CPS Release Notes, Release 10.1.0

First Published: September 2, 2016

Last Updated: September 13, 2016

Contents

This document describes the new features, feature versions and limitations for the Cisco Policy Suite software. Use this document in combination with documents listed in the Obtaining Documentation and Submitting a Service Request, page 13.

This document includes the following sections:

New and Changed Information

The following sections provide the descriptions of various features that have been added/modified in this release:

Mobile

Diameter Redirect for Gx Localization

CPS can now reject incoming CCR-I messages with DIAMETER_REDIRECT_INDICATION (3006) error by acting as a redirect agent (RFC 3588). This decision to redirect a request is configured using an STG or CRD. CPS expects the STG or CRD to include a Redirect Request Column (of type True or False). There is no restriction on the condition that determines the redirect behavior.

For more information see section *Gx Clients* in *CPS Mobile Configuration Guide*.

Table Driven Predefined Charging Rules

CPS now supports Table Driven Predefined Charging Rules service configuration.

For more information, see section *Gx Service Configuration Objects* in *CPS Mobile Configuration Guide*.

Operations

Bulk Session Termination

CPS now supports the `terminatesessions` utility to support bulk session terminate requests.

In addition, the `show` utility shows the status of the submitted command(s) while the `cancel` utility cancels the further execution of the submitted command.

Note: For fresh installations of CPS 10.1.0, this feature is enabled by default. However, for upgrades from systems prior to CPS 10.1.0, this feature needs to be enabled as follows:

In the `/etc/broadhop/pcrf/features` file, add `com.broadhop.policy.command.feature`.

Remember: For the termination of sessions without any criteria (**ALL**) and termination of sessions with IMSI range as criteria (**IMSIRANGE A-B**), CPS must be configured to create sessions with **tags** field having **ImsiKey:imsi:<imsivalue>** as element. If this element is not configured, the command does not terminate sessions for ALL and IMSI range as criteria.

Important: To eliminate the impact of TPS and session count in the system, add the following entry in the `/etc/broadhop/qns.conf` file on the Cluster Manager VM:

```
-Ddistribution.blocked.duration=1800000
```

The entry value is in milliseconds, which converts to 30 minutes. The recommended value is multiples of 30 minutes.

After configuring the above values, run the following commands:

```
copytoall.sh /etc/broadhop/qns.conf
stopall.sh
startall.sh
```

For more information see *CPS Commands* chapter in *CPS Operations Guide*.

Alarm Name Change Notification

The name of the following alarms has been changed for this and later releases:

Table 1 Alarm Name Changes

Old Alarm Name	New Alarm Name
LdapAllPeersDown	LDAPAllPeersDown
LdapPeerDown	LDAPPeerDown
AllSMSCNotificationServerDown	All SMSC server connections are down
AtLeastOneSMSCNotificationServerUp	Atleast one SMSC server connection is up
SMSCNotificationServerDown	SMSC server connection down
SMSCNotificationServerUp	SMSC server connection up
AllEmailNotificationServerDown	All Email servers not reachable
AtLeastOneEmailNotificationServerUp	At least one Email server is reachable
EmailNotificationServerDown	Email server is not reachable
EmailNotificationServerUp	Email server is reachable

Installation Notes

Download ISO Image

Download the 10.1.0 software package (ISO image) from:

https://software.cisco.com/download/release.html?i=!y&mdfid=284883910&softwareid=284979976&release=10.1.0&os=

Md5sum Details:

3baf9e9d622459ee04f0cb75a000a187 CPS_10.1.0_Base.release.tar.gz

dbe52479f5bb202554d91850b5c732f5 CPS_10.1.0.release.iso

Component Versions

The following table lists the component versions for the CPS 10.1.0 Release:

Table 2 Component Versions

Component	Version
ANDSF	1.3.1.release
API router	1.2.1.release
Audit	1.8.1.release
Balance	4.1.1.release
CALEA	1.1.1.release
Cisco API	1.4.1.release
Cisco CPAR	1.4.1.release
Control Center	3.8.1.release
Congestion Reference Data	1.6.1.release
Core	10.1.0.release
CSB	2.1.1.release
Custom Reference Data	3.1.1.release
DRA	1.2.1.release
DHCP	1.8.1.release
Diameter2	4.1.1.release
Fault Management	1.4.1.release
Hotspot	1.2.1.release
ISG Prepaid	2.2.1.release
LDAP	2.1.1.release
Notification	7.1.1.release
Policy Intel	3.1.1.release
POP-3 Authentication	1.8.1.release

