ID	Headline
CSCvj99796	IMSI clearing function in control center can result in 2 Sy STR messages
CSCvk05578	High Rx 5065 response time with secondary key full db scan
CSCvk12418	PCRF is creating SyPrime session but not sending AAR and then later sends Syp STR leading to a 5002
CSCvk14078	RAR delay while using ToD schedules
CSCvk16033	CPS performance impact is seen & call model breaks at 10K TPS within few mins
CSCvk18087	CPS: System upgrade using option 3 fails for Incompatible libdevmapper
CSCvk18956	API keepalive check trap alert and recovery occurs on separate VMs
CSCvk22276	PCRF sending unexpected Gx RAR during custom mute testing
CSCvk23671	BEMS681875: Observing intermittently that Policy Trace stops working
CSCvk28033	Old EDR generated when PB Config changes
CSCvk28074	AIDO process status in diagnostics.sh
CSCvk28087	False logs "Few replica sets are not configured or some members are down"
CSCvk28504	aido server logs are not rotating based on file size
CSCvk29927	geo_mongoconfig_template should be in sync with gr configuration guide
CSCvk30446	Cannot add new set of replica in mongoConfig using API on OSP setup
CSCvk30794	Session expiry time is not honored if G/W does not respond to stale session RARs
CSCvk30990	CPS 18.3 Nessus Vulnerability: Apache Zookeeper Missing Authentication Remote Quorum Joining
CSCvk31015	Exception observed while running E911 feature
CSCvk32228	AIDO Client - ADMIN db not recovered if OPLOG size not defined in mongoconfig.cfg
CSCvk32331	During 18.3 ISSM forward path, restore of cluman from previously taken cluman backup fails
CSCvk32830	vPCRF - PSB - Security fixes
CSCvk33962	CPS Nessus Vulnerability: Pivotal Software Redis 2.6.x < 4.0.3 DoS
CSCvk35290	Display issue for new RAT values (1005/1006) in qns/engine log
CSCvk35874	All QNS services on LB,QNS and pcrfclients are killed every 30 days
CSCvk36422	CALEA listTargetResult text in debug log does not obfuscate the IMSI
CSCvk39390	Issue with ordering of IMSI/MSISDN for SLR(Intermediate) over Sy interface
CSCvk39711	Gx transaction processing message to be corrected in snmp script gen-gx-drop script

CDETS ID	Headline
CSCvk39793	Openstack fresh installation sucessful without redis_enable parameter configuration
CSCvk40776	Assigning p-bit for all the tenants in MOG
CSCvk40979	Support of Flow Usage and Flow Status in ModifyRxDynamicRule
CSCvk40988	Support of MCPTT-Identifier in ModifyRxDynamicRule
CSCvk41519	During 18.3 ISSM,qns process not paused on lb01 after traffic swap
CSCvk44800	PCRF is applying default policy for all subscriber on high TPS
CSCvk45000	Issue with subscriber id in STR/SNA when "Skip Subscriber Id In Slr Intermediate=true"
CSCvk47407	mongo upgrade 3.4
CSCvk48917	QNS node CRD data refresh optimization
CSCvk49834	UM gets disabled even when quota present with subscriber
CSCvk52931	Loss of 1K Subscription Profile Repository (SPR) records when failing from Interface sh1 to sh2
CSCvk53472	PB Publish with SPR config changes results in call-processing impact
CSCvk53841	PCRF is not responding to Gateway with CCA-I message after CPS 18.2 migration
CSCvk60724	Rx binding based on IMSI+FramedIp does not work for second AAR
CSCvk60851	display iso name/patch name in about.sh
CSCvk60936	CALEA provTargetReq does not generate Gx RAR for existing Gx session
CSCvk66772	POST sent to PGW -PCRF has Gx but no UDC Session, BEMS865374 / SR684918844
CSCvk66983	All CRD APIs to add cool down period for crdversion and import all API to increase crdversion once
CSCvk72014	During PB publish QNS VMs load CRD tables simultaneously without staggering
CSCvk72030	Vulnerabilities in wpa_supplicant
CSCvk72151	Vulnerabilities in sssd
CSCvk72178	Vulnerabilities in microcode_ctl
CSCvk72228	Vulnerabilities in patch
CSCvk72240	Vulnerabilities in libvirt
CSCvk72260	Vulnerabilities in openssh
CSCvk72276	Vulnerabilities in git
CSCvk72289	Vulnerabilities in qemu-kvm
CSCvk72307	Vulnerabilities in php

