CPS Release Notes, Release 11.1.0

First Published: December 23, 2016

Last Updated: December 23, 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 11.

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

Asynchronous Notifications to a Notification Server

Real-time notifications have been enhanced to allow the sending of REST/JSON messages to a defined server when policy thresholds are breached.

For more information, see the section “Real Time Notifications” in Notification Services chapter in the *CPS Mobile Configuration Guide*. A Content Type pull-down list has been added to the Real Time Notification configuration in which you can select text/XML, application/json, or application/x-www-form-urlencoded.

Default/Dedicated Bearer Procedures for Automated Traffic Management

CPS now supports the creation and modification of default and dedicated bearers based on attributes received from MOG over the Rx prime interface.

For more information, see “Rx Services” and “Service Configuration Objects” in the *CPS Mobile Configuration Guide*.

Diameter AVP handling, logically derived attributes mapped to Custom AVP

CPS already supports mapping of Custom AVPs or 3GPP defined AVPs and stores the mapped target AVP values in a Diameter Custom AVP session. Previously, CPS did not create, modify, or update target AVPs after the Custom AVP session was initially created. Now, through the entire session lifecycle, CPS can create new target AVPs or modify/update previously stored target AVP values with its corresponding (received or evaluated) updated source AVP value. Once the target AVP is created, the AVP is stored in the custom AVP session and is sent out with the latest updated values in the future diameter messages it is configured for. Until the source AVP is created, CPS does not send the corresponding target AVPs over the configured outgoing Diameter messages.

CPS also supports the ability to forward these mapped target AVPs over any or all outgoing Diameter messages, including outgoing responses on the same or different interface.

Note:

- In case multiple source AVPs are mapped to the same target AVP, the value of the target AVP is overwritten with the last evaluated source AVP mapping.

For more information see topic “Mapped Target AVPs Not Received in Diameter Message” in *CPS Troubleshooting Guide*.

Selective Muting of Flows

CPS now supports the selective muting of the flow corresponding to a TDF-Application-Identifier on a dedicated bearer after it receives the first Application_Start event trigger on the dedicated bearer from PCEF.

For the default bearer, CPS selectively mutes the flow corresponding to a TDF-Application-Identifier after it receives the Application_Start event trigger on the default bearer from PCEF and maximum limit is reached on the dedicated bearer.

For more information, see “Diameter Configuration” in the *CPS Mobile Configuration Guide*.

Operations

MIB Additions or Changes

No changes are introduced in this release.

SNMP Alarm Additions or Changes

No new alarms are introduced in this release.

Statistics Additions or Changes

No changes are introduced in this release.

Installation Notes

Download ISO Image

Download the 11.1.0 software package (ISO image) from:

https://software.cisco.com/download/release.html?i=!y&mdfid=284883882&softwareid=284979976&release=11.1.0

Md5sum Details:

385dce1ca964e968f4d43b7901919f0d Base_11.1.0_20161213_060520_412.qcow2.tar.gz

10553ab4a79f806089f753194a44d1db	Base_11.1.0_20161213_060520_412.vmdk.tar.gz
c2ec318237d0a8b2055a015fefe6712d	CPS_11.1.0_20161213_060520_412.iso

Component Versions

The following table lists the component versions for the CPS 11.1.0 Release:

Table 1 Component Versions

Component	Version
ANDSF	11.1.0.r096038
API router	11.1.0.r096038
Audit	11.1.0.r096038
Balance	11.1.0.r096038
CALEA	11.1.0.r097120
Cisco API	11.1.0.r096038
Cisco CPAR	11.1.0.r096038
Control Center	11.1.0.r096039
Congestion Reference Data	11.1.0.r096038
Core	11.1.0.r097143
CSB	11.1.0.r096954
Custom Reference Data	11.1.0.r096040
DRA	11.1.0.r096040
DHCP	11.1.0.r096040
Diameter2	11.1.0.r097498
Entitlement	11.1.0.r096047
Fault Management	11.1.0.r096040
ISG Prepaid	11.1.0.r096040
LDAP	11.1.0.r096040
Notification	11.1.0.r097303
Policy Intel	11.1.0.r096233
POP-3 Authentication	11.1.0.r096041
RADIUS	11.1.0.r096041
Recharge Wallet	11.1.0.r096501
SCE	11.1.0.r097390
Scheduled Events	11.1.0.r096501
SPR	11.1.0.r096501
Unified API	11.1.0.r096501
Web Services	11.1.0.r096501

New Installations

- VMware Environment, page 4

VMware Environment

To perform a new installation of CPS 11.1.0 in a VMware environment, see *CPS Installation Guide for VMware*.