Table 2 Component Versions

Component	Version
RADIUS	3.7.1.release
Recharge Wallet	1.6.1.release
SCE	2.5.1.release
Scheduled Events	1.7.1.release
SPR	3.1.1.release
Unified API	3.1.1.release
Web Services	1.9.1.release

New Installations

- VMware Environment, page 4
- OpenStack Environment, page 4

VMware Environment

To perform a new installation of CPS 10.1.0 in a VMware environment, see *CPS Installation Guide for VMware*.

OpenStack Environment

To perform a new installation of CPS 10.1.0 in an OpenStack environment, see *CPS Installation Guide for OpenStack*.

Upgrading an Existing CPS Installation

To upgrade an existing CPS installation, see *CPS Upgrade Guide*.

Note: In-service software upgrades to 10.1.0 are supported only from CPS 7.0.5 or higher. If needed, upgrade CPS to 7.0.5 or later before proceeding.

Note: In-service software upgrades to 10.1.0 are supported only for Mobile installations. Other CPS installation types (Wi-Fi, MOG) cannot be upgraded using ISSU.

Note: Currently, All-in-One (AIO) upgrades are not supported.

Post Upgrade Steps

Re-apply Configuration Changes

After the 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 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 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, this 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 customer needs to reconfigure multiple Subscriber Id in SpendingLimitReport under Service Configurations.

Additional Notes

The following section contains some additional notes which are 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.
- CSCuq83478: Diameter haproxy configuration is not correct for IPv6 addresses.

  Fix: IPv6 tables need to be turned OFF for IPv6 traffic on lb01, lb02. Management and IPv6 Gx traffic should be on different VLANs in VLAN.csv file at the time of deployment.
- CSCux20675: High message timeouts observed after qns*xx* power on

  Problem Description: High Timeouts observed when qnsxx is brought back into service/recovered after an VM outage.

  Conditions/Scenario: Normal HA setup with call model running.

  Workaround: Any recovery (blade/VM) should be done during off-peak hours when other VMs CPU is < 50%.
- CSCuz43943: Replacing SrcAddress and Port to any is not working

  Problem Description: PCRF has no option to ignore SOURCE IP in AAR request and send ANY to PGW.

  Conditions/Scenario: SOURCE IP is sent in flow description in AAR from the AF.

  Workaround: Custom policy needs to be added in AF to replace the SOURCE IP in flows to ANY before sending it to PCRF.
- CSCuz44551: Usage Monitoring key AVP sent in GX RAR when no Usage monitoring needed

  Problem Description: Usage Monitoring key AVP is sent out in Gx RAR in case no Usage monitoring is required.

  Conditions/Scenario: The Monitoring key AVP is sent even if the usage monitoring is enabled/disabled for sponsored data use case.

  Workaround: This issue has no adverse effect as monitoring key without monitoring information in Gx RAR is ignored by PGW.
- CSCuy82522: Incorrect config file on system leads to SSH blocked after upgrade

  Problem Description: SSH is blocked on Installer

  Conditions/Scenario: The /root/.ssh/config file is modified duing install.sh which blocks ssh

  Workaround: The /root/.ssh/config file is modified as below which blocks ssh.

  ```
  [root@C_installer .ssh]# cat /root/.ssh/config
  StrictHostKeyChecking=noUserKnownHostsFile=/dev/null
  LogLevel=quiet
  ```

  Manually change to:

  ```
  [root@C_installer .ssh]# cat /root/.ssh/config
  StrictHostKeyChecking=no
  UserKnownHostsFile=/dev/null
  LogLevel=quiet
  ```
- CSCuy82546: custom config file results in HTTPD process unable to start after ISSU

  Problem Description: ISSU upgrade fails with errors:

  ```
  http://installer/rpms/quantum/qps/x86_64/repodata/repomd.xml: [Errno 14] PYCURL ERROR 7 - "couldn't
  connect to host"
  Trying other mirror.
  Error: Cannot retrieve repository metadata (repomd.xml) for repository: QPS-Repository. Please
  verify its path and try again
  ```

```
You could try using --skip-broken to work around the problem
You could try running: rpm -Va --nofiles --nodigest

Starting httpd: Syntax error on line 1 of /etc/httpd/conf.d/reqtimeout.conf:
Invalid command 'RequestReadTimeout', perhaps misspelled or defined by a module not included in the
server configuration
                                [FAILED]
```

Conditions/Scenario: The httpd process is unable to start.