CDETS ID	Headline
CSCvk72331	Vulnerabilities in gnupg2
CSCvk72343	Vulnerabilities in pcs
CSCvk72546	USuM configuration plugin update to Remote SPR needs restart
CSCvk72894	session_cache_ops.sh script - netcat timer increase
CSCvk76306	CALEA specific logging is occurring in the engine log and qns log
CSCvm06686	Logrotate is not happening for graphite_access.log and qns-default_access.log under /var/log/httpd
CSCvm07434	Restarting a qns node while SPR is primary on S2 causes 5012 error codes for all traffic on that QNS
CSCvm09462	Sh UDR TPS is lower than Gx CCR-I TPS after complete GR failover and failback
CSCvm11085	ASA is not seen in Consolidated CDR logs for timer expiry scenario
CSCvm17119	CPS is not taking any traffic
CSCvm17879	mongo_stat.sh causes excessive CPU utilization
CSCvm19253	mongo version 3.4.16 is not coming in CPS Diagnostic output
CSCvm19657	Changing "ADTM" to "Active Traffic Management"
CSCvm20557	Null Pointer exception for Volte while handling AAR
CSCvm21356	LdapChangeMessage broadcast deserialisation throws exception
CSCvm22725	Calea - after start up - create UUID process taking too much time.
CSCvm24594	CentOS 7 : yum-utils (CESA-2018:2285)
CSCvm24598	CentOS 7 : gcc (CESA-2018:0849)
CSCvm24606	CentOS 7 : linux-firmware (CESA-2018:0094) (Spectre)
CSCvm26131	race condition causing missing CALEA AVPs
CSCvm26396	Disabling Extended-BW-NR feature causing call failures
CSCvm26729	F1929: PCRF should be sending new QoS AVP for BW-NR instead of old avp's when qos value > 4294967295
CSCvm42022	Np Interface support:Rule Deactivation Time not sent based on Throttle Duration
CSCvj93363	Error code : 5012 observed post External and Replication VLAN down GR CPS18.3
CSCvk05578	High Rx 5065 response time with secondary key full db scan
CSCvk18956	API keepalive check trap alert and recovery occurs on separate VMs
CSCvk30794	Session expiry time is not honored if G/W does not respond to stale session RARs

CDETS ID	Headline
CSCvk36422	CALEA listTargetResult text in debug log does not obfuscate the IMSI
CSCvk48917	QNS node CRD data refresh optimization
CSCvk53472	PB Publish with SPR config changes results in call-processing impact
CSCvk60936	CALEA provTargetReq does not generate Gx RAR for existing Gx session
CSCvk66983	All CRD APIs to add cool down period for crdversion and import all API to increase crdversion once
CSCvk72546	USuM configuration plugin update to Remote SPR needs restart
CSCvk76306	CALEA specific logging is occurring in the engine log and qns log
CSCvm02867	SVN based CRD publish results in service impact
CSCvm17119	CPS is not taking any traffic (diagnostic failures: upgrade to CPS_18.3.2_20180823_171208_133.iso)
CSCvm19622	IC_MR1: B420 M3 discovery failure: Unable to change server power state-MC Error
CSCvk49018	SVN framework and SVN data out of sync during publish
CSCvm19662	Changing "ADTM" to "Active Traffic Management"

Microservices Resolved CDETS

Table 6 Microservices Resolved CDETS

CDETS ID	Headline
CSCvg54121	DRA throwing incorrect error for number of retries exceeded
CSCvi23347	DRA Hardening: CCR-I timeouts at Relay DRA doesn't clear sessions in Relay DRA's database
CSCvi88541	DRA successfully processing the answer of already timedout request
CSCvi95797	DRA VPAS: Incorrect session count on grafana, not refreshing count after redeployment of Bindings Db
CSCvj93080	PCRF IPv6 session query sent to PCRF even when IPv6 binding is not marked for lookup
CSCvj95108	DRA is sending timeout in 1.7 seconds always when PCRF session query gives no response
CSCvj97280	Delaying Gx CCR-I message process towards PCRF, which is causing to 3002-002 Error back to-wards GW
CSCvk08699	vDRA: Outbounds peers not reconnect after disconnecting from dsTest
CSCvk26397	18.3 DRA Security Testing- Missing HTTP Strict-Transport-Security Header

CDETS ID	Headline
CSCvk30239	vPAS DRA: REST API query for IPv6 binding not working beyond 100TPS
CSCvk34091	DRA is throwing exception for PCRF session query even if not configured in CRD
CSCvk39637	DRA is not putting the PCRF end point to Inactive List if the URL has systax error in configuration
CSCvk40196	Support for consolidating Prometheus stats into single file and format changes
CSCvk46511	DRA Relay: More labels should be included in counter "relay_peer_messages_total"
CSCvk49723	BEMS850905 Change in Bind key Creation Map table structure is not working after the policy publish
CSCvk72430	BEMS789018 P2,CPS vDRA, M Bit not properly set for 281 and 284
CSCvk75938	BEMS861296 API activePeerEndpoints shows incorrect output (output changes with a browser re-fresh)
CSCvm00663	DRA is throwing timeout message instead of Binding DB error when some DBs are down
CSCvm00946	BEMS824052 In 18.2 Api query for "peerDetails" is not working as it was in 13.1 post 18.2 upgrade
CSCvm03827	Revert curl to fix broken build
CSCvm05131	keepalived version v1.2.19.0 build failure
CSCvm05512	DRA - Diameter Requests [CCR-I & AAR] failures after db redeploy without binding/worker restart
CSCvm06498	AAR failing in binding lookup when one of the dbs is down
CSCvm07234	Allow setting vnc ip and ports for packer builds of base vmdk
CSCvm08838	DRA is not able to delete bindings when Session DB is not reachable
CSCvm15870	vPAS: Very high CPU usage on MSISDN+ IMSI bibding DB
CSCvm17454	DRA DB stats shows different count for different binding workers
CSCvm20042	vDRA VNF limited to 31 VMs
CSCvm23823	DRA is not writing the IPv6 binding record in DB from PCRF session query
CSCvm27383	DRA is not sending DPR to all remote peers in case of graceful director shutdown cli.
CSCvm36740	Database records in grafana app summary are not consistent

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 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.

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)