OpenStack Environment

To perform a new installation of CPS 11.1.0 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 11.1.0 are supported only from CPS 8.1 or higher.

Note: In-service software upgrades to 11.1.0 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.

- CSCuz11476: Puppet fails to run and configure properly LB nodes other than lb01/lb02

  If upgrading from a release prior to 10.0.0, the following changes are made to the folders and files on the Cluster Manager:

  – The contents of `/var/qps/current_config/image-map` on the Cluster Manager is modified to consolidate the existing lb entries (lb01 and lb02) into a single lb entry (lb=iomanager).

  – The existing `/var/qps/current_config/etc/broadhop/iomanager01` and `/var/qps/current_config/etc/broadhop/iomanager02` directories are consolidated into a single `/var/qps/current_config/etc/broadhop/iomanager` directory.

- CSCuy23530: Receiving error msg while creating subscriber from SPR API

  Conditions/Scenario: If `clusterPeers` flag is configured in `/etc/broadhop/iomanager01/qns.conf` file OR `/etc/broadhop/iomanager02/qns.conf` file in previous installation of CPS and you are upgrading to 9.1.0.

  Apply Configuration Change:

  If `clusterPeers` flag is configured move the flag with same value to `/etc/broadhop/qns.conf` file

OR

If `clusterPeers` flag is not configured, add `clusterPeers` entry to `/etc/broadhop/qns.conf` file. Also remove `clusterPeers` entry from `/etc/broadhop/iomanager01/qns.conf` file and `/etc/broadhop/iomanager02/qns.conf` file.

Impact if above change is not applied:

If `clusterPeers` flag is not moved to new location, cluster broadcast message will not happen.

Recommended: This change is highly recommended to be applied.

- 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.

- CSCvb74725: Avoid manual steps in API based GR installation

  Problem: 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 --add 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 will replace 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 --add all
```

- CSCvc56428 / CSCvc56520: Rollback:11.1to10.1_Diameter endpoint not coming up

  Problem: During an ISSU rollback from 11.1 to 10.1, diameter endpoints did not come up.

  Workaround: Clear the endpoints from osgi console for each endpoint using the clearExcludedEndpoints command. For example:

```
[root@CPS~]# telnet lb01 9093
Trying xx.xx.xx.xx...
Connected to lb01.
Escape character is '^]'.

osgi> clearExcludedEndpoints
ZMQ SILO cleared.