Workaround: Check if `/etc/httpd/conf.d/reqtimeout.load` is present.

If it is, edit /`etc/httpd/conf.d/reqtimeout.conf` and add `Include conf.d/reqtimeout.load` as the first line of the file. For example:

```
[root@installer cluman]# cat /etc/httpd/conf.d/reqtimeout.conf
Include conf.d/reqtimeout.load
RequestReadTimeout header=10-20,minrate=500
RequestReadTimeout body=10,minrate=500
```

- 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.

- If TPS is high, user needs to disable “STA”. To disable STA, user needs to create custom policies. For more information, contact your Contact Technical Representative.

- CSCuz59023: CPS should not allow non-root users to check sudosh logs.

  Problem Description: TACACs users that do not have superuser privileges can access all the files on the systems and some of the files (sudosh logs) contain sensitive data. Currently read-only/admin users can read the sudosh logs.

  Conditions/Scenario: User having qns-ro/qns-admin role.

  Workaround: A log reader utility has been implemented so that non-root user will not be allowed to view the sudosh logs.

  Users (qns-ro, qns-admin) are allowed to view logs files at specific paths according to role and maintenance requirement. User are able to access logs via only white listed path. As per current configuration `/var/log/`, `/var/log/broadhop/scripts/`, `/var/log/httpd`, `/var/log/redis`, `/var/log/broadhop` paths have been white listed. There is no recursive access implemented. Hence any new/sub directory needs to be white listed separately.

  User will not be able to execute `cat`, `less`, `more`, `find` commands using sudo anymore.

  For reading any file, user needs to execute the script using sudo.

  ```
  $  sudo /var/qps/bin/support/logReader.py -r h -n 2 -f /var/log/puppet.log

  -r allowed t,tf,h which corresponds to tail,tailf and head respectively
  -n this is optional parameter. No. of lines to be read this works by joining the with -r option.
  -f complete file path to be read.
  ```

  Support reading `gunzipped` files is also available.

- CSCuz87423: qns entries in haproxy.cfg is only 4 but configured qns is 16.

Problem Description: Puppet adds entries for only four policy server (qns) only in `/etc/haproxy/haproxy.cfg` on lb01/02 if user configures more than four policy server (qns) instances.

Conditions/Scenario: When the user configures **haproxy_qns_instances** value equal to actual policy server (qns) instances which are greater than four in **Configurations.csv** file.

Workarounds:

Workaround 1:

1. Replace the following line in `/var/qps/install/current/puppet/modules/qps/manifests/haproxy.pp` file

   ```
   if( ( $::haproxy_qns_instances ) and ( $::haproxy_qns_instances < $::qns_instances ) ) {
   ```

   with

   ```
   if( ( $::haproxy_qns_instances ) and ( $::haproxy_qns_instances <= $::qns_instances ) ) {
   ```

2. Run `build_puppet.sh` script from Cluster Manager to rebuild puppet.
3. Run `/etc/init.d/vm-init` from both lb01 and lb02.

Workaround 2:

Add entries for total number of qns instances manually into `/etc/haproxy/haproxy.cfg` file on both lb01 and lb02.

- CSCvb13731: False SNMP Alarms of pcrfclient01-pb & CC are seen in traps.

  Problem Description: False critical SNMP alarms are generated for pcrfclient01 - PB and CC.

  Conditions/Scenario: There are traps for process going down and clear traps for coming up.

  However, when checked the qns process for PB and CC is up and running and the PID is constant.

  The snippet of traps is as below:

  ```
  2016-08-30T02:19:59.888561-04:00 lb01 snmptrapd[6457]: 2016-08-30 02:19:59 pcrfclient01
  [172.20.32.168] (via UDP: [172.20.32.168]:45367->[172.20.32.161]) TRAP, SNMP v1, community
  public#012#011BROADHOP-MIB::broadhopNotificationPrefix Enterprise Specific Trap
  (BROADHOP-MIB::broadhopClearAlarm) Uptime: 49117561#012#011BROADHOP-MIB::broadhopAlarmDeviceName =
  STRING: QNS#011BROADHOP-MIB::broadhopAlarmErrorNumber = INTEGER:
  7300#011BROADHOP-MIB::broadhopAlarmErrorText = STRING: KpiEvent [id=7300,values={msg="controlcenter
  server on pcrfclient01 vm is up", sub_id=7301, event_host=pcrfclient02,
  status=up}]#011BROADHOP-MIB::broadhopAlarmDateAndTime = STRING: 2016-08-30 at 02:19:59
  -0400#011BROADHOP-MIB::broadhopAlarmProbableCause = STRING:
  #011BROADHOP-MIB::broadhopAlarmAdditionalInfo = STRING:
  ```

  Workarounds: To solve the issue, execute the following script on pcrfclient01 VM:

  ```
  /etc/init.d/vm-init
  ```

  Note: Do not execute `diagnostics.sh` script on pcrfclient01 after you have executed the `vm-init` script. You can execute the `diagnostics.sh` script on Cluster Manager VM.

Limitations and Restrictions

This section covers the following topics:

Limitations

- If you have a system with the old installer (6.1 or prior), it is mandatory to use the new installer to create VMs and use the new release trains. The latest release train does not work with the old environment (AIO/HA).
- 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 which 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 sessions 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 which 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:

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

  This is a known issue affecting ESXi 5.x. Currently, there is no workaround. The `messages.log` file entries are cosmetic and can be safely ignored. For more information, refer to http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2094561
- CSCva02957: Redis instances will 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)

The following is the list of publicly known Common Vulnerabilities and Exposures (CVE) apply to this version of CPS:

- For OpenSSL:
  - March 2016 Vulnerabilities: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl

  Currently, only two medium vulnerabilities out of March 2016 incident (CVE-2016-0703 and CVE-2016-0704) are open. The rest of the OpenSSL vulnerabilities have been fixed in this release.

- Pacemaker v1.1.10 Vulnerability (CVE-2013-0281):

  Pacemaker contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service condition on a targeted system. The vulnerability exists because the network socket used by the affected software fails to close a remote connection after a certain period of inactivity. An unauthenticated, remote attacker could exploit this vulnerability by connecting to the Pacemaker socket. When connected, the socket may wait for an infinite amount of time to perceive the authentication credentials, which could allow the attacker to block all other connection attempts, causing a DoS condition for legitimate users.

CDETS

The following sections lists Open CDETS and Resolved CDETS for Cisco Policy Suite. 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 the CPS 10.1.0 release.

Table 3 Open CDETS

CDETS ID	Headline
CSCuu70484	Grafana: Zooming Issue
CSCux38241	GR A/A sys test: Grafana stats missing in graph during and after failover
CSCux55463	CPS SCTP connection with SSl is taking ~20min to come up during linkflap
CSCuz41330	diagnostics.sh: why prompt for password for all operations
CSCuz52587	Evaluation of CPS for OpenSSL May 2016 Vulnerabilities
CSCuz52898	Error is recorded into the puppet log
CSCuz82321	Receiving "Skipping message due to queue overload" in cons..... qns log
CSCuz92894	Can't delete subscribers when balance replica set not in sm01 and sm02
CSCva06854	GC (Allocation Failure) error is coming frequently due to high CPU at LB
CSCva10877	CPS 9.0 Haproxy doesn't allow HTTPS with clients using java <1.8