osgi> disconnect
Disconnect from console? (y/n; default=y)
```

Limitations and Restrictions

This section covers the following topics:

Limitations

- 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:

- 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.
- TCP Off-path Exploits Vulnerabilities (CVE-2016-5696)

  On August 10th, 2016, a new vulnerability on the TCP stack of Linux kernels was disclosed. This vulnerability may allow an attacker to perform a blind data injection on a TCP session, or reset an established session.

  References:

  - NVD entry for CVE-2016-5696
  - RedHat advisory for CVE-2016-5696
- Dirty COW Vulnerability (CVE-2016-5195)

  On October 19th, 2016, a new vulnerability was disclosed that a race condition existed in the memory manager of the Linux kernel. This vulnerability could allow an unprivileged local user to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

  For more information, see: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-linux
- NTF NTP Vulnerabilities (CVE-2016-9311, CVE-2016-9310, CVE-2016-7427, CVE-2016-7428, CVE-2016-9312, CVE-2016-7431, CVE-2016-7434, CVE-2016-7429, CVE-2016-7426, CVE-2016-7433)

Cisco Policy Suite includes a version of ntpd that is affected by the vulnerabilities. For more information, see: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161123-ntpd

- OpenSSL Vulnerabilities

  On September 22nd, 2016, the OpenSSL Software Foundation released an advisory with details on fourteen vulnerabilities. Out of those fourteen vulnerabilities, the OpenSSL Software Foundation classifies one as " High Severity" , one as " Moderate Severity" and the other twelve as " Low Severity" .

  On September 26th the OpenSSL Software Foundation released an additional advisory with details on two new vulnerabilities affecting some of the OpenSSL versions that were released to address the vulnerabilities disclosed on the 22nd September Advisory, one of the new vulnerabilities was rated as " High Severity" and the other as " Moderate Severity" .

  For more information, see https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160927-openssl

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 11.1.0 release.

Table 2 Open CDETS

CDETS ID	Headline
CSCvc01018	SVN repos is down intermittently on AIO setup
CSCvc21144	CPS: E2E and H2H values getting set to 0 in Gy RAA
CSCvc26506	CPS: Inconsistency seen in deducting quota
CSCvc33587	PCRF is sending Rx_RAR with Specific-Action 8 when only default bearer is BOOSTed from MOG
CSCvc35495	CPS not sending DPCC Status to MOG when default bearer BOOST resulted into dedicated bearer collapse
CSCvc36484	Validation for AF-App-Id is failing when present at AF Session Level in Rx-AAR
CSCvc37328	Randomly one of qns showing High load compared to other qns VM
CSCvc37519	Sh Call model impact - Continuous Timeout on Sh SNR
CSCvc38446	MOG is picking Media-Type from session in case of PUT request
CSCvc40535	CPS sends Custom AVP with latest AVP code though AVP Mapping configured with earlier AVP code
CSCvc41628	Collectd Error - exec plugin: exec_read_one: error = try 'mongostat --help' for more information

Table 2 Open CDETS

CDETS ID	Headline
CSCvc41798	CPS must log WARN/ERROR for Messages getting Time Out for better Troubleshooting
CSCvc41885	FSM_Overloaded Exceptions seen during longevity
CSCvc42265	Not able to send TDF-Application-ID as Custom AVP on Target Interface
CSCvc43947	CPS: Realtime Notification configuration is not backward compatible
CSCvc45288	Evaluation of qps for NTP November 2016 Vulnerabilities
CSCvc46271	Unexpected exception processing message
CSCvc53849	ActiveMQConnFactoryWrapper exception during ISSU
CSCvc54761	Vendor ID bit not set in case Pb has configuration set with Vendor Cisco and ciscoSystems
CSCvc56074	3GPP to 3GPP AVP Mapping in AVP Mapping Table allows Custom AVP to be configured as Target AVP
CSCvc56358	High response time observed for Gx-Rx call with RealTimeNotification.
CSCvc56428 CSCvc56520	Rollback:11.1 to 10.1_env_import.sh did not run successfully

Resolved CDETS

The following table lists the resolved/verified CDETS in the CPS 11.1.0 release.

Table 3 Resolved CDETS

CDETS ID	Headline
CSCuy67211	OCSQuotaRecharge causing timeouts and high CPU in longevity
CSCva60409	Puppet failure after vm-init due to group add failure.
CSCvb33505	Hijack the mind attribute value
CSCvb56017	ChangeSubscriberAvps does not properly delete specific AVPs
CSCvb56051	AF-Application-ID received at session level is not processed by CPS
CSCvb65001	Case Senstive Column Name RxSponseredDataChargingParameterSTGConfiguration
CSCvb65312	CPS sending infinite SLR message on receiving SLA on mismatch number of counter
CSCvb65376	while terminating the MSRP, RX- STA is not sent in response to RX-STR.
CSCvb69540	CPS uses 'Missing AVP value' even when the attribute is received as empty/blank in Sh UDA.
CSCvb71372	4G to 3G and 3G to 4G RAT change from PGW to PCRF giving incorrect values
CSCvb72350	Few files are missing in /etc/int.d/ observed in 12.0 and 11.0 AIO fresh installation
CSCvb78893	Empty values in subscriber profile AVPs not working when single sh request is enabled
CSCvc01658	CALEA: maxLength and minLength for 'mf-x2-ip-address' differs from XML schema
CSCvc07366	sudo script in CPS allows qns user to escalate process permissions to root
CSCvc16563	Improve PB performance response to handle a very large number of xmi files

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 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 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.