Table 3 Open CDETS

CDETS ID	Headline
CSCva12736	gen-db-traps.sh script causing continuous stream of false SNMP alerts
CSCva15232	CPS 910 SVN run repository getting deleted
CSCva28926	session_cache_ops.sh --db-shrink fails due to time out
CSCva42625	On pcrfclients at /var/lib/corosync, core files are taking huge space
CSCva46231	CPS: CPS must not send success CCA-U if charging-rule-report AVP missing
CSCva49160	Need patch of OpenSSH to address security vulnerability
CSCva60409	Puppet failure after vm-init due to group add failure.
CSCva63979	Performance over IPv6
CSCva66134	Mongo backup in backup and restore guide
CSCva74240	PCRF is not restoring default bearer on Rx session Termination by MOG
CSCva74353	Grafana memory charts are not counting buffers and cache as free memory
CSCva77930	Flag files being stored under /var/tmp on CPS installation
CSCva78158	Disable Admin DB error logging.
CSCva78370	env_export.sh only backs up one shard for balance.
CSCva84576	session_cache_ops.sh script not working for multi clusters
CSCva84940	running puppet-update-all.sh on cluman Wipes all data from cluman
CSCva85852	RAR's replied with 5002
CSCva85936	Logs which require a rotation mechanism
CSCva85997	Exception while executing policy action: DiameterRxTGPPDeviceMgr
CSCva86270	Swap memory used on lb's
CSCva91263	Multiple Services with AutoBalanceProvisioning from Unified API broken
CSCva92484	PSIRT: Evaluation of CPS for TCP Vulnerability, August 2016
CSCva93020	SPR DB Interoperability Issue during CPS upgrade from older version
CSCva97068	aggstats file grows uncontrollably occasionally after collectd restart
CSCvb01666	Policy Builder reacts slowly to user interaction
CSCvb01926	ERROR c.b.c.executor.impl.CommandExecutor for BulkSessionTermination
CSCvb01931	CPS: Too many errors seen without any explanation
CSCvb02229	Observed duplicate DIAMETER_SUCCESS(2001) AVP in RX STA.
CSCvb13731	False SNMP Alarms of pcrfclient01-pb & CC are seen in traps.
CSCvb18576	Orchestration API fails to create sysuser

Resolved CDETS

The following table lists the resolved/verified CDETS in the CPS 10.1.0 release.

Table 4 Resolved CDETS

CDETS ID	Headline
CSCuy82102	Remove IPv6 from STR in case ANGW has only IPv4 address
CSCva06624	Two callbacks are coming where there is no RAR received within timeout.
CSCva12698	Can't run scripts needing valid URLs in UnifiedApi.wsdl/UnifiedApi.xsd.
CSCva17209	Sy Interface: key off of 2001 result code for learning new Origin-Host
CSCva17876	Relax missing AVP check to bring the functionality similar to CPS7.5
CSCva26149	wrong AVP code observing in logs
CSCva27253	PB Service API resulting in 404 error
CSCva30491	Gx retry not happening as configured
CSCva31942	snmptrapd not sending traps if multiple trap receivers configured.
CSCva43165	Account Balance Template optimization
CSCva47411	Sh retry not working with LINEAR_INTERVAL Backoff Algorithm
CSCva48836	Sh retries on lb level are “eating” from qns level retries
CSCva49095	diagnostics.sh [FAIL]: numd-site-2 spr node is not available
CSCva54600	PCRF is arming extra Event trigger while removing Dynamic rule in RAR
CSCva57082	redis-server is running and consuming resources even if it is disabled.
CSCva62242	Sy-SNR Null Session Id
CSCva71592	Sh retry to Alternate peer
CSCva75688	CPS initiate Gx_RAR and Sy' STR simultaneously on bulkSessionTermination
CSCva75707	All session of same subscriber should get deleted at same time
CSCva79724	Rollback fails when custom hostnames w/ standard hostnames in mongo conf
CSCva80124	password is getting logged in command.log
CSCva84226	Rollback fails when additional hosts used in mongo config file
CSCva89414	Command status not moved to completed when no distributions are created
CSCva89422	Output when invalid number is provided with --rate option
CSCva94230	BulkSessionTermination commands are not working for high no. of sessions
CSCvb00311	Incorrect description to configuration [Avp Code to Disable Query]
CSCvb14527	API orchestration post config fails due to mentioned config parameter

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 the Cisco Policy Suite.

- *CPS ANDSF Configuration Guide*
- *CPS Backup and Restore Guide*

- *CPS Geographic Redundancy Guide*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide - VMware*
- *CPS Mobile Configuration Guide*
- *CPS Operations Guide*
- *CPS Policy Reporting Guide*
- *CPS Release Notes*
- *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *CPS Troubleshooting Guide*
- *CPS Unified API Reference Guide*
- *CPS Upgrade Guide*
- *CPS Wi-Fi Configuration Guide*

The documents can be downloaded from the following links:

- All Guides

  http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-bng/products-installation-and-configuration-guides-list.html

- Mobile Configuration Guide:
  http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-mobile/products-installation-and-configuration-guides-list.html

- Wi-Fi Configuration Guide:
  http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-wi-fi/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*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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)

This document is to be used in conjunction with the documents listed in the Obtaining Documentation and Submitting a Service Request, page 13 section.

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.

© 2016 Cisco Systems, Inc. All rights reserved.